BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 16-1404

29 MAY 2015

AIR FORCE MATERIEL COMMAND
Supplement

17 FEBRUARY 2016

WRIGHT-PATTERSON AIR FORCE BASE
Supplement

18 JANUARY 2017
Certified Current, 5 February 2020
Operations Support

AIR FORCE 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: SAF/AAZ

Certified by: SAF/AA
(Ms. Zarodkiewicz)

Supersedes: AFI 31-401, 1 November 2005;
AFI 31-406, 29 July 2004

Pages: 116

(AFMC)

OPR: HQ AFMC/IP

Certified by: HQ AFMC/IP
(Mr David D Day)

Supersedes: AFI 31-401_AFMCSUP,
19 March 2014

Pages: 116

(WRIGHTPATTERSONAFB)

OPR: 88 ABW/IPI

Certified by: 88 ABW/IP
(Mr. Danny Myers)

Supersedes: AFI31-401_AFMCSUP_
WRIGHTPATTERSONAFBSUP,
26 January 2011

Pages: 6

This publication implements Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*; Department of Defense (DoD) Directive 5210.50, *Management of Serious Security Incidents Involving Classified Information*, DoD Instruction (DoDI) 5210.02, *Access and Dissemination of RD and FRD*, DoDI 5210.83, *DoD Unclassified Controlled Nuclear Information (UCNI)*, DoD Manual (DoDM) 5200.01, *DoD Information Security Program, Volume 1, Volume 2, Volume 3, and Volume 4*; and DoDM 5200.45, *Instructions for Developing Security Classification Guides*. It applies to individuals at all levels who create, handle, or store classified information and CUI, including Air Force Reserve, Air National Guard (ANG), and contractors when stated in the contract or DD Form 254, *Department of Defense Contract Security Classification Specification*, except where noted otherwise. This AFI may be supplemented at any level, but all supplements will be routed to the Office of Primary Responsibility (OPR) prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847 from the field through the appropriate chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, and T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the tier numbers. Submit requests for waivers through the chain of command to the appropriate tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

(AFMC) This instruction extends the guidance of AFI 16-1404, *Air Force Information Security Program*. This supplement replaces AFMC supplement to AFI 31-401; major change includes open storage supplemental controls can only be 4 hour checks or intrusion detection system. Supplement adds requirements of Top Secret accountability, Security Manager Meetings, and the visit of Center/Wing organizations to complete the Center/Wing Annual Self-Inspection Report. This supplement is applicable to US Air Force Reserve units and personnel tenant on AFMC Installations. This publication does not apply to the Air National Guard. This publication may be supplemented at any level, but all Supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command to HQ AFMC/IP. Submit written requests for clarification to this supplement to HQ AFMC/IP. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air

Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

(WRIGHTPATTERSONAFB) AFI16-1404, 29 May 2015, is supplemented as follows: This supplement implements Air Force Instruction (AFI) 16-1404, *Air Force Information Security Program*, and AFI16-1404_AFMCSUP, *Air Force Materiel Command Information Security Program*. It applies to all organizations located on Wright-Patterson AFB (WPAFB), including US Air Force Reserve units and other units under applicable host-tenant support agreements. Send comments and suggestions about this publication for improvements on AF Form 847, *Recommendation for Change of Publication*, to the Office of Primary Responsibility (OPR). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

The publication has been substantially revised and must be completely reviewed.

(WRIGHTPATTERSONAFB) This supplement has been substantially revised and must be completely reviewed. Major changes include clarification of security manager duties, and additional information for visitors requiring access.

Chapter 1

PROGRAM OVERVIEW AND ADDITIONAL ROLES AND RESPONSIBILITIES

1.1. Air Force Security Enterprise. AFPD 16-14 defines the Air Force Security Enterprise as the organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard AF personnel, information, operations, resources, technologies, facilities, and assets against harm, loss, or hostile acts and influences.

1.1. (AFMC) Air Force Security Enterprise. Air Force Security Enterprise also includes technology development and acquisition programs (including testing and sustainment activities) during the development, acquisition, fielding, sustainment, decommission, and disposal of systems, subsystems, end items, and services as defined in DoDD 5000.01, Defense Acquisition System; DoDI 5000.02, Operation of the Defense Acquisition System; DoDI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E); DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN); AFI 63-101/20-101, Integrated Life Cycle Management (ILCM); and AFPAM 63-113, Program Protection Planning for Life Cycle Management.

1.2. Information Protection. Information Protection is a subset of the Air Force Security Enterprise. Information Protection consists of a set of three core security disciplines (Personnel, Industrial, and Information Security) used to:

1.2.1. Determine military, civilian, and contractor personnel's eligibility to access classified information or occupy a sensitive position (Personnel Security).

1.2.2. Ensure the protection of classified information and controlled unclassified information (CUI) released or disclosed to industry in connection with classified contracts (Industrial Security).

1.2.3. Protect classified information and CUI that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security (Information Security).

1.3. Information Protection Oversight. These key positions direct, administer, and oversee management, functioning and effectiveness of Information Protection.

1.3.1. The Senior Agency Official (SAF/AA) is the Secretary of the Air Force appointed authority responsible for the oversight of Information Protection for the Air Force.

1.3.2. The Security Program Executive (SPE) is appointed by the MAJCOM/DRU Commander in accordance with AFPD 16-14 and is responsible for oversight of Information Protection for their MAJCOM/DRU.

1.3.2. **(AFMC)** AFMC/CV is the AFMC SPE.

1.3.2.1. **(Added-AFMC)** Center CVs are the Center's SPE.

1.3.3. Wing Commanders provide oversight of Information Protection by ensuring security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate, for their wings. This may be delegated to the Wing/CV.

1.3.3. **(AFMC)** This also applies to the 66 ABG Commander and AEDC Commander.

1.3.3. **(WRIGHTPATTERSONAFB)** At Wright-Patterson AFB this responsibility has been delegated to 88 ABW/CV.

1.3.3.1. **(Added-AFMC)** Oversight provided to units/organizations outside the ABW/TW/ABG/AEDC will be defined in host tenant support agreements, memorandum of understanding (MOU), memorandum of agreement (MOA), or Center supplement in accordance with AFI 25-201. **(T-2).**

1.4. Information Protection Managers. These key positions develop guidance, as necessary, and serve as principal advisors to the personnel identified in paragraph 1.3.

1.4.1. Director of Security, Special Program Oversight and Information Protection (SAF/AAZ) is responsible to the Senior Agency Official and addresses the equities within the functional portfolio related to Information Protection.

1.4.2. MAJCOM/DRU Director, Information Protection is responsible to the SPE and for integrating Information Protection into MAJCOM/DRU operations and provides oversight and direction to the security specialists assigned to the MAJCOM/DRU Information Protection Directorate/organizational structure.

1.4.2. **(AFMC)** HQ AFMC/IP is AFMC's Director, Information Protection.

1.4.2.1. **(Added-AFMC)** The Center CV is responsible for assigning a Center Chief, Information Protection (CIP) responsible for advising the Center in Information Protection (IP) policy and processes. The Center CIP may be dual-hatted as the Wing CIP or organizationally aligned elsewhere within the Center as determined by the Center/CV. Center CIPs will coordinate with Wing CIPs at all locations where the Center has organizations to ensure IP support requirements are agreed upon and delegated appropriately through host tenant support agreements, MOU, MOA, formal Center-to-Center level agreements, or Center supplement in accordance with AFI 25-201. **(T-2).**

1.4.3. Chief, Information Protection. Executes Information Protection on behalf of the Wing Commander and provides oversight and direction to group and squadron commanders, directors, and security managers, and the security specialists assigned to the Wing Information Protection Office.

1.4.3. **(AFMC)** Air Base Wing/Test Wing (including 66 ABG and AEDC) IP office is the Wing CIP. The Wing CIP provides support and oversight to all organizations within the Wing, to include all tenant organizations when required by a host tenant support agreement, MOU, or MOA in accordance with AFI 25-201.

1.4.3.1. **(Added-AFMC)** The Center CIP serves as the interface with MAJCOM and Center leadership in the development and implementation of IP policy and procedures across the Center.

1.4.4. Commanders and Directors ensure military and civilian personnel are properly cleared for access to classified information and CUI, integrate contractors into their existing security programs, and protect classified information and CUI under their authority to support Information Protection.

1.5. Information Protection Implementation. The key security professionals below are responsible for implementing Information Protection core security disciplines (information, industrial, and personnel security).

1.5.1. Security Specialists are Office of Personnel Management (OPM) occupational series 0080, Security Administration, and are responsible for implementing Information Protection core security disciplines (Information, Personnel, and Industrial Security). Security Specialist responsible for these core security disciplines:

1.5.1.1. At a MAJCOM/DRU are assigned to the Information Protection Directorate and report to the MAJCOM/DRU Director, Information Protection.

1.5.1.1. **(AFMC)** At a Center, Security Specialists that manage the Center's Information Protection program are assigned to the IP Office and report to the Center CIP.

1.5.1.2. At Wings are assigned to the Wing Information Protection Office and report to the Wing Chief, Information Protection.

1.5.1.3. **(Added-AFMC)** Security Specialists are also assigned within other organizations and perform functions which incorporate the core security disciplines into unique organizational missions such as research, development, acquisition, and test activities.

1.5.2. Security managers are principle advisors to group/squadron/detachment commanders, and directors. They implement the core security disciplines under the guidance and direction of the Wing's Chief, Information Protection.

1.5.2.1. **(Added-AFMC)** For Centers with GSUs located at other Center and/or MAJCOM locations, the Center CIP is responsible for developing and formalizing organizational responsibility for guidance, direction, and oversight of GSU security manager programs. This could include support from host Wing IP offices, Center IP office, or another IP office and will be defined in host tenant support agreements, MOU, MOA, or Center supplement in accordance with AFI 25-201. The intent is to ensure each unit security manager program is provided support and oversight on a consistent and continual basis as outlined in this instruction. **(T-2).**

1.6. Air Force Information Security. Is a core security discipline within Information Protection that is designed to identify and protect classified national security information and CUI in accordance with DoD policy issuances. DoDM 5200.01, Volumes 1-4, DoDI 5210.02, DoDD 5210.50, DoDI 5210.83, and DoDM 5200.45 provide the foundational guidance and this AFI clarifies responsibilities within these DoD governances where needed.

1.6.1. The Air Force standard guidance for marking collateral classified information is DoDM 5200.01, Volume 2, *Marking of Classified Information*. Personnel assigned to Special Access Program (SAP) and Sensitive Compartment Information (SCI) will follow additional guidance as mandated by their security officials. The standard for marking CUI (e.g., For Official Use Only (FOUO)) is DoDM 5200.01, Volume 4, *Controlled Unclassified Information (CUI)*.

1.6.2. Submit requests for clarification through information protection channels to SAF/AAZ when conflicts between this publication and DoD guidance occur. (T-1)

1.6.2. **(AFMC)** In the event of conflicts between this supplement, AF, and DoD guidance, submit requests for clarification through IP channels to HQ AFMC/IP. IP channels are defined as Wing CIP to Center CIP to HQ AFMC/IP; HQ AFMC/IP will interface with SAF/AAZ. **(T-2).**

1.6.3. Headquarters AFOTEC Information Protection maintains Information Protection oversight of all assigned AFOTEC headquarters agencies and geographically separated units. (T-1)

1.7. Other Roles and Responsibilities. Several Air Force organizations have responsibilities in implementing the Air Force Information Security Program.

1.7.1. The Deputy Under Secretary of the Air Force, International Affairs (SAF/IA) serves as the senior official responsible for directing, administering, and overseeing the Air Force Information Security Program pertaining to Foreign Government Information (FGI), the disclosure of classified information and CUI to foreign governments and international organizations, and security arrangements for international programs.

1.7.1. **(AFMC)** AFLCMC/WFNJ, Foreign Disclosure Office, is the AFMC responsible office.

1.7.2. The Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1) ensures civilian and military performance rating/appraisal systems includes the designation and management of classified information as a critical element or item to be evaluated in accordance with DoDM 5200.01, Volume 1.

1.7.2. **(AFMC)** HQ AFMC/A1 is the AFMC responsible office.

1.7.3. The Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2) serves as the Air Force Head of the Intelligence Community Element (HICE) and is the authority for all actions regarding the security, use, and dissemination of SCI.

1.7.3. **(AFMC)** HQ AFMC/A2 is the AFMC responsible office.

1.7.4. The Deputy Chief of Staff, Logistics, Installations and Mission Support (AF/A4) serves as the Air Force unclassified controlled nuclear information (UCNI) reviewing official.

1.7.4. **(AFMC)** HQ AFMC/A4 is the AFMC responsible office.

1.7.5. The Assistant Chief of Staff, Strategic Deterrence & Nuclear Integration (AF/A10) provides subject matter expertise for information security issues related to Nuclear Weapons Data (NWD).

1.7.5. **(AFMC)** HQ AFMC/A10 is the AFMC responsible office.

1.7.6. SAF/CIO A6 ensures Information Systems Security Officials execute duties in accordance with DoDM 5200.01, Volume 1, Enclosure 2.

1.7.6. **(AFMC)** HQ AFMC/A6 is the AFMC responsible office.

1.7.7. The Director, Information Management (SAF/AAI) serves as the focal point for the management of declassification programs to include Automatic, Systematic, Scheduled, and Mandatory Declassification Review (MDR).

1.7.7. **(AFMC)** HQ AFMC/IP is the AFMC responsible office.

1.7.7.1. Establishes the Air Force declassification program IAW DoDM 5200.01, Volume 1, Enclosure 5 and develops declassification training. See **Chapters 3** and 6 for details.

1.7.7.2. Establishes the Mandatory Declassification Review (MDR) Program for the Air Force. See **Chapter 3** for additional details.

1.7.7.3. Provides data for completion of the Agency Security Classification Management Program Data, Agency Annual Self-Inspection Program Data, and Office of the Assistant to the Secretary of Defense reports.

1.7.7.4. Establishes Air Force criteria to evaluate declassification programs and assists with completing the Agency Self-Inspection Report.

1.7.8. The Commander, Headquarters United States Air Forces in Europe (USAFE) serves as the Air Force Executive Agent (EA) for the North Atlantic Treaty Organization (NATO) Safeguarding Program. The USAFE Director, Information Protection represents the Air Force at NATO meetings and interagency forums, and forwards requests to establish and disestablish AF sub-registries to the Central United States Registry (CUSR).

1.7.8. **(AFMC)** HQ AFMC/IP provides AFMC policy, support, and guidance to the AFMC NATO Safeguarding Program.

1.7.9. **(Added-AFMC)** HQ AFMC/A5/8Z, Special Access Program Management Office, provides AFMC SAP policy, support, and guidance.

1.7.10. **(Added-AFMC)** HQ AFMC/A5RL is responsible for the AFMC Trusted Systems and Network (TSN) and Critical Program Information (CPI) Protection programs.

Chapter 2

AIR FORCE INFORMATION SECURITY IMPLEMENTATION

2.1. Security Program Executives (SPE). Uses the core security disciplines within Information Protection and any other program's processes (e.g., COMSEC, OPSEC, FDO, FOIA, PA, etc.) to identify, promote information sharing, facilitate judicious use of resources, and simplify management of, employ, maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting; and mitigate the adverse effects of unauthorized access or disclosure, compromise or loss by investigating and acting upon reports of security violation involving classified information and CUI for the command.

2.1.1. Designate a Restricted Data Management Official if the command creates, stores, or handles Restricted Data (RD), Formerly Restricted Data (FRD), Critical Nuclear Weapons Design Information (CNWDI), or Department of Energy (DOE) Sigma information.

2.1.1. **(AFMC)** HQ AFMC/IP is the AFMC Restricted Data Management Official.

2.1.2. Designate a NATO subregistry officer in accordance with United States Authority, North Atlantic Treaty Organization (NATO) (USSAN) 1-07 and DoDM 5200.01, Volume 1, Enclosure 2, if the MAJCOM/DRU creates, store or process NATO information.

2.1.2. **(AFMC)** 88 CS/SCOKMI operates/manages the AFMC NATO Sub-registry.

2.1.2. **(WRIGHTPATTERSONAFB)** AFIMSC, Det 6 maintains the Wright-Patterson AFB NATO subregistry.

2.1.3. Validate Original Classification Authority (OCA) designations annually, upon request.

2.1.3.1. OCAs that manage a security classification or declassification guide will maintain their authority until the security classification/declassification guide is terminated.

2.1.3.2. OCAs that do not manage or provide oversight of a security classification guide are validated by using the general rule standard in DoDM 5200.01, Volume 1, Enclosure 4.

2.1.4. Serve as the approval authority to allow command personnel to remove Secret and Confidential information from designated working areas for work at home in accordance with DoDM 5200.01, Volume 3, Enclosure 2.

2.1.4. **(AFMC)** Center CIP sends approval package through their Center/CV to HQ AFMC/IP.

2.1.5. Establish or leverage an existing forum to address issues related to the MAJCOM/DRU security enterprise and mission.

2.1.6. Ensure appropriate security measures to protect classified information stored on military assets such as aircraft, military platforms or classified munitions items not specifically addressed in **Chapter 5** of this AFI are adequately protected.

2.1.6.1. Coordinate with other MAJCOMs when in transit or deployed to support MAJCOM operational missions.

2.1.6.2. Address specific measures for aircraft in foreign countries where non-U.S. security support is provided.

2.1.7. Fully implement the MAJCOM/DRU MDR program by appointing primary and alternate MDR monitors in writing and submit the appointment to **usaf.pentagon.saf-aa.mbx.mdr-workflow@mail.mil** or mail to SAF/AAII, 1000 Air Force Pentagon, Washington DC, 20330-1000. Include the individual's Rank/Grade, Name, Unit/Office Symbol, Phone, E-mail, and Organizational Address.

2.1.7. **(AFMC)** HQ AFMC/IP will submit the primary and alternate AFMC MDR monitors.

2.1.8. Submit Senior Agency Self-Inspection and Agency Security Classification Management Program Data reports annually to SAF/AA in accordance with **Chapters 10** and 11 of this AFI.

2.2. MAJCOM/DRU Director, Information Protection . Coordinates the execution of Information Protection and collaborates with other security program managers (e.g., COMSEC, OPSEC, FDO, FOIA, PA, etc.) to identify, promote information sharing, facilitate judicious use of resources, and simplify management of, employ maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting; and mitigate the adverse effects of unauthorized access or disclosure, compromise or loss by investigating and acting upon reports of security violation involving classified information and CUI on behalf of the SPE.

2.2.1. Provide the SPE risk-based countermeasure strategies to assure mission protection and success.

2.2.2. Chair/participate in SPE designated forum to address Information Protection concerns.

2.2.3. Ensure supplements and self-assessment checklists are coordinated with SAF/AAZ prior to publishing and loading into the Management Internal Control Tool (MICT) database.

2.2.4. Ensure Information, Industrial, and Personnel Security Specialists assigned to the Information Protection Directorate are trained in accordance with **Chapter 6** of this AFI. This applies to any military personnel assigned to the directorate and managing the Information, Industrial, or Personnel Security Program.

2.2.5. Serve as a focal point for Security, Education, Training and Awareness (SETA) by appointing an individual in the Information Protection Office to interact with SAF/AAZ SETA Program Manager.

2.2.6. Develop and maintain security violations and infraction metrics and report them to SAF/AAZ when requested.

2.2.7. Provide guidance to Wing Chief, Information Protection.

2.2.7. **(AFMC)** Provide guidance to Center CIP.

2.2.8. Provide direction to staff Directors and Special Staff.

2.2.9. Prepares Senior Agency Self-Inspection and Agency Security Classification Management Program Data reports in accordance with **Chapters 10** and 11 of this AFI for the SPE.

2.2.10. Develop staff packages for approval of classified residential storage.

2.2.11. Coordinate with wings and perform staff assistance visits as required.

2.3. MAJCOM/DRU Information Security Specialist.

2.3.1. Analyze security violations and infractions to determine security impact on protecting classified information and CUI.

2.3.2. Determine training requirements for Top Secret Control Officers (TSCO), if mandated.

2.3.2. **(AFMC)** The use of TSCOs and TS accountability is mandated within AFMC. See paragraph 5.4 for accountability requirements. **(T-2).**

2.3.3. Coordinate security requirements with other commands to assure protection of classified information aboard aircraft and other military platforms.

2.3.4. Collect and maintain metrics for security violations and infractions.

2.3.5. Participate in development of risk-based countermeasure strategies to assure mission protection and success, as requested.

2.3.6. Provide oversight of the security incident inquiry/investigation process.

2.3.7. Identify security education and training requirements and communicates these requirements to the SAF/AAZ Information Protection Program SETA representative.

2.3.8. Provide documentation of OCA initial and refresher training, when requested.

2.3.9. Coordinate on security classification guides, instructions, and other program related guidance resources.

2.4. Wing Commanders. Uses the core security disciplines within Information Protection and coordinates with other program managers (e.g., COMSEC, OPSEC, etc.) to identify, promote information sharing, facilitate judicious use of resources, and simplify management of, employ maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting; and mitigate the adverse effects of unauthorized access or disclosure, compromise or loss by investigating and acting upon reports of security violations involving classified information and CUI for the wing.

2.4. (AFMC) Wing Commanders. These duties are also performed by the Center/CV at the Center level. Replace "Wing" with "Center" for the Center/CV duties unless otherwise stated. The Center/CV is responsible for determining and/or deconflicting Center and Wing roles and responsibilities as outlined in this section and throughout this instruction. **(T-2).**

2.4.1. Designate a Restricted Data Management Official if the wing creates, stores, or handles RD, FRD, CNWDI, or DOE Sigma information. (T-1)

2.4.2. Appoint a NATO Control Point Officer if the wing processes or stores NATO information. Request the establishment of a control point through your servicing NATO Subregistry. (T-1) Multiple NATO control points could be established depending on the volume of NATO information the wing processes.

2.4.2. **(AFMC)** A NATO Control Point can be established at the Center, Wing , or Center and Wing level depending on the organizations needing access to NATO information.

2.4.3. When needed, make security-in-depth and supplemental control determinations, in accordance with **Chapter 5** of this AFI. (T-1)

2.4.4. Establish 1 day each year with specific attention and effort focused on disposing of unneeded classified material (clean-out day). (T-0)

2.4.4. **(WRIGHTPATTERSONAFB)** The second Friday of March is the designated, annual clean-out day for all organizations on WPAFB.

2.4.5. Reviews Wing's annual self-inspection report and security classification management program data reports and submits results to the SPE. (T-1)

2.4.6. Ensure Chief, Information Protection is assigned as a member of the Wing's Integrated Defense Council. (T-1)

2.4.6. **(AFMC)** Wing/CC/CV may assign the Wing CIP to an existing Wing risk management forum or establish a new forum to discuss Security Enterprise issues.

2.4.6.1. **(Added-AFMC)** Center/CV's may assign the Center CIP to an existing Center risk management forum or establish a new forum to discuss Security Enterprise issues.

2.4.7. Approve and recertify open storage rooms/areas, as required. (T-1)

2.4.7. **(AFMC)** Vaults/secure rooms previously approved by the Wing CIP don't need to be recertified and approved by the Wing Commander unless the room vault/secure room does not meet the security requirements of DoDM 5200.01 or there is a change/modification to the vault/secure room.

2.5. Wing Chief, Information Protection. Coordinates the execution of Information Protection and any other program's processes (e.g., COMSEC, OPSEC, etc.) to identify, promote information sharing, facilitate judicious use of resources, and simplify management of, employ maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting; and mitigate the adverse effects of unauthorized access or disclosure, compromise or loss by investigating and acting upon reports of security violation involving classified information and CUI on behalf of the Wing/CV.

2.5. (AFMC) Wing Chief, Information Protection. These duties are also performed by the Center CIP at the Center level. Replace "Wing" with "Center" for the Center CIP duties unless otherwise stated.

2.5.1. Ensures the Information, Industrial, and Personnel Security Specialists are trained IAW DoDM 5200.01, Volume 3, Enclosure 5. (T-0) **Chapter 6** of this AFI provides options for meeting this requirement.

2.5.2. Conducts staff assistance visits, when requested. (T-1)

2.5.3. Provides guidance, direction, coordination, and oversight to commanders, directors, security managers, TSCOs, and others in security management roles as necessary. (T-1) Ensure they are kept abreast of changes in policies and procedures. (T-0)

2.5.3. **(AFMC)** Ensures commanders or directors are aware of their responsibilities explained within this AFI. **(T-2).**

2.5.4. Conducts annual self-inspection on major areas identified in DoDM 5200.01, Volume 1, Enclosure 2 and **Chapter 10** of this AFI. (T-1)

2.5.5. Writes a wing instruction or leverage another directive that applies to all wing personnel, (T-1) which includes:

2.5.5. **(AFMC)** A Center instruction can replace the requirement for a Wing instruction, if all requirements are met.

2.5.5.1. Provisions for safeguarding classified information during emergency situations and military operations, if appropriate. (T-0)

2.5.5.2. Security measures and procedures regarding visitors who require access to classified information or facilities that contain classified information. (T-0)

2.5.5.3. Identification of a classified storage location for personnel arriving unexpectedly or while in transit and in possession of classified information. (T-1)

2.5.6. Assists commanders and directors with solving information security related issues.

2.5.7. Provides countermeasure strategies to assure mission protection.

2.5.8. Develops approval/recertification packages for open storage areas/secure rooms. (T-1) Ensure the package includes a statement the room meets construction standards. (T-1)

2.5.8.1. Recommend coordinating with the local civil engineers and request an assessment of the construction standards.

2.5.8.2. Consider contacting the Wing Information Assurance Office.

2.5.8.3. Consult with parent unit when a new facility design may contain open storage rooms.

2.5.9. Prepares Senior Agency Self-Inspection and Agency Security Classification Management Program Data reports for Wing/CC in accordance with **Chapters 10** and 11 of this AFI and processes them through Information Protection channels to MAJCOM/DRU Director, Information Protection. (T-1)

2.5.9. **(AFMC)** Center CIP will consolidate their Wing's annual Senior Agency Self-Inspection and Agency Security Classification Management Program Data reports into one Center report, obtain Center/CV's signature, and submits results to HQ AFMC/IP. **(T-2).**

2.5.10. Participates as a member of the Wing's Integrated Defense Council. (T-1) This may be delegated to a member of the Information Protection Office.

2.5.10. **(AFMC)** Or participates as a member of the forum established to discuss Security Enterprise issues, depending on the Wing/CC/CV's direction.

2.5.10.1. **(Added-AFMC)** Center CIPs may participate as members of the forum established to discuss Security Enterprise issues, depending on the Center/CV's direction.

2.5.11. **(Added-AFMC)** Center CIPs will submit security incident data to HQ AFMC/IP by the 10th of each month. **(T-2).**

2.5.12. **(Added-AFMC)** Conduct security manager meetings no less than semi-annually. **(T-2).**

2.5.13. **(Added-AFMC)** Center CIP determines who with review Foreign Military Sales Security/Transportation Plans concerning movement and/or transfer of classified material/information for adequacy of security arrangements.

2.6. Wing Information Security Specialist.

2.6. (AFMC) Wing Information Security Specialist. These duties are also performed by the Center Information Security Specialists at the Center level. Replace "Wing" with "Center" for the Center Information Security Specialists duties unless otherwise stated.

2.6.1. Maintains records of OCA initial and annual training, if OCAs are assigned. Submit the documentation when requested. (T-1)

2.6.1. **(AFMC)** Records can be maintained at either the Center or Wing level, they don't need to be maintained at both levels.

2.6.2. Provides guidance and direction to commanders and directors or designated security manager when requested on all aspects of the Air Force Information Security Program. (T-1)

2.6.3. Provides oversight of the security incident inquiry/investigation process to include establishing a central tracking system. (T-1)

2.6.4. Analyzes security violations and infractions to determine security impact. (T-1)

2.6.5. Provides technical guidance and advice to commanders/directors for conducting information security risk assessments in accordance with DoDM 5200.01, Volume 3, Enclosure 3. (T-1)

2.6.5. **(AFMC)** Recommends utilizing risk assessments already complete for the wing/installation, such as for the Anti-Terrorism program and Threat Working Group.

2.6.6. Trains security managers on their duties and responsibilities in accordance with **Chapter 6** of this AFI. (T-1)

2.6.6. **(AFMC)** Trains TSCOs. **(T-2).**

2.6.7. Coordinate on security classification and declassification guides, Air Force instructions, and other program related guidance resources as needed. (T-1)

2.6.8. Advises commanders on types of emergency plans to develop based on local threats of hostile actions, foreign intelligence, natural disasters, or terrorist activity. (T-1)

2.6.9. Provides OCAs and derivative classifiers guidance, direction, and oversight for marking classified information and CUI. (T-1)

2.6.10. Validates construction standards, with assistance from the Wing Civil Engineer if needed, for open storage area (secure room) and vaults, and recommends supplemental safeguarding standards, based on a risk assessment, to commanders and directors prior to approval. (T-1)

2.6.10. **(AFMC)** Recommends utilizing risk assessments already complete for the wing/installation, such as for the Anti-Terrorism program and Threat Working Group.

2.6.11. Provides commanders and directors assistance in developing exception to policy staff packages to deviate from protection standards identified in DoDM 5200.01. (T-1)

2.6.11. **(AFMC)** Exceptions to policy staff packages will flow from commanders and directors to their servicing CIP, through the Center CIP who will submit packages through their Center/CV to HQ AFMC/IP. HQ AFMC/IP will submit the request through AFMC/CV to SAF/AAZ. **(T-2).**

2.6.12. Integrate on-base contractor operations into the installation's Information Security Program. (T-1)

2.6.13. Coordinate with Wing Information Assurance Office to ensure full integration of information technology requirements to include: access, security, and response action to security incidents involving classified information and CUI on IT systems. (T-1)

2.6.14. Assist Chief, Information Protection with annual self-inspection.

2.7. Commanders and Directors.

2.7. (AFMC) Commanders and Directors. Commanders and directors perform these duties at all locations under their command to include geographically separated units (GSU). If authorized, commanders and directors may delegate these duties at GSUs to the GSU's lead position (e.g., Division, Branch Chiefs). **(T-2).**

2.7.1. Appoint a Security Manager in accordance with DoDM 5200.01, Volume 1, Enclosure 2, and ensure they are trained IAW DoDM 5200.01, Volume 3, Enclosure 5 within 6 months of appointment. (T-0) Contractors and personnel assigned to the Information Protection Directorate/Office cannot be appointed to serve in this role. Forward the appointment to the Wing Information Protection Office. (T-1)

2.7.1. **(AFMC)** Current Security Managers, from the date of this supplement, that do not meet the grade requirements of DoDM 5200.01, Volume 1, Enclosure 2, may continue to fulfill the security manager role. Security Managers appointed after the date of this supplement will need to meet grade requirements.

2.7.1.1. Security managers may be appointed to serve combined populations of smaller units, groups, and staff agencies rather than multiple units appointing a security manager. For example, a group may appoint a security manager to oversee all the assigned squadrons within the group and the squadrons appoint security assistants to perform administrative functions.

2.7.1.1. **(AFMC)** Security managers will be appointed at organizations GSUs. **(T-2).**

2.7.1.2. If assistant security managers are appointed, train to the same standard as the security managers. (T-0)

2.7.1.2. **(AFMC)** Organizations that generate, process or store classified material will appoint an assistant security manager. Organizations with small amounts of classified material, may appoint a security assistant instead of an assistant security manager. **(T-2).**

2.7.1.2. **(WRIGHTPATTERSONAFB)** In addition to a primary security manager, all activities will appoint an alternate security manager. The alternate security manager will be trained and involved in the unit's program to fulfill duties in the primary's absence. Submit written appointment of primary and alternate security managers to 88 ABW/IP on WPAFB Form 1404, *SM Appointment Record,* or a memorandum including the equivalent information as the WPAFB Form 1404.

2.7.1.3. Security Assistants may be appointed to assist the security manager with performing administrative tasks such as processing forms for access or security clearances, documenting security education and training and validating security clearances. Appointments must be in writing and in accordance with DoDM 5200.01,

Volume 1, Enclosure 3, and they must be trained within 6 months of assuming duties. (T-0)

2.7.1.3. **(WRIGHTPATTERSONAFB)** When deemed necessary, appoint security assistants to assist the security manager. Security assistant duties and methods for disseminating information will be defined in the organization's security operating instruction. Security managers will maintain appointment records for security assistants.

2.7.2. Grant personnel access to classified information and continually evaluate their trustworthiness in accordance with DoDM 5200.01, Volume 1, Enclosure 2, and AFI 31-501 (CHANGING TO AFI 16-1405)), *Personnel Security Program Management*, and **Chapters 5**, 8, and 9 of this AFI. (T-0) This may not be delegated. (T-0) Ensure all collateral access is reflected in the security access requirement (SAR) level shown on the unit manning document. Consider suspension of an individual's access whenever their trustworthiness, loyalty, or honesty becomes questionable in accordance with AFI 31-501 (CHANGING TO AFI 16-1405). (T-1)

2.7.3. Implement an ongoing security education and training program which includes all elements detailed in **Chapter 6** for initial and annual refresher training. (T-1)

2.7.4. Identify personnel whose duties require derivative classification and ensure they are trained IAW DoDM 5200.01, Volume 3, Enclosure 5. (T-0) **Chapter 6** of this AFI identifies options to meet this requirement. As a minimum, persons with access to classified information systems will be identified. (T-1) Ensure training records are maintained by the individual or develop a system for maintaining the records. (T-1)

2.7.4.1. Instruct derivative classifiers to document derivative classification decisions to support the annual security classification management program data collection effort when requested. (T-1)

2.7.5. Evaluate security incidents to determine appropriate measures to be taken to prevent further occurrences and if sanctions should be administered. (T-1)

2.7.6. Identify areas within the unit where classified information is discussed or processed. (T-1) If the area contains information systems, communications systems, or cryptographic equipment contact the wing Information Assurance (IA) office to conduct an Emission Security assessment of the areas prior to processing classified information. (T-1) If this assessment has not been completed prior to the publication of this AFI the wing IA office must be contacted within 6 months of the date of this AFI to schedule assessments. (T-1)

2.7.6.1. Areas such as open storage rooms, offices with secure telephone equipment (STE), conference rooms, and etc. are examples. Do not restrict the list to just these areas or types of equipment.

2.7.7. Develop a unit security plan/instruction to: (T-1)

2.7.7. **(AFMC)** Include GSUs in the unit's security plan/instruction or develop a separate security plan/instruction specifically for the GSU. **(T-2).**

2.7.7.1. Protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action based on the threats/risks of these incidents occurring. (T-0) Refer to DoDM 5200.01, Volume 3, Enclosure 2, and Wing Information Protection Office for guidance on developing the plan.

2.7.7.2. Prohibit the use of government or personal cellular/PCS and or radio frequency (RF), infrared (IR) wireless devices, and other devices such as cell phones and tablets, and devices that have photographic or audio recording capabilities in areas identified in paragraph 2.7.6 of this AFI in accordance with DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)* unless written approval has been received by the Authorization Official, formerly called Designated Approving Authority. (T-0) Items listed in paragraph 2.5 of DoD 8100.02 are exempt.

2.7.7.3. Address security incidents when Government and personal cellular/PCS, RF wireless, and similar devices are discovered in Air Force-controlled classified areas. (T-1) Refer to **Chapter 5** of this AFI for additional information on processing these types of security incidents.

2.7.8. Establish a system to conduct end of day security checks using SF 701, *Activity Security Checklist*, at the close of each duty and/or business day to ensure classified information is secure within unit work centers. (T-1) This is not required for 24/7 work centers.

2.7.8. **(AFMC)** Use the SF 702, Security Container Check Sheet, "Checked By" column to verify the security status of containers, vaults and secure storage rooms during the end-of-day security check for each duty and/or business day. Annotate it whether or not they were opened during the day. This is not required for 24/7 work centers. **(T-2).**

2.7.8. **(WRIGHTPATTERSONAFB)** End-of-Day Security Checks. The unit's security operating instruction, signed by the unit commander/director, will include procedures for conducting end-of-day security checks.

2.7.9. Identify features, parts or functions of equipment used to process classified information that may retain all or part of the information. (T-0) Once identified develop security procedures to address safeguarding measures. (T-0) Refer to DoDM 5200.01, Volume 3, Enclosure 2, for guidance on what to address.

2.7.10. Will approve and address procedures for equipment used for reproducing Top Secret, Secret and Confidential information and if applicable, ensure the system is accredited. (T-1) The approval must facilitate oversight and control of the reproduction of classified information and the use of the equipment for such reproduction. (T-1) Prior to approval review DoDM 5200.01, Volume 3, Enclosure 2, for addition guidance. Coordinate with Wing Information Assurance to ensure accreditation requirements are identified and addressed or verified as not necessary, if device will be networked to a government IS. (T-1)

2.7.10. **(WRIGHTPATTERSONAFB)** Post WPAFBVA 31-9, *Caution: Authorized for Reproduction of Classified Material*, or equivalent visual aid, on or clearly visible above copiers, facsimiles, microfiche machines or any other machines capable of and approved for reproduction of classified material. Post WPAFBVA 31-10, *STOP Do Not Use This Machine for Classified Reproduction*, or equivalent visual aid, on or clearly visible above all other machines used for reproduction of unclassified material. Security managers must engage their unit cyber-security liaison (CSL) and copier vendor prior to utilizing a copier to reproduce classified information. Specifically, procedures to clear the memory and hard drives (if applicable) must be attained, documented, and included in posted classified

copying procedures. Post WPAFB Form 1414, *Stored Information Notice*, on or clearly visible above all copiers, multifunctional devices, scanners, and facsimiles or any other machine capable of processing and storing controlled unclassified information. Security managers must engage their unit CSL, operations security coordinator, and office equipment vendor prior to having any data storage capable office equipment maintained/serviced, prior to allowing a data storage capable device to leave the unit, and prior to decommissioning and/or turn-in. Specific procedures to clear the equipment's memory and/or hard drives must be obtained and documented.

2.7.11. Establish a process to ensure the names of the people having knowledge of combinations to security containers, open storage rooms, and vaults are maintained on a list and combinations are changed in accordance with DoDM 5200.01, Volume 3, Enclosure 3. (T-0)

2.7.12. Contact the Wing Information Protection Office to establish a secure room or a vault, and assist with risk assessment, if needed. (T-1) This includes new facility designs that may require secure rooms. (T-1) Do not use rooms until they are approved. (T-1)

2.7.12. **(WRIGHTPATTERSONAFB)** Appropriately-constructed secure conference facilities (those meeting the sound standards referenced in ICD 705, **Chapter 9** and constructed IAW DODM 5200.01, Volume 3, Enclosure 3) provide protection for classified discussions without further compensatory measures; coordinate construction and testing requirements for such facilities with 88 ABW/IP. Upon approval of the secure conference facility by 88 ABW/CV, 88 ABW/IP will issue a letter of certification on WPAFB Form 1475, *Classified Storage/Conference Room Certification*. 88 ABW/IP must be notified before any modification to the room or facility. Modification includes any construction modifications, alarm modifications, penetration of walls, changes in equipment, etc. 88 ABW/CE will use DODM 5200.01, Volume 3, Enclosure 3, Appendix, *Physical Security Standards*, for any new secure room construction standards.

2.7.13. Approve classified meetings and conferences. Ensure:

2.7.13.1. An official has been designated as a security manager for the meeting if the organization's security manager does not perform these duties. (T-0) This individual implements the security provisions established in DoDM 5200.01, Volume 3, Enclosure 2. See Attachment 4, Classified Meeting/Briefing/Conference Checklist, for quick reference.

2.7.13.1. **(WRIGHTPATTERSONAFB)** For classified meetings and conferences that will not be held in an approved open-discussion area coordinate security plans with 88 ABW/IP at least 10 working days before the start of the event. The hosting activity is responsible for all actions associated with conducting a classified meeting on base. A hosting official will coordinate security requirements through the activity's security manager. The hosting official will establish entry control and, when necessary, obtain perimeter area surveillance by posting personnel from the hosting activity. (**NOTE:** Local security forces personnel do not provide this function.) The hosting official will instruct individuals to remove electronic devices such as pagers, cell phones, and Blackberries prior to entry.

2.7.13.2. Meetings or conferences, or classified sessions thereof, do not take place outside a U.S. Government facility or a cleared U.S. contractor facility with an appropriate facility security clearance unless an exception is approved in advanced by SAF/AA. (T-0)

2.7.13.2.1. Submit exception requests to SAF/AAZ and include a security plan in accordance with DoDM 5200.01, Volume 3, Enclosure 2 through Information Protection Program channels. (T-1)

2.7.13.2.1. **(AFMC)** Center CIPs will submit exception request to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit the exception request through AFMC/CV to SAF/AAZ. **(T-2).**

2.7.13.2.2. Submitted an after-action report to SAF/AAZ within 90 days following the conclusion of the meeting or conference through information protection channels. (T-0)

2.7.13.2.2. **(AFMC)** Servicing CIPs will submit after-action report to HQ AFMC/IP through their Center CIP. HQ AFMC/IP will submit the after-action report to SAF/AAZ. **(T-2).**

2.7.14. If an area hosts special access program activities, a corresponding site-specific treaty inspection readiness plan that includes detailed managed access provisions in accordance with AFI 16-701, *Management, Administration and Oversight of Special Access Programs,* is needed.

2.7.15. Take corrective actions to address areas identified by the Wing Information Protection Office self-inspection report. (T-1)

2.7.16. **(Added-AFMC)** Establish a Top Secret Control Account when the organization originates, stores, receives, or dispatches Top Secret material and designate a TSCO, with one or more alternates, to maintain it. See paragraph 5.4 for Top Secret accountability requirements. **(T-2).**

2.8. Security Managers . Manages and implements one or more of the Information Protection core security disciplines (information, industrial, or personnel security) on behalf of their Commander or Director. These duties may be tailored to meet the organizational needs, but as a minimum must address the items listed below.

2.8.1. Complete training requirements IAW DoDM 5200.01, Volume 3, Enclosure 5 within 6 months of assuming duties. (T-0) **Chapter 6** of this AFI list options for compliance with this item.

2.8.1. **(WRIGHTPATTERSONAFB)** Security managers and alternate security managers must attend security manager training provided by 88 ABW/IP.

2.8.2. Train security assistants within 6 months of assuming duties. (T-0) The Wing Information Protection can assist with development of the training prior to execution.

2.8.2. **(WRIGHTPATTERSONAFB)** Security managers will train security assistants on their specific duties within 2 months of appointment.

2.8.3. Ensure initial orientation and refresher training is conducted for all cleared and uncleared personnel IAW DoDM 5200.01, Volume 3, Enclosure 5. See **Chapter 6** of this AFI for addition guidance.

2.8.4. Notify Wing Information Protect Office of security incidents and coordinate actions. (T-1)

2.8.5. Notify the Wing Information Protection Office when areas/rooms are considered for open storage/secure room/vault or when new facility designs contain plans for these areas. (T-1)

2.8.5. **(WRIGHTPATTERSONAFB)** 88 ABW/CV is the approval authority for collateral classified open storage areas. The requesting activity will contact 88 ABW/IP to inspect the facility for construction compliance and standards, including written standard operating procedures. WPAFB Form 1475, *Classified Storage/Conference Room Certification*, will be posted inside the entry door. 88 ABW/IP must be notified before any modifications to the room or facility.

2.8.6. Update assigned personnel accesses in JPAS. (T-1) Monitor and act on JPAS notifications. (T-1) Use JPAS to in-process and out-process all unit personnel. (T-1)

2.8.7. **(Added-AFMC)** Attend servicing CIP hosted security manager meetings. **(T-2).**

2.8.7. **(WRIGHTPATTERSONAFB)** Security Managers Meeting. At least one Security Manager representative from each organization must attend; if the security manager is not availalble another representative from the organization will attend in his/her absence.

2.8.8. **(Added-WRIGHTPATTERSONAFB)** Establish a security manager's handbook and maintain pertinent program records. The handbook and records can be either in electronic or physical form. At a minimum, the handbook will include:

2.8.8.1. **(Added-WRIGHTPATTERSONAFB)** Security manager, alternate security manager, and security assistant appointment records.

2.8.8.2. **(Added-WRIGHTPATTERSONAFB)** Security manager and alternate security manager training certificates.

2.8.8.3. **(Added-WRIGHTPATTERSONAFB)** Unit security operating instruction.

2.8.8.4. **(Added-WRIGHTPATTERSONAFB)** Most recently completed unit IP self-assessment checklists.

2.8.8.5. **(Added-WRIGHTPATTERSONAFB)** Most recent Information Protection Security Review (IPSR) report and corrective actions taken.

2.8.8.6. **(Added-WRIGHTPATTERSONAFB)** SF 311, *Agency Information Security Program Data*, for the current and previous fiscal year.

2.8.8.7. **(Added-WRIGHTPATTERSONAFB)** A list of security containers (i.e. vaults, safes, secure rooms, and secure classified discussion areas) within the organization (including: make, container ID#, lock type, location, primary and alternate custodian, and last operational visual inspection date).

2.8.8.8. **(Added-WRIGHTPATTERSONAFB)** Training documentation with date and material presented (initial and recurring).

2.8.8.9. **(Added-WRIGHTPATTERSONAFB)** Miscellaneous items. (e.g., Position Code Review).

2.8.9. **(Added-WRIGHTPATTERSONAFB)** Implement and manage the organization's Industrial Security Program IAW AFI 16-1406, *Air Force Industrial Security Program*.

2.8.10. **(Added-WRIGHTPATTERSONAFB)** Implement and manage the organization's Personnel Security Program IAW AFI 31-501, *Personnel Security Program Management,* (changing to AFI 16-1405).

Chapter 3

CLASSIFICATION, DECLASSIFICATION, AND MANDATORY DECLASSIFICATION REVIEW (MDR) PROGRAM

3.1. Classification . There are three types of classification: Original, Tentative, and Derivative. DoDM 5200.01, Volume 1, Enclosure 4 is the foundational guidance for Original, Tentative, and Derivative Classification.

3.2. Original Classification. The SECAF delegates Top Secret original classification authority (OCA) to Air Force officials. SAF/AA may delegate Secret and Confidential OCA.

3.2.1. No other Air Force OCA has delegation or designation authority.

3.2.2. SAF/AAZ maintains the Air Force list of all OCA delegations by position and level of authority.

3.2.3. Prior to submitting a request for OCA the MAJCOM/DRU SPE or SAF/HAF Director considers:

3.2.3.1. Can the need be met through issuance of security classification guides by an existing OCA in the chain of command?

3.2.3.2. Is referral of the decision impractical for reasons such as geographical separation?

3.2.3.3. Is there sufficient expertise and information available to the prospective OCA to permit effective classification decision-making?

3.2.4. Submit request for OCA through established Information Protection channels to SAF/AAZ. (T-1) Include in the request:

3.2.4. **(AFMC)** Center CIPs will submit OCA requests to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit the request through AFMC/CV to SAF/AAZ. **(T-2).**

3.2.4.1. Position title. (T-1)

3.2.4.2. Brief mission-specific justification. (T-1)

3.2.4.3. A need statement (T-1) indicating one of the following:

3.2.4.3.1. The position will have oversight of a security classification guide(s). (T-0)

3.2.4.3.2. The position will exercise their authority at least twice a year. (T-0)

3.2.5. Before exercising OCA duties and annually thereafter the OCA:

3.2.5.1. Receive training from the Wing Information Protection Office. (T-1)

3.2.5.1. **(AFMC)** Training may be accomplished by the Center IP Office.

3.2.5.2. Certify in writing that they have received training in the areas specified in DoDM 5200.01, Volume 1, Enclosure 4.

3.2.6. The Wing Information Protection Office will maintain OCA delegation letters and training certifications of assigned OCAs and will submit the delegation letters and training certifications when requested through Information Protection channels to SAF/AAZ. (T-1)

3.2.6. **(AFMC)** Records can be maintained at either the Center or Wing level.

3.2.7. OCAs issue security classification and declassification guidance, use approved methods for protecting classified and CUI, review security incidents for compromise, and conduct damage assessments when information is considered compromised.

3.2.7.1. Issue classification and declassification guidance as soon as practical in the life cycle of the system, plan, program, or project to ensure only information requiring protected is identified. OCAs may use memoranda and other communication media to issue classification guidance, but the preferred method is a security classification guide (SCG). Coordinate all classification guidance through the Wing Information Protection Office. This does not apply to SAP or SCI guides. Wing Information Protection Offices review the guides for proper formatting and ensure all classification marking are present. Regardless of the medium used, OCAs review their guidance once every 5 years IAW DoDM 5200.01, Volume 1, Enclosure 6. When making declassification decisions use:

3.2.7.1. **(AFMC)** Coordination of SCGs may be accomplished by the Center IP Office.

3.2.7.1.1. A date less than 10 years. If not, can it be declassified at the 10 year mark? Mark the Declassify On line with the date using YYYYMMDD format.

3.2.7.1.2. A date between 10 years, but less than 25 years. If not, can it be declassified at 25 years? Mark the Declassify On line with the date using YYYYMMDD format.

3.2.7.1.3. An event (e.g., upon completion of tests) used in conjunction with either 3.2.7.4.1. or 3.2.7.4.2. Mark the Declassify On line as: YYYYMMDD, Completion of Test, Whichever is later."

3.2.7.1.4. An exemption approved by the Interagency Security Classification Appeals Panel (ISCAP). The Air Force Declassification Office (AFDO) publishes and maintains the *Air Force Declassification Guide for Historical Records* approved exemption categories. If an exemption is not listed in this guide then a formal request to the ISCAP must be submitted through the AFDO following the guidance in DoDM 5200.01, Volume 1, Enclosure 5.

3.2.7.2. Use DoDM 5200.45, *Instructions for Developing Security Classification Guides* for completing the guide. Attachment 2, Security Classification and Declassification Guide Formatting, is the standard format for the Air Force. Ensure the guides are processed in accordance with DoDM 5200.01, Volume 1, Enclosure 6, and if distributing the guide ensure a copy is sent to SAF/AAI. See Attachment 3 for instructions on how to complete the DD Form 2024, *DoD Security Classification Guide Data Elements*.

3.2.7.3. Do not publish declassification guidance in Air Force publications. If an Air Force publication has already been issued to disseminate original classification guidance ensure:

3.2.7.3.1. It contains declassification instructions.

3.2.7.3.2. Has OCA classification authority block (see DoDM 5200.01, Volume 2, Figure 3. Example of Originally Classified Document) and is signed by the OCA or a supervisor within the OCAs chain of command with OCA at the appropriate level of classification.

3.2.7.4. Alternative compensatory control measures (ACCM) are not authorized for use in the Air Force.

3.2.7.5. When notified of a compromise of classified information take actions to verify the classification and duration of classification initially assigned to the information in accordance with DoDM 5200.01, Volume 3, Enclosure 6.

3.2.7.6. Conduct damage assessments in accordance with DoDM 5200.01, Volume 3, Enclosure 6. Damage assessments are undertaken to determine the effect of a compromise following a security incident that could lead to compromise when it cannot be determined if a compromised occurred.

3.2.7.6. **(AFMC)** OCAs provide a copy of damage assessments to their servicing CIP. **(T-2).**

3.2.8. OCAs provide data to support the Senior Agency Official (SAF/AA) annual reporting requirements to the Information Security Oversight Office identified in **Chapters 10** and 11 of this AFI.

3.3. Tentative Classification. A process used by individuals who submit information to an OCA for making classification decisions. Tentative classification answers the statements in the original classification process. Follow the guidance in the DoDM 5200.01, Volume 1, Enclosure 4, for instructions on tentative classification.

3.4. Derivative Classification. All Air Force personnel (military, civilian, and on-site contractors) with access to classified information systems are considered derivative classifiers and any other person designated by the commander or director. Derivative classifiers are responsible for all markings associated with the documents they create and may be subject to sanctions identified in DoDM 5200.01, Volume 1, Enclosure 3. (T-1) Derivative classifiers must:

3.4.1. Receive initial training and refresher training every 2 years. (T-0) Refer to **Chapter 6** of this AFI for requirements. Maintain copies of training records and provide them to the security manager, information protection office, or inspector general upon request. (T-1)

3.4.2. Follow the instructions in the security classification guide if there is a conflict between a SCG and other source document. (T-0)

3.4.3. Consult with an OCA, originator of the source document, or notify the Security Manager/Wing Information Protection Office when required markings are missing or omitted from a source document. (T-0)

3.5. Declassification and Changes in Classification . Declassification does not authorize release of information to the public. Refer DoDM 5200.01, Volume 1, Enclosure 5, prior to releasing any previously classified document or any of its pages to the public.

3.5.1. Top Secret, Secret, and Confidential information may be declassified or downgraded by an OCA with classification, program, or functional responsibility; supervisory officials of the OCA if appointed as an OCA, or by the AFDO.

3.5.2. Air Force OCAs, MDR officials and AFDO may not declassify RD and FRD.

3.5.2.1. Restricted Data (RD). Only the DOE may declassify RD.

3.5.2.2. Formerly Restricted Data (FRD). The DOE/DoD jointly declassifies FRD.

3.5.3. If an Air Force organization no longer exists:

3.5.3.1. The organization that inherited the function of the originating organization will determine appropriate declassification action.

3.5.3.2. If the functions of the originating organization were dispersed to more than one organization, it cannot be determined which organization should inherit the function, or the organizations ceased to exist, the AFDO works with the Senior Agency Official to determine the declassification action to be taken.

3.5.4. Prior to declassifying or downgrading information marked with a date or event on the "declassify on" line:

3.5.4.1. Confirm the OCA has not extended the classification period by reference to the applicable security classification or declassification guide or by consultation with the OCA.

3.5.4.2. Apply the appropriate declassification markings and who authorized the declassification. Refer to Figure 9 in DoDM 5200.01, Volume 2 for an example on how to apply declassification markings.

3.5.5. Refer to DoDM 5200.01, Volume 1, Enclosure 5, for declassifying of information marked with old declassification instructions.

3.5.6. Refer to DoDM 5200.01, Volume 1, Enclosure 5, for downgrading classified information.

3.5.7. Air Force Declassification Office (AFDO):

3.5.7.1. Ensure AFDO personnel receive training as specified in DoDM 5200.01, Volume 3, Enclosure 5, and **Chapter 6** of this AFI upon initial designation and every 2 years thereafter.

3.5.7.2. Reviews Air Force-originated records > 25 years old, subject to automatic declassification, and located at the National Archives at College Park, MD (Archives II). This also includes other-agency records at Archives II which contain Air Force equities.

3.5.7.3. Reviews Air Force-owned records stored at the Washington National Records Center in Suitland, MD.

3.5.7.4. Provides trained reviewers to the National Declassification Center at Archives II.

3.5.7.5. Prepares and maintains the *Air Force Declassification Guide for Historical Records*.

3.5.7.6. Assists with historical document classification reviews requested under the Freedom of Information Act (FOIA) or MDR processes, and with manuscript review, when requested.

3.5.7.7. Develops and conducts training in classification/declassification, equity recognition, nuclear weapons information protection, MDR, and classified FOIA review on a cost-reimbursable basis to requesting Air Force organizations.

3.5.7.8. Assists Air Force organizations and installations, and Federally Funded Research and Development Centers (FFRDCs), requesting classification review of records generated for Air Force use.

3.5.7.9. Conducts environmental archival research for the Air Force Legal Operations Agency to support environmental litigations.

3.5.7.10. Serves as the focal point for processing Air Force referrals.

3.5.7.11. Conducts staff assistance visits/quality control reviews within one year of an individual(s) completion of the AFDO Declassification Training and Certification Program.

3.5.8. SPEs, Commanders, Directors, and OCAs must designate in writing Air Force personnel (military and civilian) with responsibilities to exercise declassification authority and ensure they complete training IAW DoDM 5200.01, Volume 1, Enclosure 5 initially and every 2 years thereafter. (T-0) Refer to **Chapter 6** of this AFI for AFDO Training and Certification Program standards. Include the individual's name, unit address, phone number, and e-mail address in the designation memorandum. (T-1)

3.5.8.1. OCAs and Air Force military or civilian personnel that make recommendations to an OCA or designated declassification authority are exempt from this requirement.

3.5.8.2. Contractors are not authorized to be designated as declassification authorities, but may make recommendations to an OCA or designated declassification authority.

3.5.8.3. Submit designations through Information Protection channels to SAF/AAZ. SAF/AAZ forwards the designation to AFDO.

3.5.8.3. **(AFMC)** Center CIPs submit designations to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit through AFMC/CV to SAF/AAZ. **(T-2).**

3.5.8.4. AFDO contacts the individual and arranges training.

3.6. Mandatory Declassification Review (MDR) Program. A MDR is a provision that allows members of the public to request classified information in both document and electronic form to be reviewed for declassification. Refer to DoDM 5200.01, Volume 1, Enclosure 5, for additional guidance. In the event a HAF/SAF/MAJCOM/DRU or Wing receives an MDR, SAF/AAII will be notified immediately, but not later than the end of the next duty day.

3.6.1. SAF/AAII (MDR) is the OPR for MDR requests. SAF/AAII shall:

3.6.1.1. Determines if the request describes the document or material with enough specificity to allow the OPR to locate the records with a reasonable amount of effort. If not deny the request.

3.6.1.2. Provide written acknowledgement to the requester not later than 24 hours after receiving the request.

3.6.1.3. Ensure each request is logged into the SAF/AAII (MDR) database.

3.6.1.4. Control and process MDR requests until completed.

3.6.1.5. Refer requests to the appropriate Office of Primary Responsibility (OPR) for declassification determination. If the OCA/organization originating the classified

information no longer exists, the functions of the OCA/organization were dispersed to more than one organization, the inheriting OCA/organization cannot be determined, or the document is lacking markings to indicate what information is classified, then determine the declassification action to be taken on behalf of the senior agency official IAW DoDM 5200.01, Volume 1, Enclosure 5.

3.6.1.6. Establish procedures to assess and collect fees, approve or deny fee waivers, and notify requester in writing of possible MDR fees.

3.6.1.7. Send extension notices to requester.

3.6.1.8. Notify requester of the right of administrative appeal when information is denied in full or in part.

3.6.1.9. Prepare annual SF 311, *Agency Security Classification Management Program Data* report on behalf of SAF/AAI in accordance with **Chapter 11** of this AFI.

3.6.1.10. Make final determination on all "no records" responses.

3.6.1.11. Contact MAJCOM/DRU MDR monitors and schedule training within 15 days of receiving appointment letter. As a minimum the training will consist of determining equities or ownership of information contained in a document or electronic form.

3.6.2. MAJCOM/DRU MDR Monitors**.** Work closely with SAF/AAII (MDR) to ensure MDR requests are properly processed and meet timelines and serves as the liaison between the MAJCOM/DRU OPR and SAF/AAII (MDR).

3.6.2.1. Contact SAF/AAII (MDR) with 15 days of appointment to determine training requirements. Complete the requirements in accordance with SAF/AAII (MDR) process.

3.6.2.2. Determines MAJCOM/DRU OPR with equities and staffs request.

3.6.2.3. Processes the release or denial with SAF/AAII (MDR) office.

3.6.2.4. Submit requests for extensions 60 days prior to the 1-year date to SAF/AAII (MDR) at **usaf.pentagon.saf-aa.mbx.mdr-workflow@mail.mil** or 1000 Air Force Pentagon, Washington DC 30330-1000.

3.6.2.5. Respond to set timelines for interim updates on progress.

3.6.2.6. Notify SAF/AAII (MDR) when:

3.6.2.6.1. Extensions are required. Submit requests within 60 days of 1-year suspense to allow sufficient time to notify the individual or organization that submitted the request. The extensions maybe submitted sooner.

3.6.2.6.2. The requester is denied information.

3.6.2.6.3. External agency equities are involved to ensure proper coordination with the appropriate organization.

3.6.2.6.4. Unable to make a determination because the OCA/organization originating the classified information no longer exists, the functions of the originating OCA/organization were dispersed to more than one organization, inheriting OCA/organization cannot be determined, or the document is lacking markings to indicate what information is classified.

3.6.2.7. Upon receipt of the review from the OPR:

3.6.2.7.1. Use brackets to identify the classified information and cite the applicable exemption under paragraph 3.6.3.2 in the margins closest to the bracketed information.

3.6.2.7.2. Use brackets to identify the unclassified information not releasable under FOIA and cite the FOIA exemption (2-9) in the margins closets to the bracketed information. Refer to DoDM 5200.01, Volume 4, Enclosure 3, for a list of the exemptions and their definitions. Do not use Exemption 1 in this process.

3.6.3. Initial Denial Authority. The Initial Denial Authority is a reviewer who has authority to deny requested information. SAF/HAF Directors and MAJCOM/DRU SPE or Directors are Initial Denial Authorities. They may delegate this authority to O-6/GS-15 assigned to their organization. Upon receipt of a MDR request the Initial Denial Authority shall:

3.6.3.1. Review all classified and unclassified information submitted in the request and determine if:

3.6.3.1.1. Any of the classified information has been declassified.

3.6.3.1.2. Any of the unclassified information, including any classified information that can be declassified, falls under a FOIA exemption (2-9). See DoDM 5200.01, Volume 4, Enclosure 3, for a list of the exemptions and their definitions. Do not use Exemption 1 in this process.

3.6.3.1.3. Deny release of any information that remains classified or any declassified information that falls under one of the FOIA exemptions. Contact the FOIA office for additional guidance.

3.6.3.1.4. Approve release of all unclassified information not protected by a FOIA exemption. Contact the FOIA office for additional guidance.

3.6.3.1.5. Submit the review to the MDR Monitor. Include one or more of the exemptions identified in paragraph 3.6.3.2 below that apply for denial of classified information and one or more of the FOIA exemptions that apply to unclassified information.

3.6.3.2. Submit one of the exemptions below when denying classified information:

3.6.3.2.1. Reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.

3.6.3.2.2. Reveal information that would assist in the development, production, or use of weapons of mass destruction.

3.6.3.2.3. Reveal information that would impair U.S. cryptologic systems or activities.

3.6.3.2.4. Reveal information that would impair the application of state-of the-art technology within a U.S. weapon system.

3.6.3.2.5. Reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans.

3.6.3.2.6. Reveal information, including foreign government information that would cause serious harm to relations between the United States and a foreign government; or to ongoing diplomatic activities of the United States.

3.6.3.2.7. Reveal information that would impair the current ability of the United States Government officials to protect the President, Vice President, and others protected for whom protection services, in the interest of national security, are authorized.

3.6.3.2.8. Reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations or infrastructures relating to national security.

3.6.3.2.9. Violate a statute, treaty, international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

Chapter 4

MARKING CLASSIFIED INFORMATION AND CONTROLLED UNCLASSIFIED INFORMATION (CUI)

4.1. Classified Information . The proper marking of a classified document, to include e-mail, is the specific responsibility of the author (original or derivative classifier). Classified markings alert the holder to the presence of classified information, reasons for classification, identity of the person that classified the document in the event of a classification challenge or questions arise, and provide guidance on downgrading and declassification. The marking standards for classified information are published in DoDM 5200.01, Volume 2 and this AFI. The marking standard for SAP Material is in accordance with DoDM 5205.07, Volume 4, S*pecial Access Program (SAP) Security Manual: Marking*. Refer all marking questions to the servicing Wing Information Protection Office. All original and derivative classified documents will contain the overall classification in the banner lines, portion markings, and a classification authority block, unless specifically prohibited by rule. (T-0)

4.1.1. Do not re-mark documents marked in accordance with the Information Security Oversight Office Marking guide and any previous Executive Order guidance.

4.1.2. Process waivers involving marking of collateral classified information in accordance with DoDM 5200.01, Volume 2, Enclosure 1, through Information Protection channels to SAF/AAZ. Process waivers involving marking of SCI through AF/A2.

4.1.2. **(AFMC)** Center CIPs will submit collateral waivers to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit the waiver through AFMC/CV to SAF/AAZ. **(T-2).**

4.1.3. Banner Lines. All banner lines (outside front cover, title page, interior pages and outside back cover of bound documents, or first page, interior pages, and outside last page of other types of documents) will be marked with the overall classification of the document and any applicable control markings. (T-0) Interior pages shall specify either the highest level of classification of information on that page or "UNCLASSIFIED" if there is no classified information. (T-0) Refer to DoDM 5200.01, Volume 2, Enclosure 3, for specific guidance on marking banner lines.

4.1.3. **(AFMC)** Only banners and portions marked with "REL TO" can be released to a foreign entity without a formal foreign disclosure review. Markings with REL TO must be approved through the foreign disclosure office to designated countries PRIOR to use of the marking or identifying information as releasable in a SCG. **(T-2).**

4.1.4. Portion Marks. Every portion marking identified in DoDM 5200.01, Volume 2, Enclosure 3, will be marked with its highest level of classification that it contains. (T-0)

4.1.4.1. If the portion contains classified information and For Official Use Only (FOUO) information do not mark the document with its classification level and FOUO control marking. (T-0) Mark the portion only with its highest level of classification. For example: the correct marking for a portion that contains SECRET and FOUO is (S), not (S//FOUO). (T-0)

4.1.4.2. If the portion marking contains unclassified information and FOUO then mark the portion (U//FOUO) as depicted in Figure 2 of DoDM 5200.01, Volume 2. Refer to

DoDM 5200.01, Volume 4, Enclosure 3, for an explanation of marking classified documents containing FOUO.

4.1.4.3. Figure 2 DoDM 5200.01, Volume 2 provides examples of approved portion markings.

4.1.4.4. **(Added-AFMC)** Also see paragraph **4.1.3** for "REL TO" portion marks.

4.1.5. Classification Authority Block. There are two types of classification authority blocks. One type is used by OCAs and the other by derivative classifiers. DoDM 5200.01, Volume 2, contains guidance on creating the classification authority block for both types of classification authority and the block is required on all documents.

4.1.6. OCA Markings. The figures listed below are from DoDM 5200.01, Volume 2 and are the most common types of markings used in the OCA process. However, there are other examples available if needed. Consult with the Wing Information Protection Office for additional guidance as needed.

4.1.6.1. Figure 3. Example of an Originally Classified Document.

4.1.6.2. Figure 9. Declassification Markings.

4.1.6.3. Figure 11. Markings on Working Papers.

4.1.6.4. Figure 16 is an example of Marking E-mails. The illustration is for a derivative classified e-mail. For OCA e-mail with an original classification decision, delete the "Derived From" and replace with "Reason." List classification authority block dates in YYYYMMDD format. Mark the body of the e-mail and subject line manually until the Air Force endorsed marking tool is updated.

4.1.7. Derivative Markings. The figures listed below are from DoDM 5200.01, Volume 2 and are the most common types of markings used in the derivative classification process. However, there are others examples available if needed. Consult with your Security Manager or Wing Information Protection Office for additional guidance as needed.

4.1.7.1. Every document will include a classification authority block. (T-0) Refer to Enclosure 3, for instructions on how to complete a classification authority block.

4.1.7.2. Figure 4 is an Example of Derivatively Classified Document.

4.1.7.3. Figures 5-7 are examples of Markings on a Memorandum, Action Memorandum and Staff Summary Sheet.

4.1.7.4. Figure 11 is an example of Markings on Working Papers.

4.1.7.5. Figure 13 is an example of Transmittal Documents.

4.1.7.6. Figure 14 is an example of Markings on Briefing Slides and Figure 15 for Multiple Source Listing on Briefing Slides. Also mark captions and legends in charts, graphs, figures, pictures and similar portions and list multiple source dates in YYYYMMDD format. (T-0)

4.1.7.7. Figure 16 is an example for marking e-mails. See paragraph 4.1.6.3 for additional guidance.

4.1.7.8. Figure 17 is an example of a uniform resource locator (URL) with included portion mark and Figure 18 is an example of portion-marked URL embedded in text. The creator of a web page must include the classification in the URL string as shown in the figure. (T-0)

4.1.7.9. Figure 20 is an example of Markings on Maps.

4.1.7.10. Figure 21 is an example of Markings on Charts.

4.1.7.11. Figure 22 is an example of Markings on Photographs.

4.1.7.12. Figure 23 is an example of Markings on IT Systems and Media.

4.2. Controlled Unclassified Information (CUI). Certain types of unclassified information require markings. Such information is referred to as CUI. DoDM 5200.01, Volume 4, provides guidance on the various types of CUI and their associated markings. Any person having questions as to whether a marking is CUI should contact their Security Manager or Wing Information Protection Office for additional guidance.

4.2.1. The originator of a document is responsible for determining at origination whether the information may qualify for one of the CUI statuses identified in DoDM 5200.01, Volume 4. (T-0)

4.2.2. It is the responsibility of the originator when marking FOUO to determine which FOIA exemptions applies. (T-0) It is recommended the exemption number(s) be annotated at the end of the sentence or paragraph it applies to facilitate review and requests for public release in the future. Refer to DoDM 5200.01, Volume 4, Enclosure 3, for specific definitions of the exemptions.

4.2.2. **(AFMC)** A portion of paragraph 4.2.2, "It is recommended the exemption number(s) be annotated at the end of the sentence or paragraph it applies to facilitate review and requests for public release in the future" contradicts with DoDM 5200.01, Vol 4, Encl 3, Para 2c(2) "Information marked FOUO shall not specify, or have annotated, a FOIA exemption number." SAF/AAZ will remove this requirement when the AFI is updated.

4.2.3. All CUI documents, information technology, other electronic media, blueprints, engineering drawing, charts, maps, photographic media, sound recordings, microfilm, microfiche, and similar microform media, **not** contained in a classified document, will be marked in accordance with DoDM 5200.01, Volume 4, Enclosure 3. (T-0)

Chapter 5

SAFEGUARDING, STORAGE AND DESTRUCTION, TRANSMISSION AND TRANSPORTATION OF CLASSIFIED AND CONTROLLED UNCLASSIFIED INFORMATION (CUI)

5.1. Safeguarding. All Air Force personnel who work with classified information or CUI are personally responsible for taking proper precautions to ensure unauthorized persons do not gain access to classified information and CUI. (T-1) Only methods identified in DoDM 5200.01, Volumes 3 and 4 may be used to store classified information and CUI when it is not under the personal observation and control of an authorized individual.

5.1.1. Access. Commanders and Directors grant and terminate access to classified information. (T-1) Security managers provide administrative support to process approved accesses and terminate accesses.

5.1.1.1. Prior to granting access the commander or director validates the individual has:

5.1.1.1.1. A security clearance.

5.1.1.1.2. A signed Standard Form (SF) 312, "*Classified Information Non-Disclosure Agreement*" (NDA). (T-0) If the individual refuses to sign an NDA deny access to classified information (T-0) and initiate a Security Information File in accordance with AFI 31-501 (CHANGING TO AFI 16-1405)) (changing to AFI 16-1405). (T-1) Contact the local civilian human resources office or military personnel office for instructions on how to process the form for retention in personnel records.

5.1.1.1.3. A valid need to know. (T-0)

5.1.1.2. Sign the AF Form 2583 Block 26. (T-1) Once access is granted the security manager will:

5.1.1.2. **(AFMC)** May sign memo granting access to multiple individuals or use other similar signed documentation to grant access.

5.1.1.2.1. Update the Joint Personnel Adjudication System (JPAS) to show access level and NDA execution. (T-1)

5.1.1.2.2. Process the NDA in accordance with servicing personnel office (MIL/CIV) guidance. (T-1)

5.1.1.3. Commanders and Directors will terminate access to classified information whenever a person's loyalty, reliability, and trustworthiness become questionable. (T-1)

5.1.1.3.1. Document the termination on AF Form 2587, *Security Termination Statement*, and ensure the security manager is instructed to update JPAS. (T-1)

5.1.1.3.1. **(AFMC)** Individuals retiring or separating from Government employment, will sign a SF 312, security debriefing acknowledgement section. Process the SF 312 in accordance with servicing personnel office (MIL/CIV) guidance. If the individual refuses to sign the SF 312 or AF Form 2587, have a witness sign a statement indicating the individual was informed the access was terminated. **(T-2).**

5.1.1.3.2. Establish a Security Information File IAW AFI 31-501. (CHANGING TO AFI 16-1405)), if necessary. (T-1)

5.1.1.4. Commanders and directors terminate access to classified information when the individual departs the organization for separation or retirement, permanent change of station (PCS), or temporary duty (TDY) and temporary duty assignments (TDA). (T-1) This may be delegated to the Security Manager. Document the termination on AF Form 2587, *Security Termination Statement*, and ensure JPAS is updated. (T-1) Brief the individual:

5.1.1.4. **(AFMC)** The following is a clarification of paragraph 5.1.1.4. Do not terminate access and have individuals sign an AF Form 2587 every time they go TDY or TDA. If a person is granted additional accesses for the TDY/TDA, they will need to be debriefed and sign an AF Form 2587 from the additional/temporary accesses when they depart from TDY/TDA location and return to their home station. For individuals PCSing, debrief them and have them sign an AF Form 2587 and update JPAS when the individual had access to RD/CNWDI/NATO. The individual will also need to be debriefed, sign an AF Form 2587, and JPAS updated when the person doesn't need access to collateral classified information at their new duty location. AF Form 2587s are maintained for two years.

5.1.1.4.1. Their continued responsibility to protect classified information and CUI to which they have access. (T-0)

5.1.1.4.2. On instructions for reporting any unauthorized attempt to gain access to such information. (T-0)

5.1.1.4.3. On prohibitions against retaining classified information and CUI when leaving the organization. (T-0)

5.1.1.4.4. Requirements for submitting writings and other material intended for public release to the DoD security review process as specified in DoDD 5230.09, *Clearance of DoD Information for Public Release*. (T-0)

5.1.1.4.5. The potential civil and criminal penalties for failure to fulfill their continuing security responsibilities. (T-0)

5.1.1.5. Prior to granting contractors access to classified information, in addition to para 5.1.1.1.1 thru 5.1.1.1.3, verify the information/accesses are authorized via the DD Form 254, DoD Contract Security Classification Specification, on the contract. In the case of a subcontractor, review the subcontract DD Form 254.

5.1.1.5. **(AFMC)** For solicitations (i.e., Request for Information, Invitation for Bid, Request for Proposal, or other solicitation) review the DD Form 254 included with the solicitation documentation.

5.1.2. Individuals in possession of classified information have the final responsibility for determining whether a prospective recipient is authorized to have the information. (T-0) This is done by JPAS or the holder verifying access eligibility through their security manager. For contractors also verify access to the information is authorized via the DD Form 254.

5.1.3. In an emergency where there is an imminent threat to life (e.g. fire, major accident response, natural disaster, and etc.), the on-scene CC may authorize the disclosure of

classified information, including information normally requiring the originator's prior authorization, to an individual(s) who is otherwise not eligible for access. In emergencies which there is an imminent threat to the defense of the homeland the SPE or Wing/CC may authorize the disclosure of classified information. The disclosing authority or designee will:

5.1.3.1. Debrief recipients when access is no longer required using the "Security Debriefing Acknowledgement" section of SF 312. (T-1)

5.1.3.2. Report the disclosure through Information Protection channels IAW DoDM 5200.01, Volume 3, Enclosure 2. (T-0)

5.1.3.2. **(AFMC)** The ranking on-scene CC will notify their servicing CIP, who will in turn notify HQ AFMC/IP through their Center CIP and CV. HQ AFMC/IP will notify SAF/AAZ through AFMC/CV. **(T-2).**

5.1.4. Commanders and directors must ensure recipients outside the Executive Branch have appropriate eligibility for access prior to the release of classified information. Refer to DoDM 5200.01, Volume 3, Enclosure 2, for further guidance. (T-0)

5.1.5. Commanders and Directors ensure visitors to Air Force facilities are properly processed prior to granting access to classified information. (T-0) Procedures listed in DoDM 5200.01, Volume 3, Enclosure 2, are the minimum standard for verifying identity, security clearance, access (if appropriate), and need to know.

5.1.5. **(WRIGHTPATTERSONAFB)** Visitors requiring access to classified information or access to facilities containing classified material will ensure a Visit Request is sent from their home unit to the unit to be visited via the Joint Personnel Adjudication System (JPAS). The host unit security manager will identify and verify the security clearance of visitors by checking on-hand rosters, lists, visit requests, messages, etc. that have been verified through JPAS.

5.1.6. Only the SECAF and Senior Agency Official may authorize the removal of Top Secret information from designated working areas for work at home. The SPE may approve command personnel for Secret and Confidential removal from designated working areas for work at home. Refer to specific guidance in DoDM 5200.01, Volume 3, Enclosure 2. Submit all request packages through Information Protection channels to the appropriate approval authority.

5.1.7. All personnel must notify a supervisor, manager, commander, director, security manager, or Wing Information Protection Office if they discover a cellular/PCS and or radio frequency (RF) or infrared (IR) devices in areas prohibited by the commander or director. (T-1) The following procedures are courses of actions to be used to resolve the issue:

5.1.7.1. If reported to a supervisor or manager, the supervisor or manager will notify the security manager or commander. (T-1)

5.1.7.2. If reported to the security manager, the security manager will notify the commander and Wing Information Protection Office. (T-1)

5.1.7.3. The Commander, in consultation with the Wing Information Protection and Information Assurance Offices determines whether a security incident should be initiated and the disposition of the device. Government devices may be confiscated to determine if it's contaminated with classified information. If it is suspected a personal device is

contaminated with classified information request the individual surrender it. If the individual refuses to surrender the device, the commander will consult with the servicing legal office on how to resolve the issue. (T-1)

5.1.7.4. Provide an AF Form 1297, *Temporary Issue Receipt*, or similar document, for accountability purposes if a government or personal device is confiscated. (T-1) Ensure the individual is informed on the process for retrieving the device. (T-1)

5.2. Storage and Destruction. Commanders and Directors must ensure classified information is secured under conditions adequate to deter and detect access by unauthorized persons in accordance with the standards in DoDM 5200.01, Volume 3. (T-0)

5.2.1. Security-In-Depth Determinations. The Senior Agency Official delegates security in-depth determinations to MAJCOM/DRU SPEs and Wing Commanders under their control or authority when determining supplemental controls. (T-1) Security-in-depth determinations must be documented. (T-0) They may be documented for each container, room, area, or vault or in one consolidated document for the installation or area.

5.2.2. Specialized Storage for Aircraft. All persons (military, civilian, and contractors) with access to Air Force aircraft must have a security clearance and need-to-know before performing maintenance on aircraft parts or components that contain classified information. (T-0) Passengers and other uncleared personnel will be properly escorted at all times to prevent unauthorized access to classified material aboard Air Force aircraft. Wing, Maintenance and Depot Commanders are responsible for the security of aircraft while under their control and consult their Wing Information Protection Office to determine appropriate safeguarding standards. (T-1) Aircraft commanders are responsible for the protection of classified material and components aboard their aircraft while away from their home station at Air Force and DoD installations, civilian airfields, or in a foreign country. (T-1)

5.2.2.1. Park protection level (PL) 1, 2, or 3 aircraft and/or aircraft mission inside established restricted areas, or an equivalent area, while on Air Force installations and at other DoD facilities, if possible. (T-1) If this is not possible, coordinate with the local security forces, the Wing Information Protection Office, or similar service security officials to ensure the aircraft is left under the personal control and observation of an authorized person(s) with the proper security clearance. (T-1)

5.2.2.2. If the aircraft cannot be left under the personal control and observation of an authorized person(s) with the proper security clearance:

5.2.2.2.1. Zeroize keyed COMSEC equipment in accordance with AFMAN 33-283, *Communications Security (COMSEC) Operations*. (T-1)

5.2.2.2.2. Secure removable classified components and material that are not attached or secured to the aircraft in an approved storage container. (T-1) If the aircraft is not equipped with an approved storage container or the items are too large, consult with the Wing Information Protection Office or service equivalent security official to secure proper storage. (T-1)

5.2.2.2.3. Secure all egress doors from the inside if classified components and material must remain with the aircraft. (T-1) If this is not possible, secure the egress points from the outside using a GSA-approved changeable combination padlock that

meets Federal Specifications FF-P-110J, Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack), as amended. (T-1) The locks are available from the DoD Lock Program website or through GSA Advantage, (800) 525-8027, National Stock Number (NSN) 5340-00-285-6523.

5.2.2.2.4. If the aircraft cannot be locked and is not equipped with storage container, place the removable classified in an approved security container in an authorized U.S. facility. (T-1) Classified components, attached to the aircraft, do not have to be removed.

5.2.2.3. If the aircraft cannot be parked in a restricted/controlled area and cannot be left under the personal control and observation of an authorized person(s) with the proper security clearance, follow procedures as described in paragraphs 5.2.2.3.1 – 5.2.2.3.3. (T-1) Seal the aircraft egress doors with tamper-proof seals such as evidence tape or numerically accountable metal or plastic seals to detect unauthorized access. (T-1)

5.2.2.4. At non-US controlled locations where the material and components aboard are not approved for released to the host nation:

5.2.2.4.1. Place removable classified material in a storage container aboard the aircraft, and secure the aircraft in the same manner as paragraph 5.2.2.3. (T-1) Conduct aircraft and container checks every 12-hours. (T-1) This check must be conducted within 1-hour after official aircrew rest if no other U.S. Government (USG) personnel are available. (T-1)

5.2.2.4.2. If there is no storage container on the aircraft, remove all removable classified information and store in an approved security container at a USG facility. (T-1) Secure the aircraft in the same manner as paragraph 5.2.2.4.1. (T-1) Conduct aircraft checks every 12 hours. (T-1) This check must be conducted within 1-hour after official aircrew rest if no other USG personnel are available. (T-1)

5.2.2.4.3. If the aircraft does not have a storage container and no USG facility is available, the aircraft must be kept under constant surveillance by cleared USG personnel.

5.2.2.5. Aircraft commanders must make every effort to comply with the standards in paragraphs 5.2.2.3 – 5.2.2.5. (T-1) They are authorized to take prudent risk management precautions when diverted or experience in-flight emergencies to protect classified information to include COMSEC material aboard their aircraft.

5.2.3. Bulky Material and Classified Munitions. Store bulky material in accordance with DoDM 5200.01, Volume 3, Enclosure 3 and AFI 31-101, *Integrated Defense*, when storing classified munitions. (T-1) Commanders and directors may authorize, with coordination from the servicing Wing Chief, Information Protection, the use of key operated locks for storing bulky material containing Secret and Confidential information. (T-1) Submit the following:

5.2.3. **(AFMC)** Cargo security cages or rooms used for temporary storage of classified material must have an intrusion detection alarm or be checked every 4 hours when attendants are not present. Servicing CIP ensures the area meets requirements and the Wing/CC/CV approves the area for use. **(T-2).**

5.2.3. **(WRIGHTPATTERSONAFB)** Visitors to offices on WPAFB will use storage facilities in the host's office or the host will make arrangements for overnight storage of hand-carried material. If a visitor carrying classified material is scheduled to arrive after normal duty hours, a representative from the host activity will meet the individual and ensure the material is secured. Transient personnel may temporarily store classified material, SECRET or below, in the security container at Base Operations (88 OSS/OSA), Area A, Building 206. When the size of the material exceeds the storage capability at Base Operations, the Cargo Movement Terminal (88 MSG/LGRD), Area A, Building 143, is the designated facility for temporary, in-transit storage of classified material, up to and including SECRET. During normal duty hours, cargo movement terminal personnel will take direct charge of the material. After normal duty hours, Base Operations will contact the AFMC Command Center, who will notify cargo movement terminal standby personnel for support. If NATO classified material needs to be secured, during duty hours contact AFIMSC, Det 6, during non-duty hours contact the AFMC Command Center. TOP SECRET or Sensitive Compartmented Information (SCI) can be stored at the 24-hour NASIC Control Center (NCC), Area A, Building 828. Contact the NCC at 937-OK-NASIC, (937) 656-2742, or DSN 986-2742 to coordinate after hours storage requirements.

5.2.3.1. Explanation of the special circumstances warranting deviation from standards. (T-1)

5.2.3.2. Description of the administrative procedures for the control and accounting of keys and locks. (T-1)

5.2.3.2. **(AFMC)** Keys and locks will be audited semi-annually. Document the audit using AF Form 2427, Lock and Key Control Register. **(T-2).**

5.2.3.3. Protect and store the keys as a minimum of the same level afforded the classified information. (T-1)

5.2.4. Security Containers, Open Storage Rooms/Areas, and Vaults. There shall be no external mark revealing the level of classified information authorized to be actually stored in a given container, open storage, or vault or indicating the priority assigned to the container, open storage, or vault for emergency evacuation and destruction. Commanders and directors will ensure every security container, open storage room/area, and vault has an SF Form 700, *Security Container Information*, SF Form 701 (except for 24/7 operations), and SF Form 702, *Security Container Check Sheet*. (T-1) Ensure the SF Form 700, Part 2 is sealed and stored IAW DoDM 5200.01, Volume 3, Enclosure 3. (T-0)

5.2.4. **(WRIGHTPATTERSONAFB)** A new SF Form 700 is prepared each time a change is recorded. The custodian of each safe or secure facility is the first person listed on the SF Form 700. The custodian is responsible for container(s) serviceability and contents.

5.2.4.1. Security containers, open storage, and vault doors will be visually inspected upon receipt of this AFI and every 5 years thereafter using the checklist at Attachment 6. (T-1) If the security container, open storage, or vault is used to store COMSEC material, ensure the individual inspecting the container is authorized access to the COMSEC. (T-1) The inspection should be coordinated with the COMSEC Responsible Officer. Maintain the record of inspection inside the security container and produce it when requested. (T-1)

5.2.4.1. **(AFMC)** If preventive maintenance inspections were conducted in accordance with AFTO 00-20F-2, the visual inspection does not need to be conducted until five years after the last preventive maintenance inspection.

5.2.4.1.1. The Wing Information Protection Office is responsible for training security managers and security assistants on the application of the checklist. (T-1)

5.2.4.1.2. Security manager or assistants will contact the Wing Information Protection Office if discrepancies are discovered during the inspection. (T-1) Optional Form 89, Maintenance Record for Security Containers/Vault Doors replaces Air Force Technical Order (AFTO) Form 36, *Maintenance Record for Security Type Equipment*. Maintain all records of security container and vault door maintenance, repairs, and inspections while the container is in use. (T-1) Destroy AFTO Form 36 if there is no record of maintenance on existing, in use, security containers or vaults.

5.2.4.1.3. The Wing Information Protection Office is responsible for assessing discrepancies reported by security managers or assistants and determining if a GSA approved technician is needed to fix the security container or vault door. (T-1)

5.2.4.2. Reset security container, open storage room/area doors, and vault built-in combinations locks to 50-25-50 and combination padlocks to 10-20-30 when no long used to store classified information. (T-0) The Wing Information Protection office can provide guidance on proper turn-in procedures.

5.2.4.2. **(WRIGHTPATTERSONAFB)** Before transferring safes to another unit, setting aside for future use, or turning in, the security manager will inspect the container to verify all classified material is removed and the standard combination is set (50-25-50). Name, office symbol, signature and date will be affixed conspicuously to the outside of the container; also record the following statements, "This container has been inspected and does not contain classified material. The lock is set on the standard combination (50-25-50)." Contact 88 ABW/IP before purchasing or turning in any container.

5.2.4.3. Risk assessments will be conducted and documented for each Top Secret GSA-approved security container located outside of open storage room/area and SCI/SAP facility, and for all open storage rooms/areas approved to store up to Secret information IAW DoDM 5200.01, Volume 3, Enclosure 3. (T-1) The purpose of this risk assessment is to assist commanders and directors with identifying and selecting supplemental controls.

5.2.4.3. **(AFMC)** In accordance with DoDM 5200.01, Vol 3, Encl 3, Para 3a, supplemental controls are not required when Top Secret material is stored in a GSA-approved security container equipped with a lock meeting FF-L-2740, provided the container is located within an area that has been determined to have security-in-depth. See Attachment 1, Terms for definition of security-in-depth. Recommend utilizing risk assessments already complete for the wing/installation, such as for the Anti-Terrorism program and Threat Working Group.

5.2.4.3.1. If the risk assessment determines 2 hour (Top Secret) or 4 hour (Secret) checks are sufficient and intrusion detection system (IDS) is used as a supplemental control exceeding the requirement, and the IDS malfunctions, 2/4 hour checks are required. (T-1) The checks are the responsibility of the owning unit

commander/director. The commander/director may require the security container or open storage room/area be kept under 24/7 constant surveillance.

5.2.4.3.2. If a risk assessment determines IDS is mandatory and the IDS malfunctions keep the Top Secret GSA-approved storage container or Secret open storage room/area under 24/7 until the IDS is repaired. (T-1)

5.2.4.3.3. Chief Wing, Information Protection must ensure all open storage rooms/areas approved for storage of Secret information prior to October 1, 1995 are recertified to meet the requirements of DoDM 5200.01, Volume 3, Enclosure 3, Appendix. (T-0) If rooms do not meet standards, commanders and directors have two options: keep the room/area under constant 24/7 surveillance or use other approved storage methods. (T-1) Commanders and directors have 6-months from the date of this AFI to recertify the room/area or use other approved storage methods. (T-1)

5.2.5. Destruction. Commanders and Directors will ensure classified information is destroyed by authorized means and appropriately cleared personnel in accordance with the methods and procedures prescribed in DoDM 5200.01, Volume 3, Enclosure 3. (T-0) If a shredder is no longer on the approved Evaluated Products List (EPL) commanders will comply with paragraph 17.d(1) thru (3). (T-0)

5.2.5.1. **(Added-WRIGHTPATTERSONAFB)** The Central Destruction Facility (CDF), located in Area B, Building 306, is approved for destruction of all levels of classified material. Users will contact 88 ABW/IP to schedule a time to accomplish destruction. Users will comply with CDF internal operating procedures.

5.2.5.2. **(Added-WRIGHTPATTERSONAFB)** A DVD/CD shredder is available for classified destruction in Area B, Building 8; it is only authorized for CD/DVD destruction.

5.3. Transmission and Transportation. Persons transmitting or transporting classified information are responsible for ensuring the intended recipients are authorized access, have a need to know, and have the capability to store classified information. (T-0) Information may only be transmitted in accordance with DoDM 5200.01, Volume 3, Enclosure 4 unless otherwise stated.

5.3.1. Documents created BEFORE or derived from documents created prior to June 27, 2010 may not be transmitted outside of the DoD without the originator's consent. Refer to DoDM 5200.01, Volume 3, Enclosure 4, for additional information on disseminating classified information outside DoD.

5.3.2. Commanders and Directors determine the need and proper method to be used by each individual authorized to escort, courier, or hand-carry classified material on or off the installation, and establish procedures to ensure hand-carrying classified material is minimized to the greatest extend possible and does not pose unacceptable risk to the information. (T-0) Refer to DoDM 5200.01, Volume 3, Enclosure 4, for additional guidance on Escort, Courier, or Hand-Carry of Classified Material authority, packaging requirements, and responsibilities, arrangements with customs, police and/or immigration officials, disclosure authorization, authorizations statements, and transporting classified information on commercial aircraft.

5.3.2. **(AFMC)** Servicing CIP will assist Commanders and Directors with the proper method to be used to hand-carry classified material. **(T-2).**

5.3.2.1. **(Added-AFMC)** As a minimum, couriers must have verbal authorization from their supervisor or security manager to hand-carry classified material outside their normal work areas. This approval alone is sufficient when the courier remains within the confines of an access controlled installation perimeter and does not pass through an entry/exit personnel control point. **(T-2).**

5.3.2.2. **(Added-AFMC)** Documentation. Use a courier authorization letter or DD Form 2501, Courier Authorization, when hand-carrying classified material and the courier is required to pass through an installation or facility check point. A courier must carry an authorization letter when traveling aboard commercial passenger aircraft. **(T-2).**

5.3.3. All personnel will use the AF Form 310, *Document Receipt and Destruction Certificate*, when transmitting Top Secret and Secret information, or when any level of classified information is hand-carried and not returned. (T-1) AF Form 310 may serve as the inventory when hand-carrying classified information. The following will be taken to ensure receipt of classified information:

5.3.3. **(AFMC)** When hand-carrying classified information, the AF Form 310 only needs to be used when the information is hand-carried off the installation and the information is to be transferred and left behind.

5.3.3.1. The sender will contact the recipient if the AF Form 310 is not received within 15 duty days for CONUS or 30 duty days OCONUS of the date on the AF Form 310 to determine if the package has been received. (T-1)

5.3.3.2. If the package, after confirmation by U.S. Postal Service or the shipping company that it is not in transit and has not been received by the recipient, the sender will contact their Security Manager. (T-1)

5.3.3.3. The Security Manager will contact the Wing Information Protection Office and a security inquiry will be initiated in accordance with DoDM 5200.01, Volume 3 and this AFI. (T-0)

5.4. (Added-AFMC) Administrative Control of Top Secret Information. The security of Top Secret material is paramount. Strict compliance with Top Secret control procedures take precedence over administrative convenience. These procedures ensure stringent need to know rules and security safeguards are applied to our most critical and sensitive information. AFMC accounts for Top Secret material and disposes of such administrative records according to WebRims Records Disposition Schedule.

5.4.1. **(Added-AFMC)** Establishing a Top Secret Control Account. Commanders, Directors, and lead positions at GSUs (e.g., Division, Branch Chiefs) who originate, store, receive, or dispatch Top Secret materials establish a Top Secret account and designate a TSCO, with one or more alternates, to maintain it. The Commander, Director, or lead position at GSUs (e.g., Division, Branch Chiefs) will notify the servicing CIP of the establishment of a Top Secret control account and the names of the TSCO(s). The TSCO uses AF Form143, Top Secret Register Page, to account for each document (to include page changes and inserts that have not yet been incorporated into the basic document) and each

piece of material or equipment to include IS media. ***NOTE:*** For IS information systems or microfiche media, TSCOs must either describe each Top Secret document stored on the media on the AF Form 143 or attach a list of the documents to it. This will facilitate a damage assessment if the media are lost or stolen. **(T-2).**

5.4.1.1. **(Added-AFMC)** Defense Courier Service (DCS) Receipts. TSCOs don't use AF Forms 143 as a receipt for information received from or delivered to the DCS. DCS receipts suffice for accountability purposes in these cases. Retain as prescribed by *WebRims Records Disposition Schedule*.

5.4.1.2. **(Added-AFMC)** TSCOs may automate their accounts as long as all of the required information is included in the information system, there is a means to keep inactive records, and the records are being backed up or have a hard copy back up. **(T-2).**

5.4.2. **(Added-AFMC)** Top Secret Disclosure Records.

5.4.2.1. **(Added-AFMC)** The TSCO uses AF Form 144, Top Secret Access Record and Cover Sheet, as the disclosure record and keeps it attached to the applicable Top Secret material. Each person that accesses the attached Top Secret information signs the form prior to initial access and only needs to sign the AF Form 144 once. **(T-2).**

5.4.2.2. **(Added-AFMC)** People assigned to an office that processes large volumes (i.e., several hundred documents) of Top Secret material need not record who accesses the material. ***NOTE:*** This applies only when these offices limit entry to assigned and appropriately cleared personnel identified on an access roster.

5.4.3. **(Added-AFMC)** Top Secret Inventories. Commanders, Directors, and lead positions at GSUs (e.g., Division, Branch Chiefs):

5.4.3.1. **(Added-AFMC)** Designate officials to conduct annual inventories for all Top Secret material in the account and to conduct inventories whenever there is a change in TSCOs. These officials must be someone other than the TSCO or alternate TSCOs of the Top Secret account being inventoried. The purpose of the inventory is to ensure all of the Top Secret material is accounted for, discrepancies resolved, and its status is correctly reflected on the corresponding AF Form 143. **(T-2).**

5.4.3.2. **(Added-AFMC)** Ensure necessary actions are taken to correct deficiencies identified in the inventory report. **(T-2).**

5.4.3.3. **(Added-AFMC)** Ensure the inventory report and a record of corrective actions taken is maintained with the account. **(T-2).**

5.4.3.4. **(Added-AFMC)** May authorize the annual inventory of Top Secret documents and material in repositories, libraries, or activities storing large volumes of Top Secret documents and material be limited to a random sampling using the percentage scale indicated below. If account discrepancies are discovered the Commander, Director, or lead position at GSUs (e.g., Division, Branch Chiefs) must determine if the random sample percentage method will suffice or if a higher percentage inventory will be accomplished. If the higher percentage inventory is chosen, the inventory percentage will increase by no less than 20 percent.

5.4.3.4.1. **(Added-AFMC)** One hundred percent, if there are fewer than 300 Top Secret documents.

5.4.3.4.2. **(Added-AFMC)** No less than 90 percent if the holdings range from 301 to 400 Top Secret documents.

5.4.3.4.3. **(Added-AFMC)** No less than 80 percent if the holdings range from 401 to 500 Top Secret documents.

5.4.3.4.4. **(Added-AFMC)** No less than 70 percent if the holdings range from 501 to 600 Top Secret documents.

5.4.3.4.5. **(Added-AFMC)** No less than 60 percent if the holdings range from 601 to 800 Top Secret documents.

5.4.3.4.6. **(Added-AFMC)** No less than 50 percent if the holdings range from 801 to 1,000 Top Secret documents.

5.4.3.4.7. **(Added-AFMC)** No less than 40 percent if the holdings range from 1,001 to 1,300 Top Secret documents.

5.4.3.4.8. **(Added-AFMC)** No less than 30 percent if the holdings range from 1,301 to 1,800 Top Secret documents.

5.4.3.4.9. **(Added-AFMC)** No less than 20 percent if the holdings range from 1,801 to 2,800 Top Secret documents.

5.4.3.4.10. **(Added-AFMC)** No less than 10 percent if the holdings exceed 2,800 Top Secret documents.

5.4.4. **(Added-AFMC)** Special Access Programs will follow the inventory and accountability requirements prescribed by the AFSAPCO.

5.4.5. **(Added-AFMC)** Top Secret Receipts. TSCOs use AF Form 143 or AF Form 310 as a receipt when transferring Top Secret material from one TSCO to another. **(T-2).**

5.4.6. **(Added-AFMC)** Top Secret Facsimiles. Top Secret facsimiles will be processed as another copy of the original Top Secret document in the TSCA. All the same rules apply except the register page and disclosure record will be faxed along with the document to the addressee. The addressee will sign and return them immediately to the sender for inclusion in the Top Secret account. **(T-2).**

5.4.7. **(Added-AFMC)** Records of Destruction. TSCOs will ensure:

5.4.7.1. **(Added-AFMC)** Two people with Top Secret access are involved in the destruction process; **(T-2).**

5.4.7.2. **(Added-AFMC)** Destruction is recorded on one of these forms: AF Form 143; AF Form 310; or, AF Form 1565, and, **(T-2).**

5.4.7.3. **(Added-AFMC)** The destruction record is attached to the AF Form 143 (used to account for the document) when the destruction is not recorded on the AF Form 143 itself. **(T-2).**

Chapter 6

SECURITY EDUCATION AND TRAINING AWARENESS

6.1. General Requirement. Commanders and Directors ensure their personnel receive security education and training. (T-1) The training is designed to instill and maintain continuing awareness of security requirements and assist in promoting a high degree of motivation to support program goal.

6.1. (AFMC) General Requirement. Commanders and Directors ensure personnel receive security education and training at all locations under their command to include geographically separated units (GSU). **(T-2).**

6.1.1. **(Added-AFMC)** Center/Wing CIPs ensure Commanders and Directors receive security education and training on the Commanders/Directors Information Protection responsibilities explained within DoD and AF regulations (Information, Industrial, and Personnel Security programs). **(T-2).**

6.2. Initial Orientation Training. All Air Force personnel must complete the Security Administration (formerly Information Protection) Course in Advanced Distance Learning System (ADLS) upon assignment to the unit. (T-1) This course provides the foundational knowledge of the Air Force Information Security Program which (1) defines classified information and CUI, (2) produces a basic understanding of security policies and principles, (3) notifies personnel of their responsibilities and the sanctions that can be applied, (4) ensures proper protection of classified and CUI, (5) explains actions to take if classified information or CUI is found unsecured, a vulnerability is noted, or a person seeks unauthorized access, and (6) informs the need to review all unclassified DoD information prior to public release. Prior to accessing government information systems all personnel must complete the DoD IAA Cyber Awareness Challenge training in ADLS. (T-1) Completion of ADLS training does not meet access to classified information, derivative classification or classified information systems training.

6.2. (AFMC) Initial Orientation Training . The Security Administration (formerly Information Protection) Course in ADLS is valid for one year. If the individual can show proof they have completed the ADLS Security Administration Course within the last 12 months, they meet the requirement of completing the course upon assignment to the unit.

6.2.1. Access to Classified Information. All cleared Air Force personnel must complete training that meets the requirements of DoDM 5200.01, Volume 3, Enclosure 5 upon assignment to the unit and prior to accessing classified information. (T-0) In addition, provide guidance on specific classified information and CUI created, handled or stored within the organization. (T-0) This training is developed locally.

6.2.1. **(AFMC)** Commanders and directors establish procedures to maintain initial orientation training records. Documentation methodology must allow tracking of the training to determine date of training, subject areas covered, identity of both attendees and non-attendees and percentage of the target group actually receiving/completing the training. Procedures must be in place to identify and provide make-up for those missing initial orientation training within 90 days of their hiring date or before they access classified information, whichever comes first. **(T-2).**

6.2.2. Derivative Classification Training. All Air Force personnel with access to a classified information system or designated by their commander or director must complete initial derivative classification training prior to making any derivative classification decisions and every 2 years thereafter, and maintain copies of their training records and provide them upon request. (T-0)

6.2.2. **(AFMC)** Security training records will also be maintained by the security manager or organization's training monitor. **(T-2).**

6.2.2.1. Initial Training: Complete both the Derivative Classification and Marking Classified Information web based courses located at **http://cdsetrain.dtic.mil/** or locally produced training that meets all requirements of DoDM 5200.01, Volume 3, Enclosure 5. (T-1)

6.2.2.2. Refresher Training: Complete only the Derivative Classification Refresher located at **http://cdsetrain.dtic.mil/** or locally produced training that meets all requirements of DoDM 5200.01, Volume 3, Enclosure 5. (T-1)

6.2.2.3. If records are lost or more than 2 years has elapsed between trainings then the individual must complete initial training requirements in paragraph 3.4.1.1. (T-1)

6.2.3. Classified Information Systems. All personnel must complete training prior to accessing classified information systems which specifically addresses the requirements in DoDM 5200.01, Volume 3, Enclosure 5, and definitions of Negligent Discharge of Classified Information (NDCI) and willful, negligent, or inadvertent classified information spillage. (T-1) See terms in Attachment 1.

6.2.3. **(WRIGHTPATTERSONAFB)** A record of this training will be maintained by the security manager or unit training manager.

6.3. Special Training Requirements. Refer to DoDM 5200.01, Volume 3, Enclosure 5, for a list of special training requirements and topics for deployable organizations and additional security education and training under special circumstances. This training is developed locally as situations apply.

6.4. Annual Refresher Training. All Air Force personnel must complete the Security Administration Course and DoD IAA Cyber Awareness Challenge in ADLS, and training required in 6.2.1 – 6.2.3, annually, unless stipulated otherwise. (T-0) In addition, commanders and directors will ensure these topics are addressed during refresher and/or continuing training throughout the year during commander's calls, roll call training and similar forums:

6.4. (AFMC) Annual Refresher Training. Commanders and Directors establish procedures to maintain annual refresher training records. Documentation methodology must allow tracking of the training to determine date of training, subject areas covered, identity of both attendees and non-attendees and percentage of the target group actually receiving/completing the training. Procedures must be in place to identify and provide timely make-up for those missing regularly scheduled training, at least by the end of the calendar year. **(T-2).**

6.4. (WRIGHTPATTERSONAFB) Use of email read receipts , as a sole source of tracking training, is prohibited.

6.4.1. Local threat and techniques foreign intelligence activities use while attempting to obtain classified information. (T-0)

6.4.2. Penalties for engaging in espionage and other unauthorized disclosures. (T-0)

6.4.3. Relevant changes in information security policy or procedures. (T-0)

6.4.4. Issues or concerns during Wing Information Security Program self-inspection conducted by the Wing Information Protection Office or squadron self-assessment. (T-0)

6.5. OCA and Derivative Classifier Training Waivers. Submit waiver requests for OCA and derivative classifiers through information protection program channels to SAF/AAZ. (T-1) Include a description of the unavoidable circumstances and date the individual will be required to complete the training. (T-1) If approved, the OCA or derivative classifier training must be completed as soon as practicable. (T-0)

6.5. (AFMC) Center CIPs will submit waiver requests to HQ AFMC/IP through their Center/CV. HQ AFMC/IP will submit the request through AFMC/CV to SAF/AAZ. **(T-2).**

6.6. Declassification Authority Training and Certification Program. AFDO is responsible for development and execution of this program. AFDO is authorized to alter delivery methods of this training to ensure it reaches across all Air Force organizations CONUS and OCONUS. This training is provided to all Air Force personnel (military and civilian) designated as declassification authorities IAW **Chapter 3** of this AFI. This training meets the requirements established in DoDM 5200.01, Volume 3, Enclosure 5. The purpose of this training is to efficiently and effectively protect Air Force historical information. Each individual designated declassification authority completes: (T-1)

6.6.1. Air Force Classification/Declassification Seminar.

6.6.2. Department of Energy Historical Records Restricted Data Reviewers Course.

6.6.3. Air Force Technical Applications Center Equity Recognition Course.

6.6.4. Other Government Agency equity recognition training.

6.6.5. Supervised review under the auspices of AFDO.

6.6.6. Receive 90% or better on the Air Force Initial Declassification Examination.

6.7. Management and Oversight Training. Individuals whose duties significantly involve managing and overseeing classified information (e.g. security specialists and security managers) shall receive training upon assuming duties and must be documented. (T-0)

6.7.1. Information Security Specialists. Must be trained on the areas listed in DoDM 5200.01, Volume 3, Enclosure 5. (T-0) This training may be developed by the Director or Chief, Information Protection or by using available online or in-residence courses available through the Defense Security Service (DSS), Center for Development of Security Excellence (CDSE), **www.dss.mil**. The training must be completed within 6 months. (T-0) Any one of the below curriculums, courses and certifications satisfy this requirement:

6.7.1.1. Completion of DSS on-line DoD Security Specialist Curriculum.

6.7.1.2. Completion of DSS on-line Information Security Management Curriculum.

6.7.1.3. In-resident DSS DoD Security Specialist Course.

6.7.1.4. In-resident DSS Information Security Management Course.

6.7.1.5. Conferral of Security Fundamentals Professional Certification (SFPC) under the DoD Security Professional Education Development (SPēD) Program IAW DoD 3305.13-M, *DoD Security Accreditation and Certification*. Note: SFPC must be current and in good standing. Information regarding the status of an employee's certification status can be obtained via the Air Force Security Career Field Management team (AFPC/DPIBB) at **afpc.security.cft@us.af.mil**.

6.7.2. Security Managers and Assistant Security Managers. Must complete training created by the Wing Information Protection Office that satisfies the requirements of DoDM 5200.01, Volume 3, Enclosure 5 or the Air Force Security Manager Curriculum online knowledge/awareness training in Information, Personnel and Industrial Security, or a combination of Wing and online training within 6 months of assuming duties. (T-0) These free online courses are available at **www.dss.mil**. Contact the Wing Information Protection Office for guidance on how to access these courses.

6.7.2. **(WRIGHTPATTERSONAFB)** Security managers and alternate security managers must attend security manager training provided by 88 ABW/IP. It is recommended the following online courses also be completed.

6.7.2.1. Information Security. Introduction to Information Security (IF109.16); Marking Classified Information (IF105.16); and Storage Containers and Facilities (PY105.16)

6.7.2.2. Personnel Security. Introduction to Personnel Security (PS113.16); Introduction to DoD Personnel Security Adjudication (PS001.18).

6.7.2.3. Industrial Security. Introduction to Industrial Security (IS011.16).

6.7.3. Security Assistants. As determined by the security manager to meet the need of the organization. Coordinate the training with Wing Information Protection Office. (T-1) Training must be completed within 6 months of assuming duties. (T-0)

6.7.3. **(WRIGHTPATTERSONAFB)** Security managers will train security assistants on their specific duties within 2 months of appointment.

6.7.4. MAJCOM/DRU Director and Wing Chief, Information Protection must be trained on the areas listed in DoDM 5200.01, Volume 3, Enclosure 5, within 6 months of assignment if their duties include management of one or more of the core security disciplines within Information Protection. (T-0) Local training must be approved by the MAJCOM/DRU SPE or Wing/CC. (T-0) Any one of the below satisfy this requirement:

6.7.4.1. Completion of DSS on-line DoD Security Specialist Curriculum and Information Security Management Curriculum.

6.7.4.2. Completion of in-resident DSS DoD Security Specialist Course and Information Security Management Course.

6.7.4.3. Conferral of Security Asset Protection Professional Certification (SAPPC) under the DoD SPēD Program IAW DoD 3305.13-M, DoD Security Accreditation and Certification. Note: SAPPC must be current and in good standing. Information regarding the status of an employee's certification status can be obtained via the Air Force Security Career Field Management team (AFPC/DPIBB) at **afpc.security.cft@us.af.mil**

Chapter 7

SECURITY INCIDENTS INVOLVING CLASSIFIED INFORMATION

7.1. Introduction. The compromise of classified information presents a threat to the national security and may damage intelligence or operational capabilities, lessen the Air Force's ability to protect critical information, technologies, and programs, or reduce the effectiveness of Air Force management. Refer to DoDM 5200.01, Volume 3, Enclosure 6, Security Incidents Involving Classified Information.

7.1.1. **(Added-AFMC)** Controlled Unclassified Information. For unauthorized disclosures of CUI see DoDM 5200.01, Volume 4, Enclosure 3, paragraph 1k.

7.2. Reporting and Notifications. Commanders and Directors will ensure all personnel (cleared and uncleared) are made aware of their responsibilities to report security incidents involving classified information. (T-1) All Air Force personnel who become aware of any possible security incident involving classified information (e.g., unsecured, discussed in front of uncleared personnel, etc.), regardless of whether it did or could have resulted in an actual, potential or suspected loss or compromise of classified information shall immediately report it to their commander or director, supervisor, or security manager. (T-0) Supervisors and security managers' report the security incident to their commander or director. (T-1) Commanders or directors report the incident to the Wing Information Protection Office. (T-1) The Wing Information Protection Office will assist the commander or director in determining if the incident warrants an inquiry. (T-1) The Wing Information Protection Office will track and provide oversight of the security incident. (T-1) If needed, include the process in the wing instruction.

7.2. (AFMC) Reporting and Notifications. When delegated or agreed upon through a host tenant support agreement or MOA/MOU, senior organizational leader at a GSU (e.g., Division, Branch Chiefs) reports incidents to their servicing host CIP. Incidents involving SAP information are reported through SAP channels. **(T-2).**

7.2.1. Discovery. Anyone discovering classified information unsecure or on unauthorized information systems shall:

7.2.1.1. Take custody of the information. (T-0)

7.2.1.2. Safeguard the information. (T-0)

7.2.1.3. Notify their Commander or Director, supervisor, or Security Manager using secure communication when making the notification if possible. (T-0) Identify:

7.2.1.3.1. The type or level of information involved. (T-0)

7.2.1.3.2. All the persons involved. (T-0)

7.2.1.3.3. Where the incident occurred. (T-0)

7.2.1.3.4. When the incident was discovered. (T-0)

7.2.1.3.5. Actions taken to safeguard the information. (T-0)

7.2.2. Fact Finding. Commanders and Directors initiate an inquiry, investigation, or both as circumstances warrant.

7.2.2. **(AFMC)** When delegated, the senior organizational leader at a GSU (e.g., Division, Branch Chiefs) also initiates an inquiry, investigation, or both.

7.2.3. Notifications. Commanders and Directors ensure security incidents are reported through Information Protection channels to SAF/AAZ, if needed. (T-1) SAF/AAZ notifies appropriate organizations to resolve any issues.

7.2.3. **(AFMC)** If needed, Center CIPs will submit security incident reports through their Center CV to HQ AFMC/IP. HQ AFMC/IP will submit the report through AFMC/CV to SAF/AAZ. **(T-2).**

7.2.4. **(Added-AFMC)** For security incidents involving USAF weapons systems data or information, ensure the program office for the affected system notifies the appropriate weapon system Authorizing Official and/or Security Control Assessor office for consideration of cybersecurity risks and associated security controls.

7.3. Security Inquires. Security inquiries are initiated for a security incident to determine the facts and circumstances of the incident, whether there was a loss or compromise of classified information, and to characterize the incident as an infraction or violation.

7.3.1. Inquiry Officials. Commanders and Directors shall appoint an inquiry official, in writing within two duty days from the discovery of the security incident. (T-1) These individuals will not be less in rank or grade than the person(s) involved with the incident, the security manager, persons assigned to the Information Protection Office, or Director or Chief, Information Protection. (T-1) The individual must be cleared to the highest level of information involved or be given one-time access IAW AFI 31-501 (CHANGING TO AFI 16-1405)). (T-1) The inquiry official shall:

7.3.1. **(AFMC)** See Figure **A7.1** for a sample inquiry official appointment memo. To clarify AFI 16-1404, paragraph 7.3.1, inquiry officials will be equal to or higher in rank or grade than the person(s) suspected of causing the incident. Inquiry officials will also not be the security manager, persons assigned to the Information Protection Office, or Director or Chief, Information Protection.

7.3.1.1. Consult with the Wing Information Protection Office before beginning the inquiry and prior to submitting the report to the commander/director for additional guidance and to ensure the report contains the necessary information to adequately address the security incident. (T-1)

7.3.1.1. **(AFMC)** Servicing CIPs will conduct a technical review and attach it to the inquiry/investigation report prior to submitting the report to the appointing authority. See Figure A8.1 for a sample IP technical review memo. **(T-2).**

7.3.1.2. Complete the inquiry within 10 duty days from the date of appointment and when necessary request an extension from the commander or Director. (T-0) If an extension is granted, notify the Wing Information Protection Office for tracking purposes. (T-1)

7.3.1.3. Determine and report facts, make conclusions of whether or not classified information was actually, potentially, or suspected loss or compromised, characterize the incident as a security infraction or violation and recommend actions to prevent future incidents. (T-0) Do not recommend punitive action against individuals.

7.3.1.4. Answer all questions listed in DoDM 5200.01, Volume 3, Enclosure 6. (T-0)

7.3.1.5. Use the security incident reporting format in Appendix 1 to Enclosure 6, or format prescribed by the MAJCOM/DRU or Wing. (T-1)

7.3.1.5.1. Mark the report "FOR OFFICIAL USE ONLY" if no classified information is contained in the report. (T-0) Classify the report according to the content. (T-1)

7.3.1.5.2. Include a statement citing whether the incident is willful, negligent, or inadvertent if the incident occurred on an information security systems. (T-1)

7.3.1.5.3. Include a statement that the report was reviewed by the Wing Information Protection Office prior to submitting the report to the commander or director for approval/review. (T-1)

7.3.1.5.3. **(AFMC)** This statement is not required since the servicing CIP is required to attach their technical review to the inquiry/investigation report prior to submitting the report to the appointing authority. See attachment AFMC paragraph 7.3.1.1. **(T-2).**

7.3.2. Commanders and Directors approve, endorse, and close inquiry reports after review by the Wing Information Protection Office. (T-1)

7.3.2. **(AFMC)** Commanders and Directors, or when delegated lead positions at GSUs (e.g., Division, Branch Chiefs), will close the inquiry/investigation report and forward a copy to the servicing CIP within 20 duty days from receiving the preliminary inquiry/investigation report. See Figure A9.1 for a sample closure memo. **(T-2).**

7.3.2.1. Grant inquiry officials extensions in increments not to exceed 10 duty days unless special circumstances exist. (T-1) The Wing Information Protection Office must be notified of the extension for tracking purposes and monitoring requests. (T-1)

7.3.2.2. In approvals, endorsements, and closures to reports address:

7.3.2.2.1. Concurrence in whole or part with the findings. (T-0)

7.3.2.2.2. If an actual, potential or suspected loss or compromise occurred or did not occur and whether or not further investigation is needed. (T-0)

7.3.2.2.3. Classification of the incident as a security violation or infraction. (T-0)

7.3.2.2.4. Corrective actions to prevent further occurrences are appropriate and if necessary, incorporate the actions into the security plan. (T-0)

7.3.2.2.5. Any administrative, disciplinary or punitive action taken against individual(s) responsible for the violation if warranted. (T-0) This may include verbal counseling and/or remedial training if this is deemed more appropriate for the situation. (T-1)

7.3.2.2.6. Any OCAs notified to complete damage assessments. (T-0)

7.3.2.2.6. **(WRIGHTPATTERSONAFB)** Refer to DODM 5200.01, Volume 3, Enclosure 6, for actions by the OCA and damage assessments.

7.3.2.3. Determine if user accounts will be suspended while inquiries or investigations are ongoing involving information systems. (T-0) If suspended, the individual will be required to complete training tailored to the nature of the incident prior to reinstatement. (T-0)

7.3.2.4. Consider establishing a Security Information File (SIF) IAW AFI 31-501 (CHANGING TO AFI 16-1405)) when it is determined the violation was a willful or negligent unauthorized disclosure involving information systems. (T-1) Contact the Wing Information Protection Office for guidance before authorizing entries in JPAS to ensure accurate reporting. (T-1) Some entries are permanent and cannot be removed without DoD Central Adjudication Facility approval.

7.3.2.5. Determine if debriefings are warranted. (T-0) Refer to DoDM 5200.01, Volume 3, Enclosure 6, for specific information on debriefings.

7.3.3. Wing Chief, Information Protection. Provide guidance and assistance to commanders and directors, security managers, and inquiry officials/investigators as necessary, and reviews preliminary inquiry and formal investigation reports. (T-1)

7.3.3. **(AFMC)** Servicing CIPs will conduct a technical review of all preliminary inquiry and formal investigation reports. See Figure A8.1 for a sample technical review memo. **(T-2).**

7.3.3.1. Must notify SAF/AAZ through Information Protection channels of: (T-1)

7.3.3.1. **(AFMC)** Center CIPs will ensure their Center CV is aware of the incident and then notify HQ AFMC/IP. HQ AFMC/IP will brief AFMC/CV of the incident before notifying SAF/AAZ. **(T-2).**

7.3.3.1.1. Violations involving espionage. (T-0)

7.3.3.1.2. Unauthorized disclosure of classified information in the public media. (T-0)

7.3.3.1.3. Any violation where properly classified information is knowingly, willfully, or negligently disclosed to unauthorized person. (T-0)

7.3.3.1.4. Any special circumstance that occurs requiring unique handling or consideration identified in DoDM 5200.01, Volume 3, Enclosure 6. (T-0)

7.3.3.1.5. Any inadvertent, willful, or negligent incident involving unauthorized disclosure on an information system. Include the security incident report. (T-0)

7.3.3.1.6. Incidents involving a non-Air Force organization or OCA. (T-0

7.3.3.2. Enter the individuals who caused willful and negligent unauthorized disclosure of classified information on DoD information systems in JPAS and transmit the closed inquiry/investigation report to the DoD Consolidated Adjudication Facility (CAF). (T-1)

7.3.3.2. **(AFMC)** This applies to classified message incidents (CMI) and spills on information systems whether the incident is closed as no compromise, compromise, or possible compromise.

7.3.3.3. Keep a rolling total of all security infractions and violations and submit the data, when requested. (T-1) Use these categories for reporting purposes and identify the area most impacted. Do not report the same infraction/violation in more than one area.

7.3.3.3. **(AFMC)** See paragraph **2.5.11**.

7.3.3.3.1. Unauthorized Access: Unauthorized personnel accessed or had opportunity to access classified material. This includes those with a clearance and no valid need-to-know or authorized access; and sharing classified passwords, tokens, PINs, or other access credentials permitting access into classified areas or classified systems.

7.3.3.3.2. Information Technology (IT) Data Spillage: A higher classification level of data is placed on a lower classification level system/device. 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 data spillage is not necessarily a CMI.

7.3.3.3.3. IT Classified Message Incidents (CMI): A higher classification level of data is placed on a lower classification level system/device. 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 data spillage is not necessarily a CMI.

7.3.3.3.3. **(AFMC)** The above definition is for IT Data Spill. The correct definition for IT CMI is: CMI – A higher classification level of data is transferred to a lower classification level system/device via messaging systems, e.g., e-mail, instant messaging, etc. See Attachment 1, Terms, CMI.

7.3.3.3.4. Improper Classification Action: Improper original and derivative classification decisions, classification level designations, and/or classification actions, including incorrect/missing markings that caused mishandling of classified information.

7.3.3.3.5. Improper Destruction: Destruction by unauthorized means.

7.3.3.3.6. Improper Storage: Unsecured documents, equipment, and secure rooms; unauthorized storage containers; etc.

7.3.3.3.7. Improper Transmission: Transmitting or transporting classified via unsecured or unapproved means (other than through IT systems), improper hand-carrying, errors in packaging, classified discussions over unsecured lines, and etc.

7.3.3.3.8. Unauthorized Reproduction: Reproduction by unauthorized means or reproducing material not authorized for reproduction.

7.3.3.3.9. Other: Other incidents not fitting into the above categories.

7.4. Security Investigations. When a security incident requires more details because it is not clear who, what, when, where, why and how an incident occurred or the scope of the incident is so large and involves multiple organizations both internal and external, the commander or director appoints an individual to conduct an investigation. (T-1) The appointment should include suspense for completing the investigation (normally not to exceed 30 days). (T-0)

Individuals identified in AFI 90-301, *Inspector General Complaints Resolutions*, may use the appointment process and procedures outlined in the AFI to conduct the investigation. As a minimum the appointed individual shall:

7.4.1. Be sufficiently senior. (T-0)

7.4.2. Not be anyone involved in the incident, the security manager, a person assigned to an Information Protection Directorate or Office. (T-1)

7.5. Security Incident Reporting and Oversight. Each MAJCOM/DRU Director, Information Protection will keep a rolling total of all security infractions and violations for their command using the categories in paragraph 7.3.3.3. Submit the information to SAF/AAZ when requested.

7.5. (AFMC) Security Incident Reporting and Oversight. This is accomplished through a monthly security incident data call provided by Center and Wing CIPs. See paragraph 2.5.11. **(T-2).**

7.6. (Added-AFMC) Damage Assessment. OCAs must maintain records of damage assessments they prepare in a manner that facilitates their retrieval and use. Dispose of the records IAW the Air Force Records Disposition Schedule. OCAs provide a copy of damage assessments to the servicing CIP for attachment to the file copy of the security incident. **(T-2).**

Chapter 8

NUCLEAR CLASSIFIED INFORMATION SECURITY (RESTRICTED DATA (RD), FORMERLY RESTRICTED (FRD), CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI), AND DOE SIGMA) AND NUCLEAR CUI

8.1. General. The Air Force Information Security Program consists of processes and procedures to identify, control, and disseminate the following nuclear specific information: RD to include CNWDI, FRD, DOE Sigma, and the nuclear CUI category Unclassified Controlled Nuclear Information (UCNI).

8.1.1. Additional requirements for RD, FRD, CNWDI and DOE Sigma can be found in DoDI 5210.02, *Access to and Dissemination of Restricted Data and Formerly Restricted Data.* Mark RD, FRD, CNWDI and DOE Sigma material in accordance with DoDM 5200.01, Volume 2.

8.1.2. Additional requirements for DoD UCNI can be found in DoDI 5210.83, *DoD Unclassified Controlled Nuclear Information (UCNI)* and DoDM 5200.01, Volume 4. Mark UCNI material in accordance with DoDM 5200.01, Volume 4.

8.1.3. A list of Air Force Officials Authorized to Certify Access to RD is located in DoDI 5210.02, Enclosure 4. MAJCOM/DRU and Wings supporting these visits should maintain a copy of this enclosure. These officials are responsible for certifying access to RD when Air Force personnel visit DoE organizations using DoE Form 5631.20, *Request for Visit or Access Approval*. (T-1) Air Force personnel may obtain DoE Form 5631.20 from the DoE activity they are visiting or at the DoE forms web site. Submit additions/deletions to this list through Information Protection channels to SAF/AAZ. (T-1)

8.1.3. **(AFMC)** Centers supporting these visits maintain a copy of DoDI 5210.02, Enclosure 4. Center CIPs will submit additions/deletions for Enclosure 4 to HQ AFMC/IP. HQ AFMC/IP will submit the additions/deletions to SAF/AAZ. **(T-2).**

8.2. Restricted Data (RD) Management Official. The RD Management Officials shall:

8.2.1. Disseminate implementing directives and nuclear classification guides as needed. (T-0)

8.2.2. Ensure U.S. Government and contractor personnel with access to RD and FRD are trained on the procedures for derivative classification, marking, recognizing, and handling RD and FRD information and documents, to include CNWDI, if CNWDI access is granted. (T-0)

8.3. The Director , Security, Special Program Oversight, and Information Protection (SAF/AAZ). Serves as the principle advisor to the Air Force RD Management Official (SAF/AA) on the Nuclear Information Security Program.

8.3.1. Ensure all Air Force developed training materials are coordinated with DoD/DOE.

8.3.2. Coordinates with DOE to provide DOE-certified courses when necessary.

8.4. The Deputy Chief of Staff, Logistics, Installations and Mission Support (AF/A4). Serves as the Air Force OPR for UCNI.

8.4.1. Identify DoD UCNI within the Air Force IAW DoDI 5210.83, Enclosure 3, *DoD Controlled Unclassified Nuclear Information (UCNI)*.

8.4.2. Serve as the Air Force's final authority on whether documents contain, do not contain, or no longer contain DoD UCNI, when requested.

8.5. The Assistant Chief of Staff, Strategic Deterrence & Nuclear Integration (AF/A10) provides subject matter expertise on classification and declassification of nuclear information in support of the Air Force RD Management Official (SAF/AA). AF/A10:

8.5.1. Reviews classification challenges and security incidents when RD or FRD data is involved.

8.5.2. Serves as the OPR for Air Force personnel requiring access to DOE Sigma nuclear weapon data.Notify the Air Force Personnel Center (AFPC) to ensure a permanent assignment limitation code is applied to personnel records for those personnel granted access to Sigma 14.

8.5.3. Coordinates on classification guides containing nuclear weapon data developed by DOE and DoD offices and intended for use by Air Force personnel.

8.5.4. Serves as the Air Force OPR for classification/declassification of AF information marked RD or FRD; coordinate changes with ASD(NCB), as necessary.

8.5.5. Distributes or makes available joint DOE/DoD security classification guides.

8.6. Access to FRD. To have access to FRD an individual must have a valid security clearance at a level commensurate with the information concerned and a need-to-know. (T-0) For example, an individual needs to have a Secret clearance and need-to-know to review S//FRD. There is no special indoctrination required to have access to FRD.

8.6.1. DoDM 5200.01, Volume 2, Enclosure 4, Figure 37 is an example of FRD markings, and will assist persons with recognizing FRD information in documents.

8.6.2. An individual with a TOP SECRET security clearance may have access to TOP SECRET, SECRET, and CONFIDENTIAL FRD information if they have a need-to-know.

8.6.3. An individual with a SECRET security clearance may have access to SECRET and CONFIDENTIAL FRD information if they have a need-to-know.

8.6.4. An individual with CONFIDENTIAL security clearance may have access to CONFIDENTIAL FRD information only.

8.7. Access to RD. Commanders and Directors grant personnel access to RD information based on verification of final security eligibility, need-to-know, ensuring the individual receives an RD indoctrination briefing, has a signed SF 312, and signing the AF Form 2583. (T-1) Security Managers update the access in JPAS. (T-1)

8.7. (AFMC) Access to RD. Individuals in positions listed in DoDI 5210.02, Enclosure 4 as Air Force Officials authorized to certify access to RD may also grant personnel access to RD information. When delegated, senior organizational leader at a GSU (e.g., Division, Branch Chiefs) may grant access to RD information.

8.7.1. RD Management Official provides the RD indoctrination briefing. (T-1) The RD Management Official may delegate this to appropriately trained individuals. If delegated, keep a record of the training. (T-1)

8.7.2. Complete the appropriate blocks on the AF Form 2583, *Request for Personnel Security Action*. (T-1)

8.7.2.1. In block II, *Investigation, Clearance, Eligibility, Entry and Access Requirements*, Section 9, check either Top Secret or Secret as appropriate. (T-1)

8.7.2.2. In block VI, *Access Authorization*, check RD. (T-1)

8.7.2.3. In sections 24, 25 and 26 Date, Type Name, and Sign the form. (T-1)

8.7.2.4. In block 30 type "Member possesses final [Secret/Top Secret] clearance. Restricted Data Indoctrination Brief conducted on [date]; member signature:_____." (T-1)

8.7.3. An individual with a TOP SECRET security clearance and RD access may have access to TOP SECRET, SECRET, and CONFIDENTIAL RD/FRD information if they have a need-to-know.

8.7.4. An individual with a SECRET security clearance and RD access may have access to SECRET and CONFIDENTIAL RD/FRD information if they have a need-to-know.

8.7.5. An individual with CONFIDENTIAL security clearance and RD access may have access to CONFIDENTIAL RD/FRD information only.

8.7.6. Before granting personnel access to RD information the holder of the information has the responsibility to verify the recipient's security clearance and access eligibility. (T-0) This can be done through JPAS or by written verification from the recipient's commander or director. Commanders may delegate verification authority to a member of their unit with access to JPAS.

8.8. Access to CNWDI. Commanders and Directors grant personnel access to CNWDI based on verification of final security eligibility, a need-to-know, signed SF 312, and a RD and CNWDI Indoctrination briefing. (T-0) Commanders and Directors will:

8.8. (AFMC) Access to CNWDI. Individuals in positions listed in DoDI 5210.02, Enclosure 4 as Air Force Officials authorized to certify access to CNWDI may also grant personnel access to CNWDI. Any new accesses granted after the publication of this AFI or if there are any changes to accesses of individuals with current access, the access needs to be granted by and the AF Form 2583 needs to be signed by the commander/director or AF Certifying Official listed in DoDI 5210.02, Enclosure 4. When delegated, senior organizational leader at a GSU (e.g., Division, Branch Chiefs) may grant access to CNWDI.

8.8.1. Verify the individual has U.S. citizenship. Refer to DoDI 5210.02, Enclosure 3, for exceptions. (T-0)

8.8.2. Have the security manager verify the individual has a **final** TOP SECRET or SECRET security eligibility in JPAS (as appropriate). (T-0)

8.8.3. Provide the individual with the additional CNWDI Nuclear Information Security Indoctrination Briefing. (T-1)

8.8.4. Complete AF Form 2583, *Request for Personnel Security Action*. (T-1)

8.8.4.1. In block II, *Investigation, Clearance, Eligibility, Entry and Access Requirements*, Section 9, check either Top Secret or Secret as appropriate. (T-1)

8.8.4.2. In block VI, *Access Authorization*, check RD and CNWDI. (T-1)

8.8.4.3. In sections 24, 25 and 26 Date, Type Name, and Sign the form. (T-1)

8.8.4.4. In block 30 type "Member possesses final [Secret/Top Secret] clearance. CNWDI Indoctrination Brief conducted on [date]; member signature:_____." (T-1)

8.8.5. Verify the CNWDI access is updated in JPAS. (T-1)

8.8.6. An individual with a TOP SECRET security clearance and RD/CNWDI access may have access to TOP SECRET and SECRET RD/CNWDI information if they have a need-to-know.

8.8.7. An individual with a SECRET security clearance and RD/CNWDI access may have access to SECRET RD/CNWDI information only, if they have a need-to-know.

8.8.8. Before granting personnel access to CNWDI information the holder of the information has the responsibility to verify the recipient's security clearance and access eligibility. (T-0) This can be done through JPAS or by written verification from the recipient's commander or director. Commanders may delegate verification authority to a member of their unit with access to JPAS.

8.9. Access to DOE Sigma Information. Sensitive nuclear information may be further characterized into DOE Sigma categories to provide additional need-to-know protection of specific types of RD and FRD. Currently, there are four Sigma categories: 14, 15, 18, and 20. (See definitions in Attachment 1)

8.9.1. Access to each Sigma category is approved separately by DOE and does not permit access to any other Sigma category.

8.9.2. Personnel granted DOE Sigma 14 access are prohibited from being part of a two-person concept team that may afford access to a nuclear weapon and will have a permanent assignment limitation code applied to their personnel record. (T-1)

8.9.3. Access to DOE Sigma information may be requested and granted for a specific location, event, or project, or may be granted for personnel assigned to designated positions.

8.9.4. A listing of pre-approved billets authorized for Sigma 14 and 15 is available from AF/A10-C (usaf.pentagon.af-a10.mbx.af-a10-c-workflow).

8.9.5. Include justification in requests for access to DOE Sigma information unless the individual is assigned to a preapproved billet.

8.9.6. Commanders/Directors request and renew DOE Sigma access annually. (T-1)

8.9.7. Commanders and Directors ensure: (T-1)

8.9.7.1. The individual has a final TOP SECRET clearance and need to know.

8.9.7.2. AF/A10C is contacted (usaf.pentagon.af-a10.mbx.af-a10-c-workflow) to request DOE Form 5631.20, *Request for Visit or Access Approval*, and polygraph consent form

for access to Sigma 14 and 15. Sigma 18 and 20 do not require a polygraph. (T-1) Complete the form in accordance with the instructions at Attachment 5. (T-1) Contact AF/A10-C for questions.

8.9.7.3. The individual completes the appropriate training brief for Sigma 14 and 15. (T-1) Sigma 18 and 20 do not require a briefing.

8.9.7.4. The individual signs the training certificate for Sigma 14 and 15. (T-1)

8.9.7.5. An e-mail is sent with signed training certificate, signed polygraph consent form (for Sigma 14 and 15), completed DOE Form 5631.20, and justification, if individual is not on the pre-approved billet listing, to AF-A10C at usaf.pentagon.af-a10.mbx.af-a10-c-workflow. (T-1)

8.9.8. AF/A10-C reviews and forwards to ASD(NCB), then to HQ DOE for signature and approval.

8.9.8.1. Signed and approved forms are returned through the same offices and forwarded to the requestor.

8.9.8.2. AF/A10-C retains copies of signed and approved forms provided for those personnel granted Sigma 14.

8.9.9. Approving officials maintain the signed DOE 5631.20 and notify the individual when Sigma access has been granted.

8.10. Derivative Classification and Marking of Nuclear Information. Derivative classifiers will mark derivative classification decisions for RD/FRD/CNWDI in accordance with DoDM 5200.01, Volume 2, Enclosure 4. Derivative classifiers must:

8.10.1. Complete the derivative classification training requirements identified in **Chapter 6** of this AFI first, if not already completed. (T-1)

8.10.2. Complete RD/FRD/CNWDI derivative classification training as required by the RD Management Official. (T-1)

8.10.3. Make derivative classification decisions based on joint DOE-DoD security classification guides. Place the name of the guide or DOE source document on the "Derived From:" line. (T-1)

8.10.4. To the greatest degree possible, make every attempt to not comingle RD/FRD/CNWDI with classified national security information (NSI). (T-1)

8.10.5. Never annotate a declassification instruction on documents containing solely RD/FRD information. (T-1) If the document contains RD and NSI, FRD and NSI, or RD/FRD and NSI:

8.10.5.1. Annotate the "Declassify On:" line with "Not Applicable to RD/FRD portions" and "See source list for NSI portions." (T-0)

8.10.5.2. Include a source list for each NSI portion with declassification instructions. (T-0) The source list and declassification instruction will not be on the front page or cover of the document.

8.10.6. Comply with the marking instructions in DoDM 5200.01, Volume 2. Figures 36, 37, 38, 39, and 40 are examples of RD, FRD, CNWDI, Sigma and Sigma 14 markings. (T-0)

8.11. Reciprocity. Refer to DoDI 5210.02, Enclosure 3, Table 1. DOE, Nuclear Regulatory Commission (NRC), and DoD Clearance equivalencies.

8.12. Dissemination. For guidance on dissemination of RD information between DoD Components, DoD contractors, and DOE, NRC, and NASA personnel refer to DoDI 5210.02, Enclosure 3.

8.13. Dissemination Prohibitions. For guidance on prohibitions of RD and FRD information refer to DoDI 5210.02, Enclosure 3.

8.14. Protection and Destruction of Nuclear Information. RD/FRD/CNWDI/Sigma will be protected and destroyed in the same manner prescribed for collateral information at the same level. (T-0) Sigma information has additional protection/destruction requirements which are found in DoDI 5210.02, Enclosure 3.

8.15. Declassification of RD and FRD Documents. Air Force personnel are not authorized to declassify RD/FRD information. (T-0) Refer to DoDI 5210.02, Enclosure 3 for guidance on declassification of nuclear information.

8.16. Terminating RD/CNWDI Access for Cause. Commanders and Directors will ensure all personnel are debriefed when their access is removed for cause. (T-1) Security managers may debrief personnel when the individual no longer needs access or leaves the organization, e.g., permanent change of station or assignment, separation, or retirement. Use AF Form 2587, Security Termination Statement, for this action. (T-1)

8.16.1. Insert “Restricted Data,” “Critical Nuclear Weapons Design Information,” or both on the first line.

8.16.2. The Commander or Director terminating the access will sign the block titled, “Typed or Printed Name of Debriefer.” (T-1)

8.16.3. Ensure the access/accesses are removed from JPAS. (T-1)

CHAPTER 9

NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION

9.1. General NATO Information. This chapter identifies the limited number of differences between the security measures followed by the U.S. for protection of its national classified information and those mandated or recommended by NATO security documents. For questions concerning security procedures consult with the organization's NATO Subregistry or Control Point Officer or the Wing Information Protection Office.

9.1.1. The most current United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN) Instruction when further guidance beyond this instruction is needed.

9.1.2. Sample NATO security briefings and forms are available on the CUSR website: **https://secureweb.hqda.pentagon.mil/cusr/forms.aspx**. This includes personnel granted access to the Secret Internet Protocol Router Network (SIPRNET), when their enclave has been approved for NATO, or any other classified networks which have been approved for NATO.

9.1.2. **(AFMC)** To verify if the enclave has been approved for NATO call your servicing NATO Subregistry or NATO Control Point. You may also call the CUSR at 703-545-7159 or email **usarmy.pentagon.hqda-ita.mbx.cusr-central-us-registry@mail.mil**.

9.1.2. **(WRIGHTPATTERSONAFB)** AFIMSC, Det 6, is the servicing NATO subregistry for AFMC and Wright-Patterson AFB.

9.1.3. All cleared Air Force personnel will receive a NATO briefing to facilitate potential access to NATO classified information and acknowledge, in writing, the briefing using the NATO Brief/Rebrief/Debrief form found on the CUSR website. (T-1)

9.1.3. **(AFMC)** For individuals not requiring access to NATO information, this briefing can be accomplished, acknowledged in writing, and recorded during the initial and annual refresher security training required in **Chapter 6**. For individuals requiring access to NATO follow the requirements of paragraph 9.2.

9.1.3. **(WRIGHTPATTERSONAFB)** All cleared personnel will receive a NATO awareness briefing and acknowledge the briefing in writing. The briefing can be included in the unit's normal initial and annual refresher security training. The briefing can be acknowledged using a sign-in roster or the Central US Registry (CUSR) form.

9.2. NATO Indoctrination Process. Commanders and Directors grant U.S. personnel access to NATO information based on verification of security eligibility and a need-to-know. (T-1) This includes personnel granted access to the SIPRNET when their enclave has been approved for NATO, or any other classified networks which have been approved for NATO. This action cannot be delegated. Commanders and Directors will:

9.2. (AFMC) NATO Indoctrination Process. Any new accesses granted since the date of this AFI or if there are any changes to accesses of individuals with current access, the access needs to be granted by and the AF Form 2583 needs to be signed by the commander/director. When

delegated, senior organizational leader at a GSU (e.g., Division, Branch Chiefs) may grant access to NATO information.

9.2.1. Verify the individual has the proper security eligibility (clearance) and accesses, if needed, for the level of NATO information required. (T-0) Complete all appropriate blocks of the AF Form 2583 and document the access for NATO. In block VII annotate the specific access (CTS, NS, or CTSA). (T-1) For access to:

9.2.1.1. COSMIC TOP SECRET (CTS) the individual must possess a final U.S. Top Secret security clearance. (T-0)

9.2.1.2. NATO SECRET (NS) and NATO CONFIDENTIAL (NC) the individual must possess a final U.S. Secret security clearance. (T-0)

9.2.1.3. CTS ATOMAL (CTSA) and NS ATOMAL the individual must possess a final U.S. Top Secret security clearance and read in to Restricted Data in accordance with **Chapter 8**. (T-0)

9.2.1.4. NC ATOMAL the individual must possess a final U.S. Secret security clearance and read in to Restricted Data in accordance with **Chapter 8**. (T-0)

9.2.1.5. NATO Restricted (NR) no security clearance is required.

9.2.2. Verify the individual was provided a security briefing regarding the protection of NATO classified information. (T-0) This includes individuals granted access to NR in 9.2.1.5. above.

9.2.3. Ensure the AF Form 2583 is completed:

9.2.3.1. In block II, Investigation, Clearance, Eligibility, Entry and Access Requirements, Section 9, check either Top Secret or Secret as appropriate. (T-1)

9.2.3.2. In block VI, Access Authorization, check NATO. (T-1)

9.2.3.3. In sections 24, 25 and 26 Date, Type Name, and Sign the form. (T-1)

9.2.3.4. In block 30 type “Member possesses final [Secret/Top Secret] clearance and received the NATO Security Briefing on [date]; member signature:_____” (T-1)

9.2.3.5. For access to ATOMAL: In block 30 type “Member possesses final [Secret/Top Secret] clearance and received the ATOMAL Security Briefing on [date]; member signature: _____” (T-1)

9.2.3.6. ATOMAL access requires an annual refresher briefing: In block 30 type “Member received annual ATOMAL Security Briefing on [date]; member signature:_____” (T-1)

9.2.4. Ensure the NATO access is updated in the JPAS. (T-1)

9.3. Granting U.S. Personnel Access to NATO Unclassified. Access to NATO Unclassified (NU) does not require indoctrination per paragraph 9.2 of this chapter. Grant access to NU information to personnel when the need is for official NATO purposes only. (T-0)

9.4. Terminating U.S. Personnel Access to NATO Information . Commanders and Directors will terminate an individual's access to NATO when no longer needed. Commanders and Directors will:

9.4. (AFMC) Terminating U. S. Personnel Access to NATO Information. Commanders and Directors must terminate an individual's access to NATO when their access is removed for cause. Security managers may terminate access when individuals depart the organization for separation, retirement, or permanent change of station. See paragraphs 5.1.1.3, 5.1.1.4, and 8.16. Retain the AF Form 2587 or CUSR debriefing form for two years. **(T-2).**

9.4.1. Brief the individual their access has been terminated. (T-1)

9.4.2. Ensure the individual acknowledges a statement of termination on an AF Form 2587. (T-1) If the individual refuses to sign the statement, have a witness sign a statement indicating the individual was informed the access was terminated. (T-1)

9.4.3. Verify the NATO access has been removed from JPAS. (T-1)

9.5. Access to NATO Information for Citizens of NATO Nations. Cleared citizens of NATO member nations may have access to NATO information when written assurance has been received from the appropriate home country government authority validating access and need-to-know.

9.6. Access to NATO Information for non-U.S. and non-NATO Nation citizens. Non-U.S. and non-NATO nation citizens may be granted access to NATO information if an approved Limited Access Authority (LAA) with a NATO mission essential need-to-know exists. Refer to AFI 31-501 (CHANGING TO AFI 16-1405)), *Personnel Security Management*, (will change to AFI 16-1405) for more information on LAAs. Refer to the current USSAN for instruction on granting access to non-NATO personnel.

9.7. NATO Security Clearance Certificates . Access granting authorities provide NATO security clearance certificates when Air Force personal are assigned to a NATO billet, on temporary duty to a NATO organization, or when requested. (T-1) Refer to the current USSAN instruction for a sample certificate.

9.8. Use of Coversheets. Use the appropriate NATO coversheet to protect NATO information when outside of approved storage containers and areas. (T-1) NATO cover sheets can be obtained from **https://secureweb.hqda.pentagon.mil/cusr/forms.aspx**.

9.9. Storage and U.S. Information Systems (IS) Handling NATO Classified Information. Refer to the current USSAN for storage requirements and accrediting of IS systems to include: user, technicians, and system administrators access; authorization, handling, marking and processing NATO information in electronic form; and process for handling data spills, storage media and websites.

9.10. Marking, Downgrade/Declassification, Reproduction, Transmission, Destruction of NATO Information. For marking instructions refer to DoDM 5200.01, Volume 2 and the current USSAN instruction.

9.10.1. Send challenges to classification of NATO classified information through Information Security Program channels to SAF/AAZ.

9.10.1. **(AFMC)** Center CIPs will send challenges to HQ AFMC/IP. HQ AFMC/IP will send challenges to SAF/AAZ. **(T-2).**

9.10.2. For downgrade/declassification, reproduction, transmission, and destruction of NATO information refer to the current USSAN instruction and DoDM 5200.01, Volume 3.

Chapter 10

AIR FORCE INFORMATION SECURITY PROGRAM SELF-INSPECTION AND OVERSIGHT

10.1. General . The Senior Agency Official (SAF/AA) is required to establish a self-inspection program and report annually on a Fiscal Year (FY) basis to the Information Security Oversight Office (ISOO) and Office of Under Secretary of Defense, Intelligence (OUSD(I)) on the program's adherence to the principles and requirements of EO 13526, *Classified National Security Information*, DoDM 5200.01, Volumes 1-4. The SPE and Wing Commander's assist the Senior Agency Official with the development of the reports as part of the program oversight hierarchy.

10.1. (AFMC) General. Center/CVs also assist the Senior Agency Official with the development of the reports as part of the program oversight hierarchy. **(T-2).**

10.1.1. SAF/AAZ establishes Air Force-level criteria.

10.1.2. MAJCOM/DRU Director, Information Protection develops command specific criteria.

10.1.2.1. **(Added-AFMC)** Center CIP may also develop Center specific criteria.

10.1.3. The Wing Chief, Information Protection conducts the Wing's self-inspection IAW DoDM 5200.01, Volume 1 and this AFI and summarizes findings in six areas: original classification, derivative classification, safeguarding, security violations, and security education and training. (T-1)

10.1.3. **(AFMC)** Center CIPs may also conduct Center self-inspections.

10.1.3.1. **(Added-AFMC)** Center/Wing self-inspections include all organizations within the Center/Wing, to include all tenant units the Center/Wing CIP supports through a host tenant support agreement, MOU, or MOA. Send discrepancies of non-AFMC organizations to HQ AFMC/IP. **(T-2).**

10.1.4. AFDO conducts self-inspections of the Air Force's declassification efforts IAW DoDM 5200.01, Volume 1 and summarizes findings.

10.2. Frequency. The Wing Chief, Information Protection will conduct the self-inspection annually and have it completed by the end of the FY IAW DoDM 5200.01, Volume 1. (T-0)

10.3. Execution. The Wing Chief, Information Protection and AFDO will complete the self-inspection using this AFI and DoDM 5200.01, Volumes 1-4. (T-1) The Wing Chief, Information Protection has responsibility for developing the report for areas in paragraph 10.3.1 – 10.3.6. (T-1) AFDO has responsibility for developing the report for paragraph 10.3.5 as it relates to training of declassification authorities and paragraph 10.3.7.

10.3. (AFMC) Execution. To accomplish the annual Center/Wing self-inspection, the Center or Wing IP Offices will inspect all organizations within their Center/Wing and any other organizations being supported through host tenant support agreements, MOUs, MOAs, or Center supplements. AFMC Center/Wing CIPs should ask assistance from other AF or AFMC CIPs to conduct these self-inspections at GSUs. The Center/Wing CIP also has responsibility for

inspecting the areas in AFMC paragraph 10.3.8. Center/Wing IG inspections, in accordance with AFI 90-201, can be used in place of these Center/Wing self-inspections as long as all the required information is collected to write the Center/Wing's Annual Self-Inspection Report. See Attachment 10 for further Center/Wing self-inspection requirements and a sample report. Security managers will retain the current self-inspection report until replaced with a new report. **(T-2).**

10.3. (WRIGHTPATTERSONAFB) 88 ABW/IP will conduct Information Protection Security Reviews (IPSR) of all organizations located on Wright-Patterson AFB, per applicable host-tenant support agreements. IPSRs of AFMC-assigned organizations serviced by 88 ABW/IP, but are not physically located on Wright-Patterson AFB, are the responsibility of the respective Center.

10.3.1. Original Classification. Determine if the wing supports original classification process. DoDM 5200.01, Volumes 1 and 2, and this AFI are the authoritative guidance for original classification. If so:

10.3.1.1. Validate OCA(s) have completed initial/refresher training. (T-0)

10.3.1.2. Review all original classification material in both document and electronic form generated by wing OCAs and evaluate if all required markings are annotated IAW DoDM 5200.01, Volume 2. (T-0) Do not count discrepancies identified by OCA decisions outside the wing's scope. Notify the MAJCOM/DRU Director, Information Protection of the discrepancies when discrepancies are discovered on original classification material belong to outside OCAs.

10.3.1.3. Determine the number of security classification guides and validate the guides have been distributed IAW DoDM 5200.01, Volume, Enclosure 6. (T-0)

10.3.1.4. Any other areas required by this AFI or DoDM 5200.01, Volumes 1-4.

10.3.2. Derivative Classification. Only evaluate derivative classification decisions made by wing personnel. (T-1) If discrepancies are identified from organizations outside the wing, do not count them toward the wing's report and notify the MAJCOM/DRU Director, Information Security. DoDM 5200.01, Volumes 1 and 2, and this AFI are the authoritative guidelines for inspecting this area.

10.3.2.1. Sample 20% of each organization's derivative classifiers. (T-1)

10.3.2.2. Determine if derivative classifiers have current training documented. (T-0)

10.3.2.3. Determine if derivative classifiers have access to security classification guides, especially DoD-DOE security classification guides if applicable. (T-0)

10.3.2.4. Review all required markings for derivative classification decisions in both documented and electronic media. (T-0)

10.3.2.5. Determine if derivative classifiers know the procedures for challenging classification. (T-0)

10.3.2.6. Any other areas required by this AFI or DoDM 5200.01, Volumes 1-4.

10.3.3. Safeguarding. Identify discrepancies based upon the level of information each unit is required to protect IAW with standards of this AFI and DoDM 5200.01, Volumes 3 and 4. (T-0)

10.3.4. Security Violations. All wing security violations and infractions within 12 months of the date of assessment will be evaluated. DoDM 5200.01, Volume 3 and this AFI are the authoritative guidance.

10.3.4.1. The number of security violations and infractions. (T-0)

10.3.4.2. Determine if corrective actions have been taken to prevent further occurrences. (T-0)

10.3.5. Management and Oversight. This applies to all areas of management and oversight to include security managers, security specialist, and any other person whose duties significantly involve managing and overseeing classified information. The authoritative guidance for this area is this AFI and DoDM 5200.01, Volume 3, Enclosure 5.

10.3.6. Security Education and Training. Areas of focus will be OCA, derivative classification, security managers, security specialist, initial and refresher training, and declassification training. The authoritative guidance for this area is this AFI and DoDM 5200.01, Volumes 1 and 3.

10.3.7. Declassification. Inspect all declassification systems, process, and procedures IAW this AFI and DoDM 5200.01, Volumes 1-3.

10.3.8. **(Added-AFMC)** Center/Wing self-inspections will include Personnel and Industrial Security, NATO, and CNWDI/RD/FRD requirements. See **Attachment 10**. **(T-2).**

10.4. Documentation. Document the annual self-inspection report by providing an overall analysis of each area. (T-1) Include any findings and recommended corrective actions under each area, if applicable.

10.4. (AFMC) Documentation. HQ AFMC/IP will provide Center/Wing CIPs the format for the annual self-inspection report to ISOO and OUSD(I). Center CIP will consolidate their Wing's reports into one Center report, obtain Center/CV's signature, and forward report to HQ AFMC/IP. HQ AFMC/IP will consolidate the Center reports into one AFMC report, obtain AFMC/CV signature, and forward report to SAF/AAZ. **(T-2).**

10.4.1. Include the name of the individual and contact information responsible for answering questions regarding the report. (T-1)

10.4.2. Ensure the Wing Commander signs the report. (T-1)

10.4.2. **(AFMC)** Ensure the Center/CV signs the report. **(T-2).**

10.4.3. MAJCOM/DRU Directors, Information Protection consolidate wing data and submit them to SAF/AAZ when requested.

10.5. Self-Assessments . Commanders and Directors at all levels, to include the Wing Chief, Information Protection, will conduct annual program self-assessment IAW AFI 90-201, *The Air Force Inspection System*, using the Management Internal Control Tool (MICT) checklist. (T-1)

10.5. (AFMC) Self-Assessment. Conduct a separate self-assessment at GSUs. GSU self-assessments can be recorded within their parent's self-assessment or separately. **(T-2).**

Chapter 11

STANDARD FORM (SF) 311, AGENCY SECURITY CLASSIFICATION MANAGEMENT PROGRAM DATA

11.1. General. Each FY the Senior Agency Official reports information related to classification management to the Information Security Oversight Office (ISOO) and Office of Under Secretary of Defense, Intelligence (OUSDI). This is done on the SF 311 and is commonly referred to as SF 311 reporting. A copy of the SF 311 can be obtained from the MAJCOM/DRU or Wing Information Protection Office.

11.1.1. The report is completed in nine parts, but may be less or more depending on the specific tasking from ISOO or OUSD(I).

11.1.2. Each part, its office of responsibility, and instructions for completing each part are identified below.

11.1.3. SAF/AAII and MAJCOM/DRU Director, Information Protection compares the report to the previous year's submissions on behalf of SAF/AAI and the MAJCOM/DRU SPE.

11.1.3. **(AFMC)** Center and Wing CIPs compares the report to the previous year's submissions on behalf of Center/CV and Wing Commander.

11.1.3.1. Explain large deviations from the previous years reported numbers in Part I: Explanatory Comments.

11.1.3.2. Submit the SF 311 report no later than November 5 following the completion of the FY.

11.1.3.2. **(AFMC)** Centers will forward their SF 311 report to HQ AFMC/IP by 5 October of each year.

11.1.4. SAF/AAI and MAJCOM/DRU SPE submit SF 311 reports through SAF/AA.

11.1.4. **(AFMC)** Center CIP will consolidate their Wing's reports into one Center report and submits results to HQ AFMC/IP.

11.2. Part A and B. Identifying Information and Officials with Original Classification Authority. These parts are completed by SAF/AAZ. SAF/AAZ maintains the Air Force Original Classification Authority (OCA) listing by position and classification authority.

11.3. PART C. Original Classification Decisions. OCAs complete this part by counting **all** original classification decisions. (T-0)

11.3.1. Do not count products classified by another OCA, reproductions or copies, or instant messages.

11.3.2. Security Classification Guides. Count each guide as 1 decision. Do not count each paragraph or subsection of a guide as a decision.

11.3.2.1. Count all new original decisions made during revisions to a guide. If no new decisions are made do not count.

11.3.2.2. Do not count 5-year reviews as a decision unless a new decision is made.

11.3.3. Count all memoranda that issue original classification guidance. If referencing the original memorandum in a new memorandum do not count this as a classification decision. However, count it as a derivative classification decision per paragraph 11.4.

11.3.4. Count all original classification decisions in publications and plans. If these publications or plans are updated or revised, only count the update or revision if new classification guidance is issued.

11.3.5. E-mails. Count the initial e-mail with an original classification decision and any reply or forward that includes **additional** classification decisions. Do not count e-mail used as a transmittal vehicle for classified attachments and contains no classified information itself.

11.3.6. Web Pages. Each web page created during the reporting period that has an original classification decision regardless of how many times it was modified or updated. Only count modifications or updates if new original classification decisions are made.

11.3.7. Blogs. Every individual blog entry made by the OCA that constitutes an original classification decision. Do not count entries made by other OCAs or agencies.

11.3.8. Wiki Articles. Count each wiki article that contains original classification decisions regardless of how many times it is modified or updated by other users. Only count modifications or updates if new original classification decisions are made.

11.4. Part D. Derivative Classification Decisions. Wing Information Protection Offices sample 20% of the derivative classifier population over a 2-week period during the FY (April–June). Once the numbers are received; multiply the results by 5. This will provide a sample of 100% of the population. Then multiply this number by 26 to determine the FY's derivative classification decisions. (T-1)

11.4.1. Only count the products developed by the derivative classifier.

11.4.2. E-mails. Count the initial e-mail and any e-mail reply or forward that include **additional** derivative classification decisions. Do not count e-mail used as a transmittal vehicle for classified attachments and contains no classified information itself.

11.4.3. Web Pages. Each web page created during the reporting period that has a derivative classification decision and only count modifications or updates if new derivative classification decisions are made. This includes subpages.

11.4.4. Blogs. Every individual blog entry made by the derivative classifier that constitutes a derivative classification decision. Do not count entries made by other derivative classifiers or agencies.

11.4.5. Wiki Articles. Each wiki article that contains derivative classification decisions regardless of how many times the wiki article is modified or updated by other users. Only count modifications or updates if new derivative classification decisions are made.

11.4.6. Instant Messages. Do not count instant messages.

11.5. Parts E, F, and G. Mandatory Declassification Review Requests and Appeals, Mandatory Declassification Review Decisions in Pages, and Automatic, Systematic and Discretionary Declassification Decisions are completed by SAF/AAI. Any organization within the Air Force authorized to make these decisions reports directly to SAF/AAI.

11.6. Part H. Internal Agency Oversight. Directors, Information Protection report the number of self-inspections, SAF/AAI report numbers relevant to challenges, and OCAs report numbers relevant to the number of security classification guides.

11.6.1. Only count wing-level self-inspections.

11.6.1. **(AFMC)** Count Center and Wing-level self-inspections.

11.6.1.1. Only one self-inspection is required per year. If a MAJCOM/DRU requires more inspections placed the total number on line 47 and add Explanatory Comments in Part I. For example: if AFSOC has 84 wings, then 84 self-inspections would be reported.

11.6.1.2. Do not count squadron, group, or tenant unit under a wing host/tenant agreement as separate self-inspections.

11.6.1.3. Do not count minor inspections like routine after-hours security checks.

11.6.2. SAF/AAI reports numbers related to challenges.

11.6.2.1. For block 48 count any internal or external classification challenges that may have been processed under section 1.8 of E.O. 13526 and 32 CFR 2001.14. Do not count requests received under FOIA or MDR provisions of E.O. 13526.

11.6.2.2. For blocks 49 and 50 report the number of classification challenges where the classification status was either fully affirmed or overturned in whole or part.

11.6.3. Report the number of security classification guides owned by the OCA that are still currently in use. ***This is not the number of guides created during the year; this is the total number of guides.***

11.7. Part I. Explanatory Comments. This part is used to explain any significant changes in trends/numbers from the previous year's reporting. SAF/AAI, OCAs, MAJCOM/DRU SPE, and SAF/AAZ are responsible for annotating this section. Directors, Information Protection will roll up all numbers and comments into one MAJCOM/DRU report.

11.7. (AFMC) Part I. Center and Wing CIPs will annotate this section for their Center/CV and Wing Commander. Center CIPs will roll up all numbers and comments into one Center report.

PATRICIA J. ZARODKIEWICZ
Administrative Assistant

(AFMC)

DAVID D. DAY, GS-15, DAF
Director of Information Protection

(WRIGHTPATTERSONAFB)

DANNY R. MYERS
Director, Information Protection

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 5210.50, *Management of Serious Security Incidents Involving Classified Information,* October 27, 2014

(Added-WRIGHTPATTERSONAFB) AFMAN 33-363, *Management of Records*, 1 March 2008

(Added-AFMC) AFPAM 63-113, *Program Protection Planning for Life Cycle Management*, 17 October 2013

(Added-AFMC) AFI16-1404, *Air Force Information Security Program,* 29 May 2015

(Added-AFMC) DoDD 5000.01, *Defense Acquisition System*, 12 May 2015

DoDD 5205.07, "*Special Access Program (SAP) Policy*," July 1, 2010

DoDD 5230.09, *Clearance of DoD Information for Public Release*, August 2, 2008, Certified Current through August 22, 2015

DoDD 8100.02, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*, April 14, 2004, Certified current as of April 23, 2007

DoDI 3305.13, *DoD Security Education, Training, and Certification,* February 13, 2014

DoD 5200.08, *Physical Security Program,* April 9, 2007 Incorporating Change 1, May 27, 2009

(Added-AFMC) DoDI 5000.02, *Operation of the Defense Acquisition System*, 7 January 2015

(Added-AFMC) DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E),* 28 May 2015

(Added-AFMC) DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),* 5 November 2012

DoDI 5210.02, *Access and Dissemination of RD and FRD*, June 3, 2011

DoDI 5210.83, *DoD Unclassified Controlled Nuclear Information (UCNI),* July 12, 2012

DoD 3305.13-M, *DoD Security Accreditation and Certification*, March 14, 2011

DoDM 5200.01, Volume 1, *DoD Information Security Program*: *Overview, Classification, and Declassification,* February 24, 2012

DoDM 5200.01, Volume 2, *DoD Information Security Program*: *Marking of Classified Information*, 24 February 2012, Incorporating Change 2, March 19, 2013

(Added-WRIGHTPATTERSONAFB) DODM 5200.01, Volume 3, *DOD Information Security Program: Protection of Classified Information*, 24 February 2012

DoDM 5200.01, Volume 3, *DoD Information Security Program*: *Protection of Classified Information*, 24 February 2012, Incorporating Change 2, March 19, 2013

DoDM 5200.01, Volume 4, *DoD Information Security Program*: *Controlled Unclassified Information (CUI)*, February 24, 2012

DoDM 5200.45, *Instructions for Developing Security Classification Guides*, April 2, 2013

DoDM 5205.07, Volume 4, *Special Access Program (SAP) Security Manual: Marking*, October 10, 2013

AFI 31-101, *Integrated Defense*, October 9, 2009, Incorporating Through Change 2, March 7, 2013

(Added-WRIGHTPATTERSONAFB) AFI 16-1406_AFMCSUP, *Air Force Materiel Command Industrial Security Program,* 3 June 2016

(Added-WRIGHTPATTERSONAFB) AFI 16-1406, *Air Force Industrial Security Program,* 25 August 2015

(Added-WRIGHTPATTERSONAFB) AFI 16-1404_AFMCSUP, *Air Force Materiel Command Information Security Program*, 17 February 2016

(Added-WRIGHTPATTERSONAFB) AFI 16-1404, *Air Force Information Security Program*, 29 May 2015

(Added-AFMC) AFI 25-201, *Intra-Service, Intra-Agency, and Inter-Agency Support Agreements Procedures*, 18 October 2013

AFI 31-501 (CHANGING TO AFI 16-1405)), *Personnel Security Program Management*, January 27, 2005, Incorporating through Change 2, November 29, 2012

AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, February 18, 2014

(Added-WRIGHTPATTERSONAFB) AFI 31-501, *Personnel Security Program Management,* 27 January 2005

(Added-WRIGHTPATTERSONAFB) AFI 31-501_AFMCSUP, *Personnel Security Program Management,* 21 July 2008

AFI 33-115, *Air Force Information Technology (IT) Service Management,* September 16, 2014

(Added-AFMC) AFI 63-101/20-101, *Integrated Life Cycle Management (ILCM),* 7 March 2013

AFI 90-201, *The Air Force Inspection System*, August 2, 2013

AFI 90-301, *Inspector General Complaints Resolution,* August 23, 2011

AFMAN 33-282, *Computer Security (COMPUSEC)*, March 28, 2012, Incorporating Change 1, January 15, 2015

AFMAN 33-360, *Publications and Forms Management*: *Communications and Information*, September 25, 2013

(Added-WRIGHTPATTERSONAFB) WRIGHTPATTERSONAFBVA 31-10, *STOP Do Not Use This Machine for Classified Reproduction,* 21 February 2008

(Added-WRIGHTPATTERSONAFB) WRIGHTPATTERSONAFBVA 31-9, *Caution: Authorized for Reproduction of Classified Material,* 21 February 2008

AFPD 16-14, *Security Enterprise Governance*, July 24, 2014

Prescribed Forms

(**Added-WRIGHTPATTERSONAFB**) WRIGHTPATTERSONAFB 1404, *Security Manager Appointment Record*

(**Added-WRIGHTPATTERSONAFB**) WRIGHTPATTERSONAFB 1414, *Stored Information Notice*

(**Added-WRIGHTPATTERSONAFB**) WRIGHTPATTERSONAFB 1475, *Classified Storage/Conference Room Certification*

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

(**Added-AFMC**) AF Form 2427, *Lock and Key Control Register*

(**Added-AFMC**) AF Form 1565, *Entry, Receipt and Destruction Certificate*

(**Added-AFMC**) AF Form 144, *TOP SECRET Access Record and Cover Sheet*

(**Added-AFMC**) AF Form 143, *Top Secret Register Page*

AF Form 1297, *Temporary Issue Receipt*

AF Form 2583, *Request for Personnel Security Action*

AF Form 2587, *Security Termination Statement*

(**Added-AFMC**) DD Form 2501, *Courier Authorization*

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

DD Form 2024, *DoD Security Classification Guide Data Elements*

DOE Form 5631.20, *Request for Visit or Access Approval*

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

SF 311, *Agency Security Classification Management Program Data*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Checksheet*

(**Added-WRIGHTPATTERSONAFB**) SF Form 311, *Agency Security Classification Management Program Data*

(**Added-WRIGHTPATTERSONAFB**) SF Form 700, *Security Container Information*

Abbreviations and Acronyms

ACCM—Alternative Compensatory Control Measures

AFDO—Air Force Declassification Office

AFI—Air Force Instruction

AFMAN—Air Force Manual

(Added-AFMC) AFMC—Air Force Materiel Command

AFPD—Air Force Publication Directive

AFRC—Air Force Reserve Command

ANG—Air National Guard

(Added-AFMC) CIP—Chief, Information Protection

CMI—Classified Message Incident

CNWDI—Critical Nuclear Weapons Design Information

CUI—Controlled Unclassified Information

CUSR—Central United States Registry

DEA—Drug Enforcement Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DOE—Department of Energy

DRU—Direct Reporting Unit

EA—Executive Agent

EPL—Evaluated Products List

FOA—Forward Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FRD—Formerly Restricted Data

(Added-AFMC) GSU—Geographically Separated Unit

IA—Information Assurance

(Added-AFMC) IP—Information Protection

JPAS—Joint Personnel Adjudication System

LES—Law Enforcement Sensitive

MAJCOM—Major Command

MDR—Mandatory Declassification Review

(Added-AFMC) MOA—Memorandum of Agreement

(Added-AFMC) MOU—Memorandum of Understanding

NATO—North Atlantic Treaty Organization

NSI—National Security Information

OCA—Original Classification Authority

OPR—Office of Primary Responsibility

RD—Restricted Data

SAO—Senior Agency Official

SAP—Special Access Program

SCI—Sensitive Compartmented Information

SFPC—Security Fundamentals Professional Certification

SNM—Special Nuclear Material

SPE—Security Program Executive

SSO—Special Security Officer

SPēD—Security Professional Education Development

TSCA—Top Secret Control Assistant

TSCO—Top Secret Control Officer

UCNI—Unclassified Controlled Nuclear Information

Terms

Classified Meeting or Conference—includes seminars, exhibits, symposia, conventions, training classes, workshops, or other such gatherings, during which classified information is disseminated. This does not apply to operational meetings conducted in combat situations, classes conducted by DoD schools, or gatherings of personnel of a DoD Component and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific U.S. Government contract, program, or project, or routine day-to-day staff meetings or discussion within an office on specific topics.

Classified Message Incidents (CMI)—A higher classification level of data is transferred to a lower classification level system/device via messaging systems, e.g., e-mail, instant messaging, etc.

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.

Derivative Classification—Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Includes the classification of

information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Inadvertent Spillage or Unauthorized Disclosure of Classified Information on Information Systems— An incident where a person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring while using an information system (e.g., a person reasonably relied on improper markings).

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.

Need—To-Know - A determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. For contractors their need-to-know is their requirements of the contract and DD Form 254.

Negligent Discharge of Classified Information—term based on the familiar firearms term "Negligent Discharge" to connote the seriousness of a spillage or unauthorized disclosure of classified information while using an information system.

Negligent Spillage or Unauthorized Disclosure of Classified Information on Information Systems—An incident where a person acted unreasonably in causing a spillage or unauthorized disclosure while using an information system (e.g., a careless lack of attention to detail, or reckless disregard for proper procedures).

Nuclear Weapon Data (NWD)—RD and FRD concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices.

Original Classification—Initial determination information requires, in the interests of national security, protection against unauthorized disclosure.

(Added-AFMC) Program Protection—Comprehensive effort that encompasses the security, technology transfer, intelligence, and counterintelligence processes through the integration of embedded system security processes, security manpower, equipment and facilities. It is the integrating process for managing risks to AF warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle. Program protection procedures and program protection planning throughout the life cycle are discussed in detail in AFPAM 63-113, *Program Protection Planning for Life Cycle Management*.

Senior Agency Official—The SECAF designated position for directing, administering, and overseeing the Air Force Information Security Program in accordance with DoDM 5200.01, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification,*

Enclosure 2, SAF/AA is the Air Force Senior Agency Official. There are no other Senior Agency Officials within the Air Force.

Security—in-Depth – Determinations by the senior agency official that a facility's security program consists of layered and complimentary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility. Air Force facilities located on installations with a perimeter fence or other type of legal boundary, perimeter access controls for employees and visitors, law enforcement and security patrols, and have locking doors and or another type of access controls have security-in-depth. All other determinations are made the SPE or Wing Commander for storage of Top Secret, Secret, and Confidential information.

Sigma 14—The category of sensitive information (including bypass scenarios) concerning the vulnerability of nuclear weapons to a deliberate unauthorized nuclear detonation.

Sigma 15—The category of sensitive information concerning the design and function of nuclear weapons use control systems, features, and components. This includes use control for passive and active systems. It may include weapon design features not specifically part of a use control system. Not all nuclear weapons use control design information is Sigma 15.

Sigma 18—Nuclear weapons data that includes information that would allow or significantly facilitate a proliferate nation or entity to fabricate a credible nuclear weapon or nuclear explosive based on a proven, certified, or endorsed US nuclear weapon or device. This information would enable the establishment or improvement of nuclear capability without nuclear testing or with minimal research and development.

Sigma 20—The category of nuclear weapons data that pertains to sensitive improvised nuclear device information.

Unclassified Controlled Nuclear Information (UCNI)—relates to physical protection of DoD special nuclear material (SNM), SNM equipment, and SNM facilities, including unclassified information on the physical protection of nuclear weapons containing SNM in the custody of DoD.

Willful Spillage or Unauthorized Disclosure of Classified Information on Information Systems— An incident where a person purposefully disregards DoD or Air Force Security or information safeguarding policies or requirements (e.g., intentionally bypassing a known security control).

Attachment 2

AIR FORCE SECURITY CLASSIFICATION GUIDE TEMPLATE

A2.1. This template is the Air Force standard for security classification guides (SCG). It can also be used for development of security declassification guides. Every attempt should be made to keep SCGs unclassified. When unclassified mark the guide "For Official Use Only (FOUO)." SCG format variations are authorized. Refer to DoDM 5200.45, Appendix to Enclosure 4, for format and for additional information not covered by this attachment.

A2.2. Cover Page (Figure A2.F1): include the following elements.

A2.2.1. Overall classification. FOUO or highest classification level. Mark IAW with DoDM 5200.01, Volume 2 for classified guides and Volume 4 for FOUO guides.

A2.2.2. Name of the program, systems, plan, project, etc., all in capital letters followed by SECURITY CLASSIFICATION GUIDE or SECURITY DECLASSIFICATION GUIDE as appropriate.

A2.2.3. DATE: date of the original classification decision. This date is important because it establishes the original classification of the information. This date must be on all guides that are revised. (T-1) The original classification decision date helps determine if information should be exempted prior to it reaching 25 year declassification date.

A2.2.4. REVISION DATE: is placed below the original classification date. Do not remove the original classification date.

A2.2.5. ISSUED BY: issuing office organization name, MAJCOM, and address.

A2.2.6. APPROVED BY: OCA name and title, or personal identifier.

A2.2.7. Supersession statement, if the guide supersedes a previous version. For example: "This guide supersedes Project Apple Security Classification Guide issued 13 March 2009."

A2.2.8. Distribution Statement IAW AFI 61-204, *Disseminating Scientific and Technical Information*.

A2.3. FIRST PAGE (A2.F2): include the following elements.

A2.3.1. DESCRIPTION: provide a short synopsis of the technology, system, plan, program, project, or mission.

A2.3.2. "Coordinated by" and the program/project director's name, title, and signature. For example: "Approved by Katie Smith, Program Director."

A2.3.3. "Approved by" and the OCA's name, title, and signature. For example: "Approved by Michael Brown, Director."

A2.4. The next page shall be "SECTION 1, GENERAL INSTRUCTIONS" (Figure A2.F3). (T-1) Add details for each of the following subordinate paragraphs.

A2.4.1. "Purpose."

A2.4.2. "Authority."

A2.4.3. "Office of Primary Responsibility (OPR)." Include mailing address and telephone number and, when appropriate, an email address (workflow or personal).

A2.4.4. "Classification Challenges." Include whom to contact and how.

A2.4.5. "Classification Recommendations." Include whom to contact for new classification recommendations.

A2.4.6. "Reproduction, Extraction, and Dissemination."

A2.4.7. "Public Release."

A2.4.8. "Release of Program Data on the Internet." Include this advisory: "Extreme care must be taken when considering information for release onto publicly accessible or unprotected Internet sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. Internet technology search and data mining capabilities must be assessed from a risk-management perspective. Information intended for publication on publicly accessible or unprotected Internet sites must be cleared for public release prior to publication according to AFI 35-102, *Security and Policy Review Process*. Also refer to AFI 35-107, *Public Web Communications*. If there are any doubts, do not release the information."

A2.4.9. "Release of Classified and Controlled Unclassified Information to Foreign Governments or Their Representatives."

A2.4.10. "Definitions."

A2.4.11. Other entries may also be appropriate.

A2.5. SCG content may also need to include "SECTION 2, OVERALL EFFORT" (Figure A2.F4). Add details for each of the following subordinate paragraphs.

A2.5.1. "Identification."

A2.5.2. "Goal, Mission, Purpose."

A2.5.3. "End Item."

A2.6. SCG content shall include classification/declassification tables broken out into sections. (T-1) Sections or titles may vary and may include some or all of the following sections.

A2.6.1. "SECTION 3 – PERFORMANCE AND CAPABILITIES" (Figure A2.F5).

A2.6.2. "SECTION 4 – SPECIFICATIONS" (Figure A2.F6).

A2.6.3. "SECTION 5 – CRITICAL ELEMENTS" (Figure A2.F7).

A2.6.4. "SECTION 6 – VULNERABILITIES AND WEAKNESSES" (Figure A2.F8).

A2.6.5. "SECTION 7 – ADMINISTRATIVE DATA" (Figure A2.F9).

A2.6.6. "SECTION 8 – HARDWARE" (Figure A2.F10).

A2.6.7. The classification/declassification tables (Figure A2.F11) for each section generally include the following columns:

A2.6.7.1. “Topic” or “Information Revealing” or similar.

A2.6.7.2. “Classification.”

A2.6.7.3. “Reason.”

A2.6.7.4. “Declassify On.”

A2.6.7.5. “Remarks.”

A2.6.7.6. Should any special control or dissemination markings be required, an additional “Marking” column may be added for clarity.

A2.6.7.7. Should an SCG include more than one original classification decision made on a different date, add an extra column to the table to identify the specific original classification decision dates.

Figure A2.1. SCG Template Cover Page

[CLASSIFICATION] - center classification designation here IAW DoDM 5200.01, Volume 2 for classified guides. If unclassified see bottom of this page for marking guides FOUO.

[UNCLASSIFIED NAME OF THE SYSTEM, PLAN, PROGRAM, OR PROJECT]
SECURITY CLASSIFICATION AND DECLASSIFICATION GUIDE

[Program Logo (Optional)]

[Date (if revision, this date is the date of the original SCG)]

[When applicable, revision date]

ISSUED BY: [Name and address of issuing office]

APPROVED BY: [OCA name and title, or personal identifier]

[Statement of supersession of previous guides, if any]

[Distribution statement IAW DoDI 5230.24 and AFI 16-204]

**NOTE: When the SCG or declassification guide is classified, all markings required by DoDM 5200.01, Volume 2 shall be included.

[CLASSIFICATION] – center classification here IAW DoD 5200.01, Volume 2 if guide is classified. If guide is unclassified, place FOUO designation here IAW DoDM 5200.01, Volume 4.

Figure A2.2. SCG Template Foreword Page

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

[TITLE] SECURITY CLASSIFICATION AND DECLASSIFICATION GUIDE

FOREWORD

Description. Provide a short synopsis of the technology, system, plan, program, project, or mission covered in the SCG.

COORDINATED BY:

_____

[Program/Project Director's Name, Title, and Signature]

APPROVED BY:

_____

[OCA's Name, Title, or Personal Identifier, and Signature]

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.3. SCG Template Section 1

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

[TITLE] SECURITY CLASSIFICATION AND DECLASSIFICATION GUIDE

SECTION 1 – GENERAL INSTRUCTIONS

1. Purpose. To provide instructions and guidance on the classification of information involved in (name of system, plan, program, project, or mission) using an unclassified identification of the effort. (If it is necessary to classify the guide, modify this paragraph as necessary to acknowledge the classified content.)

2. Authority. This guide is issued under authority of Executive Order 13526, DoDM 5200.01, and AFI 16-1404. Classification of information involved in (identify the effort) is governed by, and is in accordance with, (cite any applicable classification guidance or guides under which this guide is issued). This guide constitutes authority and may be cited as the basis for classification, regarding, or declassification of information and material involved in (identify the effort). Changes in classification required by application of this guide shall be made immediately. Information identified in this guide for protection as classified information is classified by (complete title or position of classifying authority).

3. Office of Primary Responsibility (OPR): This guide is issued by, and all inquiries concerning content and interpretation, as well as any recommendations for changes, should be addressed to:

(Include name, office symbol, mailing address, organizational NIPRNET email address, and DSN and commercial phone numbers. Also specify secure data and voice contact information to receive classified or sensitive communications.)

4. Classification Challenges. If at any time, any of the security classification guidance contained herein is challenged, the items of information involved shall continue to be protected at the level prescribed by this guide until such time as a final decision is made on the challenge by the OCA. Classification challenges should be addressed to the OPR.

5. Reproduction, Extraction, and Dissemination. Authorized recipients of this guide may reproduce, extract, and disseminate the contents of this guide, as necessary, for application by specified groups involved in [identification of the effort], including industrial activities. Copies of separate guides issued to operating activities in application of this guide shall be sent to the OPR. (If it is necessary to classify the guide, modify this paragraph as necessary to express any required limitations.)

6. Public Release. The fact that this guide shows certain details of information to be unclassified, including controlled unclassified information, does not allow automatic public

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements release of this information. DoD information requested by the media or members of the public or proposed for release to the public by DoD civilians, military personnel, or contractors shall be processed in accordance with DoD Manual 5200.01, *DoD Information Security Program,* DoD Directive 5230.09, *Clearance of DoD Information for Public Release,* DoD Instruction 5230.29, *Security Policy Review of DoD Information for Public Release,* AFMAN 33-302, *Freedom of Information Act Program*, and AFI 35-102, *Security and Policy Review Process*, as applicable. Proposed public disclosures of unclassified information regarding (identification of effort) shall be processed through (identify office to which requests for public disclosure are to be sent and provide contact information (information, where the specific office cannot be identified, state that requests should be processed through "appropriate channels for approval").

7. Foreign Disclosure. Any disclosure to foreign officials of information classified by this guide shall be in accordance with the procedures set forth in applicable issuances implementing DoD foreign disclosure policy, e.g., DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* and AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*]. If a country with which the DoD has entered into a reciprocal procurement memorandum of understanding or offset arrangement, expresses an interest in this effort, a foreign disclosure review should be conducted prior to issuance of a solicitation. (If it is known that foreign participation cannot be permitted because of the sensitivity of the effort, this fact should be stated. Add other guidance as appropriate.)

8. Release of Program Data on the Internet. Extreme care must be taken when considering information for release onto publicly accessible or unprotected Internet sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. Internet technology search and data mining capabilities must be assessed from a risk-management perspective. Information intended for publication on publicly accessible or unprotected Internet sites must be cleared for public release prior to publication according to AFI 35-102, *Security and Policy Review Process*. Also refer to AFI 35-107, *Public Web Communications*. If there are any doubts, do not release the information.

9. Definitions. (Include in this paragraph the definitions of any items for which there may be various meanings to ensure common understanding of the details of information that are covered by the guide.)

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.4. SCG Template Section 2

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

SECTION 2 – OVERALL EFFORT

1. Identification. (Include in this paragraph any necessary statements explaining the classifications, if any, to be assigned to various statements identifying the effort. These statements should be consistent with other program documentation.)

2. Goal, Mission, Purpose. (Include in this paragraph any necessary statements identifying information concerning the purpose of the effort that can be released as unclassified and that which must be classified. Take care to ensure that unclassified statements do not reveal classified information.)

3. End Item. (Include in this paragraph statements of the classification to be assigned to the end products of the effort, whether paperwork or hardware. In this connection it is important to distinguish between classification required to protect the fact of the existence of a completed end item, and classification required because of what the end item contains or reveals. In some instances classified information pertaining to performance, manufacture, or composition of incorporated parts or materials is not ascertainable from mere use of or access to the end item. In others, the classifiable information is that which concerns total performance, capabilities, vulnerabilities, or weaknesses of the end item itself, rather than any of the parts or materials.)

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.5. SCG Template Section 3

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

SECTION 3 – (SAMPLE) PERFORMANCE AND CAPABILITIES

(This section includes characteristics of performance and capability of an end item, or an end item's components, parts, or materials, the performance or capabilities of which require classification. In this section also provide, in sequentially numbered items, statements that express details of performance and capabilities planned and actual. Include both those elements that warrant classification and those that are unclassified. These statements normally would not set forth the numeric values that indicate degree of performance or capability, planned or attained, but merely should identify the specific elements of performance or capability that are covered. When it is necessary to state certain limiting figures above or below which classification is required, the statement itself may warrant classification. For clarity, continuity, or ease of reference it may be desirable to include performance classification data in the sections dealing with the end item or the components or parts to which the performance data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.)

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.6. SCG Template Section 4

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

SECTION 4 – (SAMPLE) SPECIFICATIONS

This section includes items of information describing standards for [qualities of materials and parts; methods or modes or construction, manufacture or assembly; and specific dimensions in size, form, shape, and weight, that require classification]. Inclusion in this section is required because the items require classification because they contribute to the national security advantage resulting from this effort, or because they frequently require classification but are unclassified in (identification of this effort). Classification of specifications pertaining to performance and capability are covered in section 3 of the guide. (Actual figures do not need to be given, merely statements identifying clearly the specific items of information involved. If figures are necessary to establish classification levels, it may be necessary to classify the statements themselves. When necessary for clarity, continuity or ease of reference, specification classification data may be included in sections on the end product or components or parts to which the data apply. Use a "Remarks" column for explanations, limitations, special conditions, associations, etc.)

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DATE OF ORIGINAL DECISION	DECLASSIFY ON	REMARKS
1. Burn rate	C	1.4(a)	19960917	20210917	
2. Power requirement	U or S	1.4(a)	19960917	20210917	"S" when associated with Model No. Otherwise "U."
3. Chemical composition	U	N/A		N/A	Composition is FOUO

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.7. SCG Template Section 5

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

SECTION 5 – (SAMPLE) CRITICAL ELEMENTS

(This section is used only if there are specific elements that are both critical to the successful operation of the end item of this effort and unique enough to warrant classification of some data concerning them. Provide in sequentially numbered paragraphs each significant items of information peculiar to these critical elements and the classification applicable. Also include in this section the classification to be assigned to information pertaining to components, parts, and materials that are peculiar and critical to the successful operation of the end item in this effort when such items of information are the reason for or contribute to the national security advantage resulting from this effort. Performance data pertaining to such critical elements can be included in this section instead of section 3 of the guide.)

TOPIC	CLASS	REASON	DATE OF ORIGINAL DECISION	DECLASSIFY ON	REMARKS

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.8. SCG Template Section 6

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

SECTION 6 – (SAMPLE) VULNERABILITIES AND WEAKNESSES

(This section is used to specify classification to be assigned to details of information that disclose inherent weaknesses that could be exploited to defeat or minimize the effectiveness of the end product of this effort. Classification assigned to details of information on countermeasures and counter-countermeasures should also be included in this section.)

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DATE OF ORIGINAL DECISION	DECLASSIFY ON	REMARKS
1. Information assurance vulnerabilities	S	1.4(a)	19960917	20210917	
2. System limitations	S	1.4(a)	19960917	20210917	

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.9. SCG Template Section 7

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

SECTION 7 – (SAMPLE) ADMINISTRATIVE DATA

(This section is used only if particular elements of administrative data, such as program information, procurement schedules, production quantities, schedules, programs, or status of the effort, and data on shipments, deployment, or transportation and manuals (e.g., field, training, etc.), warrant classification.)

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DATE OF ORIGINAL DECISION	DECLASSIFY ON	REMARKS
1. Budget data					
a. FY budget total	U	N/A		N/A	
b. Budget estimate data, including total	U	N/A		N/A	"FOUO" prior to White House /OMB release to Congress.
2. Programmed end item production rate	U	N/A		N/A	"FOUO" prior to contract award.
3. Planned delivery mode	U	N/A		N/A	
4. Planned equipment delivery rate	C	1.4(a)	20050313	20300313	
5. Actual routing of delivery of end items	C	1.4(a)	20050313	See remarks, but not later than (NLT) 20300313	Classify upon selection of route, and declassify upon completion of last delivery to site.
6. Scheduled shipping dates and times	C	1.4(a)	20050313	See remarks, but NLT 20300313	Classify upon decision to ship, and declassify upon off-load at destination.

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.10. SCG Template Section 8

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

SECTION 8 – (SAMPLE) HARDWARE

The degree of specificity to be included in this section will depend largely upon:

a. The level from which issued. When issued from a headquarters level, the classification is most likely to be applied to the hardware end item itself, rather than its individual components.

b. The channels or hands through which the guidance will travel to the ultimate user. The closer the issuer is to the user, the more detailed the guidance may become. When the issuer is removed from the user, intermediate levels of guidance may be required to expand or elaborate on the guidance provided by the basic classification guide and to cover more details concerning materials, parts, components, assemblies, and subassemblies, and the classification, if any, to be assigned. Any such expansion or elaboration should be fully coordinated with the headquarters issuing the basic guide.

c. The ease of determining when classified information could be revealed by a particular hardware item. Obscure connections and associations that could reveal classified information may require the issuer of the guide to state classification for certain hardware items. In such cases it probably would be advisable to explain why classification is necessary.

d. Whether there are factors that require consideration and action at a headquarters level. National or DoD policy, intelligence data, broad operational requirements, extraneous factors, or other matters not ordinarily available below headquarters, or that require high level consideration may result in decisions to classify certain hardware items.)

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY

TOPIC	CLASS	REASON	DATE OF ORIGINAL DECISION	DECLASSIFY ON	REMARKS
1. End item hardware:					
a. An/APR-999	C	1.4(a)	19950820	20200820	External views of the assembled AN/APR-999 are “U.”
(1) Analyzer unit	C	1.4(a)	19950820	20200820	
(2) Threat display unit	U	N/A		N/A	Display specifications are FOUO.
b. AN/ APR-0000	U	N/A		N/A	

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements

Figure A2.11. SCG Template Classification/ Declassification Table

[CLASSIFICATION] – See Figure A2.1 for proper marking requirements **CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY**					
TOPIC	**CLASS**	**REASON**	**DATE OF ORIGINAL DECISION**	**DECLASSIFY ON**	**REMARKS**
1. Range					
a. Actual	S	1.4(a)	19950615	20200615	
b. Predicted	U	N/A		N/A	
2. Accuracy/ range rate					
a. Predicted	C	1.4(a)	19950130	20200130	
b. Measured	C	1.4(a)	19950130	20200130	
3. Altitude					
a. Operational	C	1.4(a)	19950130	20200130	
b. Maximum	U or C	1.4(a)	19950130	20200130	The general statement "in excess of 50K feet is "U." Otherwise, "C."
4. Commercial Receiver Model No. xxx					
a. Receiver sensitivity, selectivity, and frequency coverage	U	N/A		N/A	Standard commercial receiver characteristics are "U."
b. Fact of application or use in this effort	S	1.4(a)	20000415	20250415	
5. Resolution, Thermal					
a. Maximum attainable	U or S	1.4(a)	19960415	20210415	Planned or actual attained thermal resolutions above 0.25 degrees C are "U." Otherwise, "S."
[CLASSIFICATION] – See Figure A2.1 for proper marking requirements [CLASSIFICATION] – See Figure A2.1 for proper marking requirements					

CLASSIFICATION LEVELS AND DURATIONS ARE SHOWN FOR ILLUSTRATION PURPOSES ONLY					
b. Operational optimum	U or S	1.4(a)	19870415	20120415	Planned or actual attained thermal resolutions above 0.25 degrees C are "U." Otherwise, "S"
c. Operational attainment	U or S	1.4(a)	19870415	20120415	
6. Speed					Generic reference to "supersonic" speed is "U."
a. Maximum	S	1.4(a)	19960115	20210115	Downgrade to "C" upon IOC.
b. Rate of climb	S	1.4(a)	19960115	20210115	Downgrade to "C" upon IOC.
c. Intercept	S	1.4(a)	19960115	20210115	Downgrade to "C" upon IOC.
7. Sample information derived from another SCG	S	N/A	20030530	20280530	Derived from Program XYZ SCG, dated 20030530. Contact POC if a copy of the Program XYZ SCG is needed.
[CLASSIFICATION] – See Figure A2.F1 for proper marking requirements					

Attachment 3

INSTRUCTIONS FOR COMPLETING DD FORM 2024

A3.1. Block 1. Reason for Submission. Check one of the following:

A3.1.1. New Guide: This is an entirely new security classification and declassification guide, never issued before.

A3.1.2. Revision: Changes have been made to the previous version of the security classification and declassification guide.

A3.1.3. Reissuance: A security classification and declassification guide has been cancelled/rescinded and is being reissued.

A3.1.4. Biennial Review: The term "biennial" is inaccurately applied to this form. Reviews are required a minimum of once every 5 years, not biennially. If the security classification and declassification guide is due for its 5-year review and there have been no changes, mark this block.

A3.1.5. Cancellation: Self-explanatory.

A3.1.6. Correction: The security classification and declassification guide may have minor issues, such as an office symbol change.

A3.2. Block 2. Promulgating Document: Do not enter the name of the security classification and declassification guide. Provide only numbered publications which contain or transmit security classification and declassification guides; for example, agency regulations, technical books, formal instructions, and MAJCOM/DRU or local regulations. If the security classification and declassification guide is published separately, letters of transmittal, etc., should not be listed. If no numbered publications, enter "None."

A3.3. Block 3. Classification Guide Title: If the security classification and declassification guide is classified, be sure to designate an unclassified title such as "(U) Battle Ram security classification and declassification guide."

A3.4. Block 4. Classification Guide Date: For a new security classification and declassification guide, enter the date of its approval (the date signed by the OCA). When reporting a reissuance, enter the date of approval of the reissued guide. For other submissions, the security classification and declassification guide date remains the same. **NOTE:** Include a "revised as of" date on the actual security classification and declassification guide.

A3.5. Block 5. Classification Guide Originator: This is the activity/OCA position which issued the security classification and declassification guide.

A3.6. Block 6. Available through DTIC. Refer to distribution statement guidance at: **http://www.dtic.mil/dtic/submit/guidance/distribstatement.html**. In order to ensure proper accessibility, DTIC requires the correct distribution statement be assigned. If there is an incorrect statement or a mix of two different statements, the security classification and declassification guide cannot be processed into the Technical Report (TR) database. Additionally, the security classification and declassification guide must have a corresponding distribution statement on the cover page that matches the distribution statement on the DD Form 2024. If a guide is not

available through DTIC, but is being submitted to the DTIC TR database, a statement must still be assigned.

A3.7. Block 7. Biennial Review Date: Biennial reviews are not required. Enter the date 5 years from the date of the security classification and declassification guide, or 5 years from the review date, whichever is applicable.

A3.8. Block 8. Number of Revisions and Date of the Latest: For example, if the security classification and declassification guide has been revised three times, annotate that number along with the date of the latest revision.

A3.9. Block 9. Subject Matter Index Terms: Generated by OCA. For a list of terms, refer to **https://www.dtic.mil/doac/stresources/standards/securityclassification/subjectmatter.pdf**.

A3.10. Block 10. Classification of Guide: Self-explanatory.

A3.11. Block 11. Index Source Number: Can be left blank. If an internal number is used, the number can be placed in this block.

A3.12. Block 12. Highest Classification Prescribed by Guide: Self-explanatory.

A3.13. Block 13. The security classification and declassification guide prescribes classification of information controlled within a SAP. SAPs are security protocols that provide additional safeguards and access restrictions that exceed those for regular (collateral) classified information. For additional information or to obtain access to the security classification and declassification guide, contact the agency listed in Block 5.

A3.14. Block 14. Remarks: Used to advise DD Form 2024 recipients of any additional information considered appropriate. Note: This information will not appear in the DTIC Index and is optional. In addition to any remarks, this block shall reflect Information Protection Office coordination. (T-1) Annotate the name, office symbol, date, and signature of an Information Protection Office official.

A3.15. Block 15. OCA information and OCA signature. The date signed cannot precede the security classification and declassification guide date.

A3.16. Block 16. SM, action officer, or other POC with knowledge of the security classification and declassification guide and/or actions taken to update the security classification and declassification guide.

Attachment 4

CLASSIFIED MEETING/BRIEFING/CONFERENCE CHECKLIST

Table A4.1. Classified Meeting/Briefing/Conference Checklist

Classified Meeting/Briefing/Conference Checklist		
	The security manager is responsible for accomplishing all items below, unless the commander or director has delegated the responsibility to another individual.	
1	**PREPARATION**	**CHECK**
1.1	Determine subject of meeting and highest level of classification, to include special handling/access, NATO, CNWDI, etc.	
1.2	Determine meeting location (USG or cleared contractor facility).	
1.3	Determine if entire meeting will be classified or limited to classified sessions	
1.4	Select a meeting location that provides good physical control of the meeting room and perimeter, has storage containers (if required), and provides protection from unauthorized audio and visual access.	
1.5	Determine where classified material will be stored before, during, and after the meeting and who will be responsible for the material.	
1.6	Determine who will be responsible for managing classified material storage.	
1.7	Determine if classified notes will be permitted and, if so, establish storage and distribution procedures.	
1.8	Identify potential attendees.	
1.9	Determine whether the any foreign attendees or representatives. If so, arrange for official information release, both unclassified and classified, from the FDO. (Any US citizen representing a foreign interest is a foreign representative.)	
1.10	Announce the meeting on a need-to-know basis (email, phone, etc.).	
1.11.	Establish routing for attendee visit requests.	
1.12.	Verify security clearances using JPAS and establish need-to-know.	
1.13.	Establish a method to identify attendees for entry/reentry (control rosters, badges, etc.).	
1.14.	Establish an assessment process for personal items (briefcases, backpacks, purses, etc.) to prevent unauthorized items from entering the meeting area.	
1.15.	Identify IS equipment to be used and ensure it is authorized for classified use.	
1.16.	Identify any special communication requirements, e.g., STE (if required).	
2	**PRE-MEETING INSPECTION**	
2.1	If not familiar with area, request the building manager be present.	
2.2	Conduct a visual check of walls, ceilings, and floors for suspicious objects, e.g., holes, openings, exposed wires, recording devices.	
2.3	Ensure all doors, windows, and other openings are closed before classified briefing begins. First-floor windows and windows on doors shall be covered to prevent visual access. Windows on other floors that allow visual access should	

	be covered.	
2.4	Check all physically accessible areas.	
2.5	Check, touch, and lift, if possible, the following items/areas for things out of the ordinary, such as recording devices: Trash containers, fire extinguishers, tables, desks, chairs, curtains, pictures, any items on walls/windows, and circuit breaker boxes.	
3	**DURING THE MEETING**	
3.1	Prevent unauthorized entry by posting appropriately cleared AF employees outside the meeting area, or lock entrances to control access.	
3.2	Ensure conversations within the meeting room/area cannot be heard by un-cleared personnel outside the area.	
3.4	Identify and verify security clearance of attendees by checking on-hand rosters, lists, visit requests, messages, etc. that have been verified through JPAS.	
3.5	Implement check of personal items and look for unauthorized, unusual, or suspicious items. If an attendee denies the inspection, the item shall not accompany the attendee past the entry control point.	
3.6	Ensure personal electronic devices (PEDs) (cellular phones, radios, tape recorders, or other devices that can transmit or record) are not allowed within rooms/areas where classified information is discussed, briefed, or processed.	
3.7	If classified note taking is permitted, brief attendees on proper safeguarding, marking, and transmission requirements prior to the start of the classified portion of the meeting/briefing.	
3.8	Identify the highest level of each classified session to the attendees.	
3.9	Remind attendees that classified briefing portions should not be discussed freely once the meeting is finished.	
3.10	Remind attendees that discussing classified information outside the designated classified areas is prohibited.	
3.11	Remind attendees about their responsibility to protect classified information.	
3.12.	Ensure all classified meeting material is properly marked.	
3.13.	Ensure classified cover sheets are affixed to the front of classified material.	
3.14.	Ensure AIS equipment used to process or project classified information is approved for classified use.	
3.15.	Protect classified materials during any breaks.	
3.16.	Follow established procedures for protection and storage of classified material at all times. Maintain all electronic records in the approved electronic records management repository; this includes the classified repository on the SIPRNET.	
3.17.	Identify all attendees upon reentry from breaks, etc.	

4	**AFTER THE MEETING**	
4.1	Check area for unattended classified or unauthorized items left behind by attendees.	
4.2	Notify unit SM or servicing Chief, Information Protection of any security incidents.	
4.3	If required, turn facility back over to Facility Manager.	
4.4	Ensure classified is secured back in an authorized container.	
4.5	Ensure completed checklist is signed and dated.	
4.6	Return completed checklist to unit SM.	
	Meeting POC signature:	
	Printed name of meeting POC:	
	Date:	

Attachment 5

INSTRUCTIONS FOR COMPLETING DOE FORM 5 631.20

A5.1. An application may contain only one applicant. If multiple applicants require access, complete a form for each applicant.

A5.2. Each form may be for only one Sigma category. If the same individual requires access to multiple Sigma categories then submit a form each category.

A5.3. Part "A" – is normally prepared by the security manager.

A5.1.1. TO block: ASD(NCB) - Nuclear Matters, Attn: DoD UCPC, ODASD(NM), COMM: (703) 703-693-4009, FAX: (703) 697-2199

A5.1.2. NAME OF FACILITY (IES) TO BE VISITED block: (use "All Authorized DoD Sites" or for single events use the specific location provided by meeting POC).

A5.1.3. FOR THE INCLUSIVE DATES block: date of event/meeting, cannot exceed a year.

A5.1.4. FOR THE PURPOSE OF block: justification for access, e.g., attend meeting, perform recurring duties.

A5.1.5. TO CONFER WITH THE FOLLOWING PERSON(s) block: name, contact info of DOE/NNSA POC. For personnel on preapproved billet roster leave blank. When "All Authorized DoD sites" is used in 6 above, use "HQ USAF/A10-C" as POC.

A5.1.5.1. Specific Information to Which Access is Requested: (specific Sigma category)

A5.1.5.2. Access Requested To: (check appropriate box)

A5.1.5.3. Prior arrangement has been made as follows: (name, contact info of DOE/NNSA POC. For personnel on preapproved billet roster leave blank. When "All Authorized DoD sites" is used "Access Requested To" use "HQ USAF/A10-C" as POC)

A5.1.5.4. Certification for Personnel Having DoD Clearance: (approving officials will sign the DOE Form 5631.20, this is the only signature on this form).

Attachment 6

OPERATIONAL VISUAL INSPECTION CHECKLIST

Table A6.1. Operational Visual Inspection Checklist

OPERATIONAL VISUAL INSPECTION (OVI) CHECKLIST FOR SECURITY CONTAINERS, VAULT DOORS, AND SECURE ROOMS Note: Contact the Wing Information Protection Office and request a GSA-certified technician to repair the container, secure room lock, or vault door. If necessary, move classified material to another security container, secure room, or vault until repairs are completed.				
No.	**Item**	**Yes**	**No**	**N/A**
1.0	Exterior of security container:			
1.1	Check for cracks, broken welds, tampering, and environment effects (rust, moisture, mold, corrosion).			
1.2	Check for modifications (repainting, alterations, unauthorized marking, camouflaged repairs, engraving).			
1.3	Check affixed GSA Certification Label.			
2.0	Lock:			
2.1	Federal Standard FF-L-2740 combination lock (X-07, X-08, X-09, X-10 or S&G 2740) in place.			
2.2	Check front/back of lock for alignment and looseness.			
2.3	Check dial for ease of spinning and "power up" procedures.			
2.4	Check digital number display for digit visibility.			
2.5	Check behind the lock for a drill plate and/or punch plate. (The drill plate is a thick piece of hardened metal usually found behind the lock between the lock and punch plate. The punch plate is a thinner piece of hardened metal which slides into the groves behind the lock housing and is between the lock housing and the cover plate.)			
3.0	Release and opening drawer mechanism:			
3.1	Check for ease of operation.			
3.2	Check the handle (should "spring back" when the bolt release is engaged).			
4.0	Drawers:			
4.1	Check for alignment.			
4.2	Check for ease of opening or closing operations (drawers should slide with no resistance).			
4.3	Check for debris on, or dryness or excessive lubrication of, sliding rails.			
4.4	Check for missing screws.			
4.5	Check for metal shavings on the ledge of the container where the drawer closes.			
5.0	Vault and secure room doors (If applicable):			
5.1	Check for cracks, broken welds, tampering, and environment effects (rust, moisture, mold, corrosion).			
5.2	Check for modifications (repainting, alterations, unauthorized marking, camouflaged repairs, engraving).			

5.3	Check affixed GSA Certification Label.			
5.4	Check bolt work linkage connections and lubrication of bolt work and hinges.			
5.5	Check bolt work detent mechanism for proper function.			
5.6	Check for ease of opening and closing operations.			
5.7	Check alignment of door frame (door should swing open smoothly without dragging or sagging).			
5.8	Check operation of the emergency escape mechanism.			
5.9	Lock: Federal Standard FF-L-2740 combination lock (X-07, X-08, X-09, X-10 or S&G 2740) in place.			
5.10	Check front of lock for alignment and looseness.			
5.11	Check dial for ease of spinning and "power up" procedures.			
6.0	Lock operation for security containers, open storage rooms, or vaults:			
6.1	Locks are loose.			
6.2	Lock abruptly stops while spinning the dial to open the container.			
6.3	Lock dial starts to pull away from the lock.			
6.4	Display on the lock shows partial numbers or numbers start skipping.			
6.5	For X-08 and X-09 locks, the lock is missing the round pin head located about the center of the lock.			
6.6	Vault door sag or drag on the floor.			
6.7	Cracked or broken welds, tampering, excessive rust, unauthorized modifications.			
6.8	Missing GSA Certification Label.			
6.9	Bolt links falling apart, missing, or broken.			

Attachment 7 (Added-AFMC)

INQUIRY OFFICIAL APPOINTMENT MEMO (SAMPLE)

Figure A7.1. Appointment of Inquiry Memorandum (Sample)

MEMORANDUM FOR *(Inquiry Official)* *(DATE)*
FROM: *(Appointing Authority)*
SUBJECT: Appointment of Inquiry Official, Incident #*(15-XAFB-01)* (Suspense Date: *(date)*)

1. Under the provisions of DoD Manual 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*, and AFI 16-1404, *Air Force Information Security Program*, you are appointed to conduct a preliminary inquiry into security incident *(incident number)*. *(Provide a short summary of the incident)*. The incident was discovered on *(date)*.

2. The purpose of this inquiry is to determine whether a compromise occurred and to categorize this security incident as either a security violation, security infraction, or unfounded. You are authorized to interview those persons necessary to complete your findings. You are further authorized access to records and files pertinent to this inquiry. Your records indicate that you have a *(Secret, TS, etc.)* security clearance. Should you determine this incident involved access to program information for which you are not authorized access, advise the Chief of Information Protection (CIP).

3. Conducting this inquiry will be your primary duty until it is completed. Contact *(name and phone number CIP's representative)*, for a briefing on your responsibilities for, conduct of, and limitations of this inquiry. Your written report shall be completed within 10 duty days of appointment (suspense date: *(date)*) and shall be submitted to the CIP and then to me, in turn. I am authorized to grant extensions as needed. As a minimum, your report must contain the following:

a. An unclassified description of the information involved, if possible.
b. A statement that a compromise or potential compromise did or did not occur. If compromise or potential compromise occurred, state the classification source or Security Classification Guide.
c. Recommended category (violation, infraction, or unfounded) of the security incident.
d. If incident took place on an information system, determine if there was willful, negligent, or inadvertent action taken by the responsible person(s).
e. Cause factors and responsible person(s).
f. Recommended corrective actions needed to preclude a similar incident.

4. Notify me immediately at *(phone number)* if you determine that a compromise has occurred. Obtain technical assistance from the Information Protection Office and, if needed, the Staff Judge Advocate *(phone number)* during the course of this inquiry.

(Signature block of Unit Commander)

Attachment 8 (Added-AFMC)

INFORMATION PROTECTION SECURITY INCIDENT TECHNICAL REVIEW MEMO (SAMPLE)

Figure A8.1. Technical Review of Security Incident Inquiry Memorandum (Sample)

MEMORANDUM FOR *(appointing authority)*

FROM: *(IP Office)*

SUBJECT: Technical Review of Security Incident Inquiry *(or Investigation)* Report #*(15-XAFB-01)*

1. I have conducted a technical review of the subject security incident inquiry *(or investigation)* report IAW AFI 16-1404, *Air Force Information Security Program.* The report is technically sufficient, and I *(concur/nonconcur)* with the inquiry *(or investigating)* official's conclusions and recommendations. *(If nonconcur, state rationale.)*

2. IAW DoDM 5200.01-V1, *DoD Information Security Program,* Encl 3 paragraph 17, sanctions are authorized and must be considered for DoD military or civilian personnel if they knowingly, willfully, or negligently cause a security incident. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information and/or Controlled Unclassified Information, and removal of classification authority. Criminal prosecution may also be undertaken in accordance with 10 USC 801-940, also known as the Uniform Code of Military Justice, and other applicable US criminal laws. If taken, such actions must focus on correcting or eliminating the conditions that caused or brought about the incident. Consult with the servicing Judge Advocate Office or Civilian Personnel Office as needed.

3. Request incident closure or if you feel the inquiry is insufficient initiate a formal investigation. Your closure memo will determine if you concur or non-concur with the inquiry official; corrective actions taken; any administrative or punitive action taken against the person(s) causing the incident; the category of the incident (security violation or infraction); and if there was or was not a compromise of classified information. If the incident is an information technology Spillage/Classified Message Incidents (CMI), close the incident as a violation and include a statement citing whether the incident was cause by willful, negligent, or inadvertent action. If you believe there was a compromise, suspected compromise, or loss of classified information, list the notification date and identification of Original Classification Authority(ies), *(state the classification source or Security Classification Guide)*. Report shall be returned to *(IP Office)* no later than *(20 duty days)*.

4. I've attached a sample closure memo to use as a template. If you have any questions please call me at *(phone number)*.

(Signature block of CIP)

Attachments:
1. Sample Appointing Official Closure Memo
2. Security Incident #15-*X*AFB-01 Report

Attachment 9 (Added-AFMC)

COMMANDERS/DIRECTORS CLOSURE MEMO (SAMPLE)

Figure A9.1. Security Incident Closure Memo (Sample)

MEMORANDUM FOR *(IP Office)*

FROM: *(Appointing Authority)*

SUBJECT: Security Incident *#(15-XAFB-01)* Closure

1. I have reviewed the *(inquiry or investigation)* report for subject security incident. I *(concur or nonconcur)* with the inquiry official's findings. *(If nonconcur, state rationale and specify next action.)*

2. Recommendations. All recommendations have been implemented *(or the plan to implement)* to preclude similar incidents from occurring in the future. *(If additional recommendations are directed, state herein.)* Incident results and recommendations will be included in our organization's security education program.

3. Personnel Actions. I have taken the following administrative or punitive action(s) against the person(s) *(state rank/grade and name)* causing the incident; *(e.g., verbal counseling, letter of counseling, security information file (SIF), and remedial training)*

4. Incident Closure. No further investigation is required, and this incident is closed as a *(security infraction with no compromise or violation with a (compromise or suspected compromise)). (If the incident is an information technology Spillage/Classified Message Incidents (CMI), close the incident as a violation, determine if there was a compromise or no compromise, and include a statement citing whether the incident was caused by willful, negligent, or inadvertent action.) (If the inquiry wasn't sufficient and more information is required, the appointing authority would close the inquiry and start a formal investigation.)*

5. *(If there was a compromise/suspected compromise, include this paragraph)* The following Original Classification Authority(ies) *(list them)* have been notified on *(date)* concerning the compromise or suspected compromise. The information was classified in accordance with *(state the classification source or Security Classification Guide)*.

6. I understand the recommendations referred to herein or cited above are subject to review by the servicing Information Protection Office during the next program review to ensure they were implemented.

(Signature block of Appointing Official)

Attachment:
Security Incident *#(15-XAFB-01)* Report

Attachment 10 (Added-AFMC)

AFMC CENTER/WING SELF-INSPECTION

A10.1. (AFMC) This attachment will assist the CIP to accomplish the Center/Wing self-inspection explained in Chapter 10. The CIP individual organization self-inspection is different than IG inspections or self-assessments explained in AFI 90-201 and are not rated. Center/Wing IG inspections can be used in place of this Center/Wing self-inspection as long as all the required information is collected to write the Center/Wing's Annual Self-Inspection Report in accordance with this AFI and AFMC supplement. The Center/Wing IG inspection will also need to include all areas required to be reviewed in accordance with this AFI and AFMC supplement. The information collected during this CIP individual organization self-inspection will be used by the Center/Wing CIP to complete the Center/Wing Annual Self-Inspection Report. These security self-inspections are assistance oriented and used as training for the organization, commander/director and security manager on how to run their security program. A good thorough Center/Wing security self-inspection, that gives references and recommended corrective actions, can help reduce security incidents and improve security polices/procedure as well as security knowledge for the whole organization.

A10.2. (AFMC) The Annual Center/Wing Security Self-Inspection Report : Requires your inspection to include original classification, derivative classification, safeguarding, security incidents, management and oversight, security education, and declassification. To give the organization's commander/director and security manager a complete look at their security program also include personnel security, industrial security, controlled unclassified information (CUI), North Atlantic Treaty Organization (NATO), Restricted Data (RD), Formerly Restricted Data (FRD), and Critical Nuclear Weapon Design Information (CNWDI) material during the security self-inspection.

A10.3. (AFMC) Annual Security Self-Inspection Report Memorandum (Sample) :

Figure A10.1. Annual Security Self-Inspection Report Memorandum (Sample).

MEMORANDUM FOR *(Commander/Director/Head of organization being reviewed)*

FROM: *(CIP's Office Symbol)*

SUBJECT: *(Organization)*: Annual *(Center or Wing)* Security Self-Inspection

1. Authority: This Information Protection security self-inspection was conducted on *(date)* in accordance with DoDM 5200.01, *DoD Information Security Program*, and AFI 16-1404, *AF Information Security Program*. It will be used to complete the *(Center's or Wing's)* Annual Security Self-Inspection Report. These security self-inspections are assistance-oriented oversight visits to evaluate your Information Security, Personnel Security, Industrial Security, and Controlled Unclassified Information (CUI) Programs. *(Your organization was also evaluated in the safeguarding of North Atlantic Treaty Organization (NATO), Restricted Data (RD), Formerly Restricted Data (FRD), and Critical Nuclear Weapon Design Information (CNWDI) material.)* These self-inspections are not rated but are conducted to determine effectiveness, benchmark processes/products, identify deficiencies, and corrective actions.

2. Team Members: *(Include the names, position and office symbol of all the individuals on the team.)*

a. *(name, position, office symbol)*
b. *(name, position, office symbol)*
c. *(etc.)*

3. Personnel Contacted: *(Include the names, position, and office symbol of all the individuals you contacted.)*

a. *(name, position, office symbol)*
b. *(name, position, office symbol)*
c. *(etc.)*

4. *(This paragraph should be marked FOUO)* General Information: *(Optional paragraph)*

a. Last Inspection: *(date)*; Next Inspection: *(date)*

b. Number of Personnel:

(1) Top Secret Clearance: Government: *(#)*; Contractor: *(#)*

(2) Secret Clearance: Government: *(#)*; Contractor: *(#)*

(3) Uncleared: Government: *(#)*; Contractor: *(#)*

c. Number of OCAs: *(#)*
d. Number of Security Classification Guides (SCG): *(#)*
e. Number of Derivative Classifiers: *(#)*
f. Number of GSA approved Safes: *(#)*
g. Number of Approved Vaults and Secure Rooms (Open Storage Areas): *(#)*
h. Number of Security Incidents in last 12 months: Violations: *(#)*; Infractions: *(#)*
i. Number of SIPRNET terminals: *(#)* (*Might want to also include SIPRNET accounts and any other classified IT system*)
j. Number of Top Secret Documents: *(#)*

k. Number of on-base classified contracts: *(#)*

l. Number of accountable NATO Documents: *(#)*

5. *(This paragraph may be marked FOUO depending on the content)* Summary: *(Optional paragraph; executive summary of the review; include key findings, repeat areas, trends, best practice, and praises to individuals or teams.)*

6. *(This paragraph should be marked FOUO)* The following deficiencies/observations/recommendations were noted during the security self-inspection: *(Provide a response for every subtopic.*

- Subtopic doesn't pertain, write "N/A", "Not Applicable", or "Area not inspected".

-No deficiencies write "Organization is meeting all requirements" or "No deficiencies identified" or give praises to individuals or teams.

-Deficiencies or observations, spell out, include recommended corrective actions, and for deficiencies list regulation.

--Deficiency is any item that does not meet the intent or direction of the regulatory guidance from DoD, AF, MAJCOM, local supplements, or an organization's security plan/instruction, and requires a corrective action.

--Observation is an item of interest that support primary security elements, is not in any specific regulatory guidance, and may or may not require corrective action. Some observations may have the potential to jeopardize security if allowed to continue.)

a. Information Security:

(1) Original Classification: *(For the Annual Report collect: Number of documents reviewed and percentages are required; number of OCAs; number of OCA with current training; number of original classified document reviewed; number of and type of discrepancies from original classified documents reviewed; number of SCGs; number of SCG discrepancies) (Examples of topics to include: OCA is on AF approved OCA list; OCA initial and refresher training; does the organization still need an OCA; review original classification actions to include marking; only OCA making classification decisions; notified IP of any OCA changes; original classification decisions meet requirements; classification challenges; OCA trained on classification challenges; reclassification; OCA damage assessment timeline; OCA sign SCG and DD Form 2024; SCG in correct format; SCGs forwarded to IP, DITIC, etc; coordination of SCG; review of SCG; declassification over 25 years; foreign release approval)*

(a) *(Deficiency #1: OCA has not received annual refresher training. (AFI 16-1404, paragraph 3.2.5)*

Recommendation: CIP will contact OCA to schedule refresher training.)

(b) (*Observation #1: OCA will be retiring shortly, recommend acting director contact CIP to schedule OCA training so there isn't a gap in OCA coverage until the new director reports for duty.)*

(2) Derivative Classification: *(For the Annual Report collect: Number of documents reviewed and percentages are required; need to sample at least 20% of the organizations derivative classifiers; number of derivative classifiers; number of derivative classifiers with current training; number of derivative classified document reviewed; number of*

and type of discrepancies from derivative classified documents reviewed) (Examples of topics to include: Derivative Classifiers initial and refresher training; access to SCGs; foreign release approval; proper markings on documents, media, hardware, equipment, parts, etc; date created for old markings; unclassified marked in containers/secure rooms; working papers; RD/FRD/CNWDI; NATO; Files and emails on SIPRNET and other classified systems; listing of multiple sources; FOUO; received an improperly marked document; REL TO; NOFORN.)

(3) Safeguarding: *(Examples of topics to include: cover sheets; end of day checks (SF 701); SF 702; residential storage; overnight storage, temporary in-transit storage; secure rooms; vaults; classified meetings; protection of classified on aircraft; copiers/reproduction; printers; GSA approved containers; prohibited items in container; SF 700; OF 89 (AFTO Form 36); locks; repair/visual inspection; combinations; key control; emergency plan;*

(a) Destruction: *(Examples of topics to include: annual cleanout day; NSA approved shredder and other destruction devices; central destruction facility)*

(b) Vaults/Secure Rooms/Open Storage: *(Examples of topics to include: approvals; security-in-depth; risk assessment; supplemental controls; alarms; 4 hour checks; access control to room; escorting unclear individuals; construction standards; prohibited items in area; bulk storage)*

(c) Transmission: *(Examples of topics to include: receipts (AF Form 310); hand carrying (on and off installation, on aircraft); methods for TS, Secret, and Confidential; authorized GSA contract overnight delivery services; packaging; electronic transmission (SIPRNET); fax classified and FOUO; secure phones)*

(4) Security Incidents: *(Review last 12 months of security incidents; number of violations; number of infractions) (Examples of topics to include: timeline for reporting security incidents, appointing an inquiry official, completing inquiry, closing incident; notified OCA when required; OCA damage assessment (at the unit with the OCA and that the assessment is attached to inquiry); implemented appointing authorities corrective actions)*

(5) Management and Oversight: *(Examples of topics to include: commander involvement, appointment of security manager (SM)/assistant, is number of SM/assistant adequate, no contractors as SM, SM involvement, SM attendance at IP's SM meetings, Unit security plan/instruction, SM folder, are contractors included in unit program, write ups from last inspection have been corrected, waivers, SF 311 reporting; AFI 90-201 self-assessment completed, corrective actions, integrated contractors included, using MICT)*

(6) Security Education and Training: *(For the Annual Report collect: percentage of cleared personnel who received initial training and annual refresher training) (Examples of topics to include: Training for OCA, derivative classification, security managers, security specialist, TSCO training, initial, annual refresher, declassification, classification challenges; records of training; unit specific training; SCG/program classification training; debriefing (AF Form 2587 and JPAS); refuse to sign debriefing; SF 312 " Classified Information Non-Disclosure Agreement"; commander/supervisor involvement; handcarrying education; foreign travel; NATO; RD/FRD/CNDWI; CUI)*

(7) Declassification: *(For the Annual Report this section will be completed by the Air Force Declassification Office (AFDO)) (Examples of topics to include: MDRs,*

Systematic Review for Declassification)

(8) Controlled Unclassified Information (CUI): *(Example of topics to include: access/release; protection during work hours and after work hours; transmission (mail and electronic); protection on web sites; marking; education/training; approved for release to public or foreign nationals; distribution statements on technical documents)*

(9) Top Secret Accountability: *(Examples of topics to include: TS account establishment, TSCO appointment, TSCO training; accountability (AF Form 143), register page (AF Form 144), transmission of TS, destruction of TS; inventories; storage of TS; added markings required for TS; working papers)*

(10) North Atlantic Treaty Organization (NATO): *(Example of topics to include: access; briefing and debriefing (2583, 2587, and JPAS); ATOMAL rebrief; final background investigation; security education; storage; NATO separation; ATOMAL separation; combination changes; marking (NATO material and US material containing NATO); accountability of ATOMAL, CTSA, and NS; annual inventory; transmission (mail and electronic); reproduction; destruction; security incidents; release US information to NATO; contractor access; DD Form 254; approval/certification of IT systems (SIPRNET and other systems))*

(11) Restricted Data (RD)/Formerly Restricted Data (FRD)/Critical Nuclear Weapons Design Information (CNWDI): *(Example of topics to include: access; briefing and debriefing (2583, 2587, and JPAS); security education; marking; security incidents; contractor access; DD Form 254; AF doesn't declassify; AF Officials Authorized to Certify Access to RD in DoDI 5210.02, Enclosure 4 and using DoE Form 5631.20; U.S. citizenship for access to CNWDI; final security clearance for CNWDI)*

b. Industrial Security:

(1) Industrial Program Management: *(Examples of topics to include: commander involvement, contractor security POC identified, no contractors as the Government unit SM, contractor management involvement, contractor security folder, contractors participate in unit program, written response to security inspections of contractors in a timely manner, write ups from last inspection have been corrected, waivers, notified CIP of contractors working in their organization; reporting adverse information; reporting security incidents; notified when on-base contract starts and expires)*

(2) Security Clearance: *(Examples of topics to include: facility clearance; FOCI; NIDs; personnel clearances for contractors; HSPD 12 investigations)*

(3) Security Education: *(Examples of topics to include: participating in Government unit's program or have their own program with all the requirements included; following VGSA; debriefs)*

(4) DD Form 254: *(Examples of topics to include: unit and contractor have a copy; only giving access to the information described on 254; is it accurate; reviewed/updated within timeline)*

(5) Visitor Group Security Agreement: *(Examples of topics to include: unit and contractor have a copy; unit and contractor following VGSA; is it accurate and up to date; subcontractor has own VGSA or signed primes VGSA)*

(6) Self-Assessment: *(Examples of topics to include: AFI 90-201 self-assessment included in integrated units; completed in timeframe, report complete and detailed, corrective actions)*

c. Personnel Security:

(1) Background Investigation: *(Examples of topics to include: has proper background investigation for position sensitivity; timely periodic reinvestigation; interim security clearance; limited access authorization (LAA); HSPD-12 investigations; information (PII) is protected; verify the date and place of birth; Presidential support; eliminate unnecessary clearances)*

(2) Access: *(Examples of topics to include: determine access level (JPAS); position sensitivity; SAR code; UMD; annual review of SAR code position sensitively; Need-to-know, SF 312; foreign nationals; contractors; visitor access/requests; only given access to their clearance level; one-time access; continuous evaluation)*

(3) Security education: *(Examples of topics to include: security manager has been trained and has a JPAS account; in-process briefing (JPAS); RD, CNWDI, and NATO briefings (AF Form 2583 and JPAS); debriefing (AF Form 2587 and JPAS); continuous evaluation; foreign travel brief)*

(4) Security Information File: *(Examples of topics to include: reporting unfavorable information; access is suspended when CAF suspends clearance; information (PII) is properly protected; establishes SIF when needed and within timeline; notification to individual; decision on access to classified, restricted area, and IT systems; debrief and AF Form 2587)*

7. A response to this report is required. Please review this report and forward to your security manager for action. Provide corrective actions for each deficiency no later than *(date; give them 30 days)*. If the first response does not close all deficiencies, provide updates every 30 days thereafter until all actions are resolved or closed. Replies to observations are optional. A copy of this report must be filed in the unit security manager's handbook for retention and subsequent review.

OR

7. No response is required. Please review this report and forward to your security manager to file in the unit security manager's handbook for retention and subsequent review.

8. If you have any questions or require assistance, please contact *(name, office symbol, email, phone number).*

(name)

Chief, Information Protection

A10.4. (AFMC) Other requirements on Conducting an Center/Wing Security Self-Inspection:

A10.4.1. **(AFMC)** All documentation should be from the CIP to the organization's commander/director/equivalent. Send a notification memo in advance of the visit; offer an in-brief with commander/director/equivalent; offer an out-brief with commander/director/equivalent; and send the report addressed to the commander/director/equivalent, signed by the CIP, within 20 days of the security review. If the review revealed numerous deficiencies, a serious deficiency, or a security incident, insist on a giving an out-brief to the commander/director/equivalent or whoever is the highest ranking individual available.

A10.4.2. **(AFMC)** To be able to answer the Annual Self-Inspection Report, you will need to start collecting numbers and percentages of information reviewed and deficiencies identified. The number and percentages needed are as follows:

A10.4.2.1. **(AFMC)** Percentage of the original classification authorities trained

A10.4.2.2. **(AFMC)** Percentage of the derivative classifiers trained

A10.4.2.3. **(AFMC)** Percentage of cleared personnel who received initial training

A10.4.2.4. **(AFMC)** Percentage of cleared personnel who received annual refresher training

A10.4.2.5. **(AFMC)** Percentage of the documents that identify the derivative classifier

A10.4.2.6. **(AFMC)** Number of documents reviewed to determine the percentage of documents that identify the derivative classifier

A10.4.2.7. **(AFMC)** Percentage of the documents that list multiple sources

A10.4.2.8. **(AFMC)** Number of documents reviewed to determine the percentage of documents that list the multiple sources

A10.4.2.9. **(AFMC)** Number of classified materials reviewed during the annual review of agency's original and derivative classification actions

A10.4.2.10. **(AFMC)** Number of discrepancies found:

A10.4.2.10.1. **(AFMC)** Over-classification

A10.4.2.10.2. **(AFMC)** Overgraded/Undergraded

A10.4.2.10.3. **(AFMC)** Declassification

A10.4.2.10.4. **(AFMC)** Duration of classification

A10.4.2.10.5. **(AFMC)** Unauthorized classifier

A10.4.2.10.6. **(AFMC)** "Classified By" line for OCA and derivative

A10.4.2.10.7. **(AFMC)** "Reason" line for originally classified

A10.4.2.10.8. **(AFMC)** "Derived From" line

A10.4.2.10.9. **(AFMC)** Multiple sources list

A10.4.2.10.10. **(AFMC)** Overall marking

A10.4.2.10.11. **(AFMC)** Portion Marking

A10.4.2.10.12. **(AFMC)** Instructions from a classification guide are not properly applied

A10.4.2.10.13. **(AFMC)** Other marking classification issues not listed above