BY ORDER OF THE COMMANDER
MINOT AIR FORCE BASE

MINOT AIR FORCE BASE
INSTRUCTION 16-1401

24 JULY 2023

Operations Support

SECURITY ENTERPRISE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 5BW/IP

Certified by: 5BW/CV
(Colonel Michael D. Maginness)
Pages: 120

This publication implements AFPD 16-14, *Air Force Security Enterprise Governance*, AFI 16-1401, *Information Protection*, AFI 16-1402, *Insider Threat Program Management*, AFMAN 16-1404, *Air Force Information Security Program*, AFI 10-701, *Operations Security* and AFMAN 16-1405, *Air Force Personnel Security Program*. It provides the basis for implementing AF instructions to execute Air Force Security Enterprise Concepts (AFSEC) Security Enterprise (SECENT) portions of the Information Protection (IP) program and the Counter-Insider Threat Program (C-InTP) of the AFSEC. This publication provides protective standards for sensitive information, regardless of the domain, classification or category of the information. It applies to all military, civilian and government contractor personnel assigned to Minot Air Force Base (Minot AFB) 5th Bomb Wing (BW) and 91st Missile Wing (MW) units. It also establishes the local policies and responsibilities for the oversight, management, and execution of the Minot AFB SECENT and IP programs and is directive in nature. Compliance is mandatory for all personnel and the terms “must,” “shall,” and “will” denote mandatory actions in this instruction. The terms “should” or “may” indicate preferred, but non-mandatory actions. Failure to comply with the publication is punishable as a violation of Article 92, Uniform Code of Military Justice (UCMJ). This instruction implements guidance and requirements prescribed in: DoD Directive 5200.43, *Management of Defense Security Enterprise*, DoDI 5200.1 - Change 2, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, DoD Manual 5200.01, *DoD Information Security Program, Volumes 1, 2, and 3,* DoD Manual 5200.02, *Procedures for the DoD Personnel Security Program (PSP),* DoDI 5200.02, *DoD Personnel Security Program (PSP),* DoDI 5200.48, *Controlled Unclassified Information, DAFI 16-1403, CUI, Code of Federal Regulations (CFR) 32, Part 117, National Industrial Security Program Operating Manual*

(NISPOM), AFMAN 16-1404 and applicable AF Guidance Memorandums and AFGSC Supplements. It also consolidates selected SE and IP policy from DoDI 8500.01, *Cyber Security*, DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards; ID Card Life Cycle*, AFPD 10-7, *Information Operations*, AFPD 33-3, *Information Management*, AFPD 35-1, *Public Affairs Management*. The more "traditional" (Security Forces-based) security programs are governed under the local 31-series publications and/or requirements. Compliance with this instruction requires the collection and maintenance of information protected by the Privacy Act of 1974 authorized by Title 50 United States Code 797. For Official Use Only and/or Privacy Act statements are required by AFI 33- 332, *The Air Force Privacy Act Program*. Systems of Records, F031 AF APO, *Documentation for Identification and Entry Authority*, apply. Maintain records created as a result of published processes prescribed IAW AFI 33-322, *Records Management and Information Governance Program*, and dispose of records IAW the AF Records Disposition Schedule (RDS), available from the Air Force Portal at the AF Records Information Management System (AFRIMS) link. Contact supporting records managers as required. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847s from the field through the appropriate functional 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, T-3") number following the compliance statement. See DAFI 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 requestors commander for non-tiered compliance items.

SUMMARY OF CHANGES

This document has been revised to capture the following changes. Minor administrative changes throughout the instruction to include identifying the successor system for DISS as NBIS and e-QIP as eApp. Additional changes were made to the following chapters: throughout the instruction and the following changes by paragraph: **Chapter 4** - adds training requirements to gain Security Officer Visit Admin access in DISS or successor system NBIS and adds mailing address USMs will send completed SF 312, *Non-disclosure Agreement* (NdA) forms. **Chapter 6** - clarifies requirements for the approval and use of collaboration peripherals devices in secure spaces and adds sub-**paragraph 6.11** address approval procedures for portable wearable fitness and medical devices in classified processing areas. **Chapters 9** - was significantly changed to capture AFGSC changes to the transportation of classified on and off-base. **Chapter 10** - adds emergency plan procedure requirement. **Chapter 13** - added sharing for derogatory information between PRAP, SAP and IP agencies. **Chapter 15** - revising OPSEC Awareness Training to be completed annually through MyLearning along with installation training. **Attachments 1** thru **Attachment 8** were not changed. **Attachment 9** AF Form 2583 was added. **Attachment 10** Request For Personnel Security Action was added. **Attachment 11** adds On Base Classified Courier/Escort Briefing Template.

Chapter 1

THE AIR FORCE SECURITY ENTERPRISE CONCEPT (AFSEC) PROGRAM OVERVIEW

1.1. Purpose. The Secretary of the AF (SAF) established the SECENT with the publication of AFPD 16-14, *Air Force Security Enterprise Governance*, AFI 16-1402, *Insider Threat Program Management*, AFMAN 16-1404, *Air Force Information Security Program*, AFMAN 16-1405*, Air Force Personnel Security Program*, and AFMAN 16-1406, Volume 2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*. The AFSEC establishes responsibilities for oversight, management and implementation of the program in AFPD 16-14 and places general oversight under SAF/AAZ. The Information Protection (IP) portfolio, which includes Information, Personnel, Industrial Security (INFOSEC, PERSEC, INDUSEC) and Counter-Insider Threat (C-InT) falls under SAF/AAZ. This does not mean IP controls the AFSEC program, only that it provides linkage between multiple agencies to provide senior leaders with needed implementation strategies, IAW AFPD 16-14. This requires interagency cooperation between IP and multiple other administrative security functions and between AFSEC and more traditional security programs which fall under the Mission Assurance portfolio described in AFPD 16-14. The combined program at Minot AFB is called the Security Enterprise (SECENT) program, and includes the IP and other administrative security functions.

1.1.1. Scope of the Minot AFB SECENT. The Minot AFB SECENT focuses on administrative security functions, leaving the more traditional Security Forces (SF) functions (e.g., physical security such as gate entry, Protection Level (PL) resource protection, base defense, etc.) to the SF functions of the 5th Security Forces Squadron (SFS) and 91st Security Forces Group (SFG). This requires two separate executive councils to ensure proper focus: the Installation SECENT Advisory Group (ISAG) for SECENT-related issues and the Integrated Defense / Antiterrorism Executive Council (ID/ATEC) for traditional SF-related items. Each council has representatives on the other council (i.e., IP has a seat on the ID/ATEC, and the SF (5 SFS and 91 SFG) has seats on the ISAG).

1.1.2. The IP Portfolio. Three specific functional areas encompass the IP Portfolio: INFOSEC, PERSEC and INDUSEC. The 5 BW IP Office (5 BW/IPO) also provides oversight for the AF SECENT Insider Threat Program. The goal of IP operations is to provide consolidated guidance for IP concerns across SECENT using a converged organizational approach to provide an integrated risk-management structure to ensure information essential to successful operations is effectively protected and available to the warfighter.

1.1.3. The IP Concept. The IP concept is based on four key pillars which consist of PERSEC, physical security, information technology and security policy. The key to the IP program is the ability of the 5 BW/IPO to act as a single focal point for senior leaders on SECENT-related matters. This may include identifying and forwarding traditional security issues to the ID/ATEC POC for consideration/action.

1.1.3.1. The 5 BW/IPO is the sole focal point on matters pertaining to AF sensitive information, regardless of classification, category or the medium, with the exceptions noted in **chapter 7** of this instruction for special information programs.

1.1.3.2. The 5 BW/IPO reports directly to the 5 BW Vice Commander (5 BW/CV) through the Chief, IP (CIP).

1.1.3.3. Another key aspect of the IP concept is the establishment Minot AFB ISAG. The ISAG is an independent executive committee which reviews, coordinates and establishes policy for the Minot AFB IP and SECENT Programs. The ISAG is chaired by the 5 BW/CV (delegated to the CIP) and membership is addressed below (Tables **2.1**, **2.2**.). The ISAG Chairman has a seat on the installation's ID/ATEC, which acts as the installation's traditional security meeting group and may brief items of interest to this group. The ISAG is described in detail in **chapter 2** of this instruction.

1.1.4. Counter-Insider Threat Program. This portion of the SECENT is a joint effort for which IP provides oversight. Duties and responsibilities are incorporated in the following paragraphs, and program specific requirements are discussed at **chapter 13** of this instruction.

1.1.5. Operations Security (OPSEC) Program. Oversight for the installation OPSEC program is provided under the Minot AFB SECENT.

1.1.5.1. The Minot AFB OPSEC program is a joint 5 BW and 91 MW effort. The 91 MW provides primary and alternate Wing OPSEC program managers (PMs) to work with 5 BW OPSEC PMs, but the 5 BW PMs act as host and accomplish needed administrative actions (e.g., data collection, response to HQ taskers, working groups, etc.), compliance oversight and conduct coordinator training.

1.1.5.2. An individual will be designated and assigned to the 5 BW/IPO to manage the OPSEC program with oversight validated during the SECENT portion of the Commander's Inspection Program (CCIPs) using SAF, MAJCOM and local Management Information Communicator Toolkit (MICT) communicators/checklists.

1.1.5.3. In addition to the DAF requirement for all personnel to complete the DAF Operations Security Total Force Awareness annually through MyLearning, local training requirements for OPSEC coordinators and unit members are incorporated into the SECENT initial/annual training. Specialized training may be identified and will be conducted as needed, for deploying personnel, planners or other specialized functions.

1.1.5.4. The Unit Security Managers (USM) at Minot AFB are also tasked and trained as unit OPSEC coordinators.

1.1.5.5. Additional subordinate OPSEC PMs and OPSEC Planners may be appointed, utilized and trained as PMs at the group level, but will fall under administrative control of 5 BW/IPO to ensure proper program oversight.

1.2. Roles and Responsibilities. All unit commanders, staff agency chiefs, security managers and supervisors will ensure personnel assigned to their units who work with or around sensitive information (classified or controlled unclassified information (CUI)) are properly trained and comply with requirements, regardless of whether they have daily access to the information or not. The basic requirements are established in DoDM 5200-series and further defined by AF and MAJCOM subordinate instructions and manuals.

1.3. The 5th Bomb Wing Commander Duties. The Bomb Wing Commander (5 BW/CC) acts as the head of the component in regards to installation Security Enterprise as a whole, using the definition from DoDM 5200.01, Volumes 1-3. This includes executing program requirements from AFMAN 16-1404, Volume 1, Enclosure 2, paragraph 8 and performs duties as the Defense Security Executive discussed in DoD Directive 5200.43 at the installation level. This ensures a holistic implementation of SECENT as defined in DoDM 5200, AFI 16-1401 and 16-series instructions and manuals which allows the IPO to de-conflict and coordinate security related functions for sensitive/national security information. The CIP and 5 BW/IPO implement this program for the commander IAW AFI 16-1401, paragraph 2.19.

1.3.1. Activity Head. All activity head duties discussed in AFMAN 16-1404, Volume 1, Enclosure 2, Section 8 are delegated to subordinate commanders.

1.3.2. Activity Security Managers. The delegated Activity Head will appoint an Activity Security Manager, in writing. The Security Assistants discussed in AFMAN 16-1404, Volume 1, Enclosure 3, Section 19, h.(1) are locally designated as USMs.

1.3.2.1. The USM accomplishes activity security manager duties outlined in DoDM 5200.01, Volume 1, Enclosure 2, Section 8 and 9 and this instruction, with the exception of grade criteria. The 5 BW/IPO INFOSEC specialist meets the Activity Security Manager grade criteria.

1.4. The 5th Bomb Wing Vice Commander Duties. The vice commander is delegated all duties and responsibilities levied on the Wing Commander in DoDM 5200.01, Volume 1, AFMAN 16-1404 and AFI 16-1401, paragraph 2.18.1. These duties are further delegated, with the exception of direct oversight for the IP Office, to the CIP.

1.5. CIP Duties. The CIP is the wing commander's primary focal point for all SECENT and IP related matters and executes duties which include:

1.5.1. Certifying Authority for Open Storage (OS). The CIP acts on behalf of the 5 BW/CC as the delegated authority for certification and approval of OS areas used to store collateral classified.

1.5.1.1. Unit commanders will follow procedures outlined in **chapter 10**, **paragraph 10.7** when considering areas for OS. Areas not formally certified will not be used for OS of classified.

1.5.2. Certifying Authority for Open Discussion (OD). The CIP acts on behalf of the 5 BW/CC as the delegated authority for certification and approval of collateral classified secure discussion facilities, also known as OD areas.

1.5.2.1. Commanders will follow procedures outlined in **chapter 10**, **paragraph 10.8** when considering areas for OD. Areas not formally certified will not be used for OD of classified.

1.5.3. Chairman of the ISAG. The CIP acts as Chairman of the Minot AFB ISAG, on behalf of the 5 BW/CV. **Chapter 2** of this instruction discusses the ISAG.

1.5.4. Oversight of the 5 BW/IPO. The CIP ensures the 5 BW/IPO accomplishes duties outlined below, as required, to support Minot AFB IP and SECENT operations. The CIP:

1.5.4.1. Maintains and updates this SECENT instruction and works with SECENT functional experts to ensure it covers requirements from DoD/AF basic guidance publications.

1.5.4.2. Ensures IP representation is present at ID/ATEC or other security-related meetings, as needed, to address or provide briefings on IP or SECENT-related agenda items.

1.5.4.3. Provides oversight for personnel filling IP office billets to ensure they are trained, as required, IAW applicable security guidance (e.g., AFMAN 16-1404, AFI 10-701, etc.).

1.5.4.4. Provides oversight, guidance and technical assistance on IP/SECENT-related matters to senior leaders and works with SECENT experts to develop/implement local guidance, as needed.

1.5.4.5. Provides oversight of unit IP/SECENT self-assessments using the SECENT CCIP/MICT process. Ensures the applicable 5 BW/IPO specialist:

1.5.4.5.1. Develops local IP-related SECENT MICT checklists or communicators. Local checklists should be reviewed by AFGSC/IP prior to being loaded into the Minot AFB MICT database.

1.5.4.5.2. Verifies inspection/assessments are accomplished, as required and USMs track noted deficiencies using applicable local/HQ databases.

1.5.4.5.3. Works with 5 BW/IG and 91 MW/IG, when possible, to integrate SECENT unit self-assessments and annual program inspections into the commander’s inspection program (CCIP) schedule.

1.5.4.5.4. Conducts OPSEC Program reviews and assessments IAW AFI 10-701, paragraph 5.1.

1.5.4.6. Prepares the annual Senior Agency Official (SAO)/Information Security Oversight Office (ISOO) self-inspection report for the wing commander’s review, prior to submitting to AFGSC/IP for inclusion in the MAJCOM annual SAF report.

1.5.4.7. The Activity Security Manager duties are delegated to USMs, as discussed above.

1.5.4.8. Prepares, reviews, approves and forwards the installation annual OPSEC program report, IAW AFI 10-701, paragraph 5.2.3.

1.6. IPO Duties. The 5 BW/IPO specialists are responsible to provide oversight for IP, CUI, C-InT and OPSEC portions of the Minot AFB SECENT program. The 5 BW/IPO conducts oversight activities IAW applicable DoD and AF guidance, as supplemented to include:

1.6.1. Program Continuity. The 5 BW/IPO provides program continuity by assisting units to understand and comply with IP-related SECENT requirements. This includes:

1.6.1.1. Maintaining documentation on serviced units. This is accomplished using unit folders which are included in the 5 BW/IPO office file plan.

1.6.1.1.1. The primary folder contains essential documents such as USM appointment/training documentation, initial/certification surveys for facilities, the unit SECENT Operating Instruction (OI), requests for survey, etc.

1.6.1.1.2. Additional files/folders may be maintained by each IP specialist, provided they are included in the official file plan. It is acceptable to reference the primary folder for required program documentation.

1.6.1.2. Managing the security incident program, to include providing trend analysis and risk mitigation recommendations to USMs and senior leaders (through the CIP). Specific requirements further discussed at **chapter 12** of this instruction.

1.6.2. Information Dissemination. The 5 BW/IPO provides USMs and senior leaders with information on Higher HQ (HHQ) or local changes to policy/procedure using email, special briefings or other forums.

1.6.2.1. The primary forum for updating senior leaders is the ISAG, discussed in **chapter 2**.

1.6.2.2. The primary forum for updating USMs is the USM meeting, typically held quarterly, but which will meet semiannually, as a minimum to brief USMs on topics of interest.

1.6.2.2.1. Out-of-cycle USM meetings may be called to disseminate urgent policy changes, collect feedback on local issues, and identify potential trends.

1.6.2.2.2. Special SECENT guest speakers may be invited to USM meetings to provide SECENT perspectives which cross traditional functional lines.

1.6.3. SECENT Training Activities. The 5 BW/IPO may provide USMs assistance with identifying training needs and developing IP-related training methods to meet the needs. This topic is covered in **chapter 11** of this instruction.

1.6.4. Inspections and Staff Assistance Visits (SAV). The 5 BW/IPO uses the CCIP process to conduct annual inspection with units conducting semiannual self-assessments under MICT. The IP inspections are the primary source for collecting data used to complete the annual ISOO self-inspection report required in DoDM 5200.01, Volume 1 Enclosure 2, Section 7.d.

1.6.4.1. The annual unit SECENT inspection is a multi-agency event conducted by all SECENT functional experts, typically on the same day, as part of the IG CCIP construct, when possible to reduce the overall annual inspection footprint on units.

1.6.4.1.1. The SECENT experts use HAF and/or localized checklists to validate compliance with DoD/AF guidance. The same checklists may be loaded into MICT for unit program managers to use during semiannual self-assessments.

1.6.4.1.2. The checklists should be reviewed by the MAJCOM functional expert prior to use, but in any case, each checklist item must have a valid DoD, AF, or local guidance reference.

1.6.4.1.3. The 5 BW/IPO utilizes IGEMS as the primary reporting tool for managing inspection deficiencies and recommended improvement areas identified during the inspection. The 5 BW/IPO participates in the full life cycle of the inspection process from conducting the inspection to approving the corrective action.

1.6.4.1.4. Any inspection findings are tracked by the unit and associated IG in IGEMS, as applicable.

1.6.4.1.5. The IP portion of the inspection includes items needed to compile the annual ISOO report.

1.6.4.1.6. Program requirements for OPSEC, CUI and C-InT are included in the IP portion of the SECENT inspections.

1.6.4.1.7. Each SECENT functional expert will assist the IGs to validate compliance and corrective actions for deficient items noted during IG events (inspections/SAVs), CCIPs or self-assessment activities.

1.6.4.1.7.1. This is primarily accomplished by reviewing the previous year's inspection report and MICT.

1.6.4.1.7.2. Additionally the functional expert will validate corrective actions during annual inspections.

1.6.4.2. Local SAVs may be requested, in writing, by the unit commander and will be conducted using MICT communicators/local checklist or applicable DoD/HHQ guidance. Typically, a SAV should not be requested within 60 days of a unit's scheduled annual CCIP event.

1.6.4.3. Participation in the SECENT inspection does not preclude a SECENT discipline from conducting a separate review/written report, if mandated by higher guidance.

1.6.4.4. The HHQ MICT communicators and local checklists used during reviews/inspections are provided to USMs and SECENT program managers for use by local inspectors and assessors. All items on local checklists will have a valid reference from published guidance for the indicated compliance action. This practice ensures compliance and keeps units prepared for no-notice events such as Command Cyber Readiness Inspections (CCRIs).

1.6.4.5. Commanders may request local SECENT special program reviews, in writing, if there is a need (e.g., self-assessments or other factors indicate issues exist). The 5 BW/IPO can help coordinate the visit and corrective actions through the applicable SECENT functional experts.

1.6.5. Unit semiannual self-assessments. Will be conducted IAW the 5 BW and 91 MW IG inspection schedule. If published, units will use the MICT/local checklists when conducting these self-assessments.

1.6.6. Conduct technical assistance visits. The 5 BW/IPO can provide technical assistance to USMs during special visits, if requested in writing by the unit commander. The goal of the visit would be to help units identify/correct any IP-related issues/deficiencies. The 5 BW/IPO may also assist in coordinating non-IP SECENT technical assistance visits. Unlike a SAV, generally no report will be generated for a technical assistance visit.

1.6.7. Coordinate facility/area surveys. The 5 BW/IPO will arrange needed functional experts to conduct facility/area surveys. This may include:

1.6.7.1. Initial risk assessment, certification or recertification surveys of OS and/or OD areas. The commander must request the risk assessment, in writing, to the CIP. Specific requirements for these areas are found at paragraphs **10.7** and **10.8**, of this instruction.

1.6.7.2. Risk assessments for Classified Processing Areas (CPAs). Follow the procedures outlined in **paragraph 6.4** of this instruction and applicable Cybersecurity requirements when reviewing CPAs.

1.7. The 5th Communications Squadron Commander. IAW AFI 16-1404_AFGSCSUP, the 5 BW/CC designates the 5th Communications Squadron Commander (5 CS/CC) as the installation Portable Electronic Device (PED) manager.

1.8. Commander/Staff Agency Chief Responsibilities. Commanders/Staff Agency Chiefs (referred to as commanders throughout the rest of this document) act as the Activity Head. They will establish, sustain and resource the necessary elements of the SECENT program IAW this instruction and DoD/AF basic directives.

1.8.1. The SECENT at Minot AFB includes IP (INFOSEC, PERSEC and INDUSEC), C-InT, CUI, OPSEC, Antiterrorism, Resource Protection, Records Management and Cybersecurity programs. This requires:

1.8.1.1. Ensuring mandated unit-level education, training and awareness is provided to assigned personnel IAW published DoD/AF guidance.

1.8.1.2. Assigning unit-level program managers/coordinators to provide oversight for identified programs. At Minot AFB, the USM assumes responsibilities for IP, OPSEC, C-InT and CUI managers. Commanders may assign independent program managers for other unit-level SECENT programs or align duties under the USM, depending on size of unit, program, etc.

1.8.1.3. Each commander will appoint, in writing, a USM and an alternate USM able to meet requirements and duties outlined in this instruction.

1.8.1.4. Ensuring USMs accomplish all training outlined in this instruction and should provide opportunities to attend in-residence professional training programs.

1.8.1.5. Not assigning contractors as USMs for government agencies.

1.8.1.6. The commander will ensure the USM develops a unit OI SECENT which addresses requirements outlined in DoDM 5200.01, Volume 1, 2 and 3. The USM will use the guidelines found at **paragraph 1.8.2** to develop the OI.

1.8.2. Unit SECENT OI. Publish a unit-level SECENT OI, signed by the commander, with a copy forwarded to the 5 BW/IPO upon signature/publication. The USM will ensure the OI complies with DAFI 90-160, *Publications and Forms Management*. As a minimum the OI:

1.8.2.1. May be published as a single, group-level instruction for agencies with multiple subordinate units (e.g. a group). If this type of group instruction is published, it must clearly identify and cover all subordinate units requirements (listed below). Subordinate units may still maintain a separate unit-level SECENT programs.

1.8.2.2. Should be based on the unit SECENT OI template provided by 5 BW/IP. It may also include requirements from other disciplines (i.e. records, emergency management, etc.), provided all mandatory SECENT guidance is present. For example, a unit may combine both physical security (AFI 31-101, *Integrated Defense*) and IP (16-14XX series) guidance into a single security OI.

1.8.2.3. Will include the unit's SECENT training plan.

1.8.2.4. Will follow procedures outlined in **chapter 10**, paragraphs **10.7** and **10.8**, when considering areas for OS and/or OD.

1.8.2.5. Will identify special area security procedures for OS/OD and CPAs areas, such as: entry/access controls, restrictions on electronic devices, etc. This also includes notifying the 5 BW/IPO 30 days prior to beginning substantial renovation or remodeling of certified open storage/discussion areas. **NOTE**: Failure to notify the 5 BW/IPO could result in decertification of the OS/OD area.

1.8.2.6. Will develop internal control procedures in the unit SECENT OI for classified and CUI which address rules for transport/transmission.

1.8.2.6.1. The custodian must ensure transfer is documented when classified is sent between on or off-base units. The use of the AF Form 310, *Document Receipt and Destruction Certificate*, is mandatory IAW AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 4, Section 4.k.

1.8.2.7. Will provide guidance in the SECENT OI on how/when combinations to security containers will be changed and that custodians are responsible to ensure this action is accomplished.

1.8.2.7.1. As a minimum, comply with AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 3, Section 11. Also consider changing container combinations annually.

1.8.2.8. Use of Forms. The USM will ensure the SECENT OI requires use of the SF 701, *End-of-Day Security Checklist* in any area where classified briefings occur, classified documents are used/discussed on a routine basis or where classified computers are used.

1.8.2.8.1. If classified containers are used, the OI will also require use of the SF 700, *Security Container Information*, the SF 702, *Container Check Sheet* and the Optional (OP) Form 89, *Maintenance Record for Security Container/Vault Doors*.

1.8.2.9. Will, as applicable, cover special program requirements (e.g., computer security (COMSEC), personnel reliability assurance program (PRAP), restricted data (RD), critical nuclear weapons design information (CNWDI), etc.), or reference the reader to appropriate local guidance.

1.8.2.10. Will require unit agencies (e.g., PRAP managers, first sergeants, supervisors, etc.) to notify USMs when derogatory information meeting Continuous Evaluation or Insider Threat thresholds is noted on unit members so the USM can complete mandatory actions in the Personnel Security Investigation (PSI) database of record and properly advise the commander. Failure to provide these notifications can negatively impact the individual's access to classified and may result in a downward derogatory notification on the individual who failed to report the information.

1.8.2.11. Will require those who provide oversight, handle, store or derivatively classify information as an integral part of their job (e.g., Cybersecurity, Intelligence career-fields, derivative classifiers, container custodians, USMs, etc.) have the duties identified as critical elements on performance reports. If the duties are not included in standard performance documents, add them in as a critical element on evaluation documents. {REF: DoDM 5200.01, Volume 1, Enclosure 2.Section 7.h.}

1.8.2.12. Will ensure access to collateral classified is granted as outlined in **chapter 4**, **paragraph 4.2.6** of this instruction.

1.8.2.13. If applicable, will provide procedures for Top Secret Control Program (TSCP) IAW DoDM 5200.01, Volume 1. The unit SECENT OI will also include the items notes at **paragraph 1.8.4** below

1.8.2.14. Will develop unit procedures addressing Imagery Review Procedures. The procedures will address.

1.8.2.14.1. Notification procedures, i.e. how and to who in the unit the requesting photographer will make pre-notification of the photography event in the area

1.8.2.14.2. Process to have an area/equipment subject matter expert to review all photos taken in the area prior to the photographer departing the area with the camera/disk.

1.8.2.14.3. The release of the approved photos to the photographer and procedure to declare a security incident and seize the camera and/or disk should a picture inadvertently capture classified information.

1.8.2.14.4. Development/use of a photography in sensitive areas checklist, see "**Attachment 14**", *Photography in Sensitive Areas Checklist*, for minimum checklist requirements.

1.8.3. Appointing USMs. All USMs, Assistant USMs, and Security Assistants will be appointed in writing, with a copy of the letter forwarded to the 5 BW/IPO. Additionally they will:

1.8.3.1. Be eligible for access **equal to the highest level of classified stored by the unit**, IAW DoDM 5200.01, Volume 1, Enclosure 2, Section 8. As a minimum, even if the unit does not store/handle classified, the USM must have current (in scope) Tier 3 investigation to allow access to the PSI database of record.

1.8.3.2. Not be considered for appointment if pending local or HQ derogatory actions. If suitability issues arise after appointment, remove the USM from duties until resolution of the matter.

1.8.3.3. There is no grade criteria for USMs or assistant USMs, but they must be mature, capable of dealing with senior unit leadership, have organizational placement allowing free access to the commander and be able to supervise assistant USMs.

1.8.3.4. If a group USM construct is used, assistant security managers for subordinate units report to the primary group USM, but may be appointed by the subordinate commander. Subordinate USMs must still meet criteria outlined in **paragraph 1.8.3.3** as they interact with unit leadership to discuss extremely sensitive personal information on unit members in the course of their duties. Security Assistants, per definition in DoDM 5200.01, Volume 1.

1.8.3.5. If possible, be assigned a billet on the unit manning document (UMD) tied to USM duties. This allows for better program continuity and consolidation of SECENT-type duties, such as Resource Protection, Force Protection, OPSEC, Personnel Reliability Assurance Program (PRAP), etc., under one program manager.

1.8.3.6. Use the “0080 Security Specialist” Performance Document (PD) for civilian positions with over 50% of duties security-related with USM duties reflected on the PD and in performance reports as critical. This does not preclude including other duties in the PD.

1.8.3.7. Complete all required training identified in this instruction within established timelines or be removed from USM duties.

1.8.3.8. If designated as an assistant (also called alternate) USM, meet appointing/training standards in AFMAN 16-1404, DoDM 5200.01, Volume 1, Enclosure 2, Section 8.c. and this instruction. At Minot AFB Assistant USMs are trained to the same standard as primary USMs, to include duties being reflected as critical on performance reports. Failure to complete training within specified timelines will result in the assistant being removed from USM-related duties.

1.8.3.9. Ensure security assistants are appointed in writing and trained IAW AFMAN 16-1404 and DoDM 5200.01, Volume 1, Enclosure 3, Section 6.e.(2) and this instruction. Security assistants will be trained to the same standards as USMs. Failure to complete training within established timelines will result in removal from security assistant duties.

1.8.3.10. Act as the unit OPSEC coordinator, CUI manager and C-InTP manager. All required training for these duties is included in the initial USM training.

1.8.4. Unit TSCP Procedures. These duties may be assigned to a unit member, including the USM, by the commander. The member assigned must have the appropriate access authorized to include any special access program (SAPs) within the organization to allow oversight/administration of the TSCP. In addition to the items covered in **paragraph 1.8.2.11** above, ensure the following are clarified in the unit’s SECENT OI:

1.8.4.1. Designate a top secret control officer (TSCO) and at least one top secret control assistant (TSCA), in writing, to manage the TSCP. If the USM or Assistant USMs are used as TSCO or TSCA, the USM appointment letter may also be used as the TSCA appointment letter.

1.8.4.2. Cover all requirements outlined in DoDM 5200.01, Volume 1, Enclosures 2, Sections 8.d. and 10 and Enclosure 3, Section 6.d, any AFGSC specific requirements and specific local procedures outlined in the unit’s SECENT OI.

1.9. Tenant Units. Tenant units are encouraged to participate in the Minot AFB SECENT program, but a tenant unit commander may decline participation. If opting out of the program, the unit commander (or equivalent) will provide a signed memorandum formally declining participation in all or part of the Minot AFB SECENT program. The memorandum will be maintained in the 5 BW/IPO unit folder and should be reviewed annually.

1.10. USM Duties. The USM is responsible for coordinating the INFOSEC, PERSEC, INDUSEC, OPSEC, CUI, and C-InT portions of the unit's SECENT Program on behalf of the commander. The USM acts as liaison between the unit and 5 BW/IPO for IP-SECENT matters. Additionally:

1.10.1. Managing Database of Record. The USMs are the sole focal point for in/out-processing personnel, submitting PSIs and keeping unit information in the database of record updated. Specific requirements are outlined in **chapter 4** of this instruction.

1.10.2. Processing PSIs. The USM uses procedures at **paragraph 4.4** to process PSIs.

1.10.3. Management of Continuous Evaluation and C-InT Reporting. In addition to the requirements outlined in **chapter 4** of this instruction, the USM will ensure procedures for actions to take if security eligibility is suspended/removed as a result of Continuous Evaluation or C-InT reporting action are documented in the unit's SECENT OI. As a minimum:

1.10.3.1. The USM will ensure the commander evaluates unescorted entry privilege to restricted areas if a CE report is generated and removed if it's an C-InT notification. Specifically:

1.10.3.1.1. If unescorted entry to restricted areas is removed, the USM will immediately notify the individual/agency identified in the unit's SECENT OI of this information.

1.10.3.1.2. The designated agency will follow 5 SFS Pass and ID rules.

1.10.3.1.3. If the individual has access to 91 MW restricted areas, the USM will notify the Keys and Codes Control Center (KCCC) to ensure the AFGSC Form 245, *Authenticator Assignment/Entry Authorization Request/Record* is updated to remove unescorted entry to the missile complex. Failure to complete this action may result in a classified security incident.

1.10.3.1.4. If escorted entry is required for duty, the USM will ensure all sections/areas where the individual will perform duties are notified, in writing, the member is no longer authorized access to classified.

1.10.4. TSCP Oversight. The USM is responsible for oversight of the unit TSCP. If a unit has top secret (TS) material, the USM needs to be eligible for TS access IAW DoDM 5200.01, Volume 1, Enclosure 2, Section 8.b.(2)(d).

1.10.5. Management of the SECENT Program. The USM is the primary focal point for SECENT Program administrative actions and the 5 BW/IPO coordinates SECENT-related tasks/suspense items through them. This may include:

1.10.5.1. Posting sufficient numbers of the "Your Unit Security Manager/OPSEC Coordinator Is…." signs throughout the unit to ensure unit personnel are aware of the appointed USMs/OPSEC Coordinators. A generic template is provided by 5 BW/IP, but any format may be used so long as it provides primary/assistant USM contact information.

1.10.5.2. Disseminating information received from the 5 BW/IPO to the unit commander and assigned unit personnel, as required. The USM should consider using newsletters, e-mails, briefings at commander's calls, etc., to disseminate this type of information.

1.10.5.3. Providing assistance to the 5 BW/IPO, as required; for example, updating appointment letters, coordinating unit's SECENT OI, monitoring SECENT training, scheduling self-assessments, collecting data for local or HHQ tasks (e.g., security incidents, unit specific tasks, etc.) and other USM-related activities.

1.10.5.4. Ensuring applicable copies of appointment letters, reports, letters, etc. are provided to the proper installation office if managing a combined SECENT program. For example, ensuring only 5 SFS RP manager information receives RP monitor appointment letters.

1.10.6. SECENT Self-assessment (SA) Program. The USM will conduct self-assessments in MICT IAW DAFI 90-302 and Minot AFB IG business rules in relation to MICT.

1.10.7. Managing Unit Security Incident Program. The USM will ensure the 5 BW/IPO is immediately notified of classified security incidents and comply with actions outlined in **chapter 12** of this instruction.

1.10.8. Attendance of USM meetings. The USM or assistant USM will attend scheduled USM meetings and provide technical assistance, as needed.

1.10.9. Reporting Classified Authorization Receipt Listing and Nuclear Weapons Related Material (NWRM) Authorization Receipt Listing (CARL/NARL) Updates. The USM works with 5th Logistics Readiness Squadron (5 LRS) to ensure the CARL/NARL is valid, to include notifying 5 LRS/LGRMC when unit members:

1.10.9.1. No longer require access to the CARL/NARL due to permanent change of assignment/station or job changes.

1.10.9.2. Lose eligibility or access to classified. Failure to make this notification to 5 LRS/LGRMC may result in a classified security incident on the receiving unit.

1.10.10. Maintain a USM handbook which contains the following:

1.10.10.1. Tab 1. Includes appointment letters (e.g., USM, TSCO, derivative classifiers, etc.), and any others the USM determines are of use.

1.10.10.2. Tab 2. Contains information concerning unit storage of classified material. As a minimum it will include the unit consolidated storage letter and the list of personnel with combinations classified storage.

1.10.10.2.1. Ensure the consolidated storage letter identifies the container/area with a unit unique designator (e.g., Container SF-1, OS area 1, etc.), the location and identifies the primary/alternate custodians for the area.

1.10.10.2.2. The consolidated unit storage letter should be signed by the commander, but may be signed by the USM. Provide a copy of this letter to the 5 BW/IPO whenever changes are made.

1.10.10.2.3. It is acceptable to include CPAs and/or OD areas on the consolidated storage letter. If not on the consolidated letter, ensure a separate listing is generated. Identify whether CPAs are temporary or permanent CPAs.

1.10.10.2.4. Include a listing of approved classified reproduction equipment and ensure a copy of it is also posted near the approved device.

1.10.10.2.5. Copies of all OS/OD, vault certification letters and approved risk assessments.

1.10.10.3. Tab 3. Includes a copy of the unit's SECENT OI. Other Air Fore Security Enterprise/IP-related instructions will also be maintained at this location if not included in the unit's SECENT OI (e.g., entry/access control for OS/OD areas or CPAs.

1.10.10.4. Tab 4. Includes the most current SAF/local SECENT-related self-assessment MICT communicators/local checklists (location of items may be referenced by a memorandum if stored electronically or in a separate binder).

1.10.10.5. Tab 5. Includes SECENT MICT self-assessment results, MICT assessment print outs, history or document on open item for unit's history information, etc.

1.10.10.6. Tab 6. Includes SECENT inspection report or Wing IG SECENT CCIP report and any other SECENT-related SAV reports within the last calendar year.

1.10.10.7. Tab 7. Includes USM and unit SECENT training documentation; SECENT training slides, unit member training documentation and USM training records.

1.10.10.8. Tab 8. Includes copies of the USM quarterly meeting minutes for the past 12 months.

1.10.10.9. Tab 9. Includes a copy of the unit's access roster pulled from the database of record, current within 30 days and updated to reflect any personnel, access level and Non-disclosure Agreement (NdA) changes.

1.10.10.10. Tab 10. Includes OPSEC program items (e.g., copy of unit critical information and indicator list (CIIL)) or any other SECENT items not covered in other handbook tabs. If an external OPSEC binder is used, place a memorandum in this section stating where the binder is maintained.

1.10.10.11. Tab 11. Includes miscellaneous items; for example, a copy of the most current UMD/Security Access Requirement (SAR) code review, copies of unit security incident inquiry/investigation reports (maintained IAW RDS).

1.10.10.12. Tab 12. Includes INDUSEC documentation (Visitor Group Security Agreement (VGSA), DD Form 254, *Contract Security Classification Specification*, management official listing, visit authorization Letter (VAL) or Visit Request, training documents, inspection results, etc.), as applicable

1.10.10.13. USM Handbook must be marked according to its contents. For example if documents in the handbook contain CUI (owning DISS/NBIS roster, facility surveys, security incident reports, etc.) the handbook must be marked CUI.

1.11. Individual Responsibilities. Each individual authorized access to any type of sensitive information (i.e., classified or CUI), regardless of the format (i.e., electronic, hardcopy, etc.), is responsible to comply with implementing DoD/AF guidance and this instruction. This includes understanding individual responsibilities for properly protecting classified information and CUI under their custody and control. Personnel (including assigned contractor personnel) must understand ANY sensitive information may be of value to our adversaries and must be properly protected, which requires:

1.11.1. Marking Sensitive Information Correctly. Each Airman must handle, mark, and properly control access to sensitive information entrusted to their care. This requires changing the mindset of "only classified" is important and also enforcing CUI safeguards, markings and controls.

1.11.2. Maintaining Positive Control. Each member must verify sensitive information under their control is properly protected when not under positive control. Positive control may be as simple as locking a computer before leaving for lunch to protect CUI or as complicated as performing closure actions to secure an alarmed area where classified information is stored.

1.11.2.1. Positive control also means never cutting corners on sensitive information, regardless of classification, category or type.

1.11.2.2. It is critical to understand our adversaries often collect CUI as a primary source of indicators for classified operations and criminals attempt to collect personal identifiable information (PII) to engage in identity theft.

1.11.2.3. Protective measures established for sensitive information are gauged on the identified risk for the specified type/category of information. Failing to use the required protective standards makes the information more susceptible to adversarial collection.

1.11.2.4. Be constantly alert to detect and report unauthorized attempts to access sensitive information at any level.

1.11.3. Reporting Incidents. Immediately report situations where sensitive information is found improperly guarded or appears to have been improperly accessed. The USM is the primary contact for collateral classified security incidents. The USM will forward the notification to the appropriate authority, depending on the category and type of information involved. If the USM is not available, report incidents as noted below:

1.11.3.1. If classified information is found improperly stored, accessed or marked, immediately secure it and report the incident to your USM, commander or supervisor.

1.11.3.1.1. If the USM is not available when the initial notification is completed, ensure they are notified afterwards.

1.11.3.1.2. If the incident occurs after normal duty hours, secure the information in an approved storage container/area and report it the next duty day. The same requirements apply, regardless of the type of information, (i.e., hardcopy, electronic media, etc.).

1.11.3.1.3. If DoD Unclassified Controlled Nuclear Information (DoD UCNI) CUI is found improperly stored, handled, accessed or is transmitted improperly over Non-secure Internet Protocol Router Network (NIPRNet), (i.e., if emailed outside the AF Network to a commercial address or other government agencies, but not encrypted/digitally signed) contact 5 SFS or 91 SFG (depending on agency generating the document) to determine if the investigative requirements outlined in DoDI 5210.83, Enclosure 3, Section 6.d. apply.

1.11.3.1.4. If PII CUI is improperly secured, improperly accessed by unauthorized individuals, or improperly transmitted over NIPRNet (i.e., is sent outside the AF Network to commercial addresses or other government agencies but not encrypted/digitally signed), contact the Minot AFB Privacy Act Manager (PA) at 723-7542 for specific actions to take.

1.11.3.1.5. All other types of CUI will be evaluated on a case-by-case basis with the originating agency to determine what, if any, administrative actions may be appropriate. If an unauthorized disclosure results in a public release of information, the AFGSC/IP office will be notified to ensure SAF/AAZ is informed for reporting purposes.

1.11.4. OS/OD or CPAs. Agencies with OS or OD facilities are responsible to follow the procedures outlined in **chapter 10**, paragraphs **10.7** and **10.8** of this instruction to ensure their facilities meet certification requirements.

1.11.4.1. If an OS/OD area has CPAs associated with it, also follow procedures outlined in **chapter 6** of this instruction.

1.11.4.2. If an area is a CPA, but not OS/OD, again follow procedures outlined in **Chapter 6**.

1.12. Container Custodian. Commanders will ensure all classified containers/storage areas have a designated custodian assigned, in writing. The Container Custodian will be a member cleared/authorized for the highest level of material stored in the container. The custodian is also responsible to ensure the assigned container is authorized for storage IAW AFMAN 16-1404, DoDM 5200.01, Volume 3. This includes maintaining the OP Form 89, SF 700, SF 701 and SF 702 and conducting the visual inspection. Additionally, they will:

1.12.1. Access Controls. Ensuring only authorized/cleared members have access to the container.

1.12.2. Training. Classified Container and Area Custodians will complete the Defense Counterintelligence and Security Agency (DCSA) Center for Development of Security Excellence (CDSE) Marking Classified Information Course (IF105.16)/Course Exam (IF105.06) and the Storage Containers and Facilities Course (PY105.16)/Course Exam (PY105.06) within 60 days of being appointed as a custodian. USMs will annotate the custodian's training date on the custodian appointment letter and maintain a copy of the training documentation (certificates). A copy of the custodian appointment letter will also be provided to 5 BW/IP. The DCSA CDSE training courses are located at: **https://www.cdse.edu/index.html**.

1.12.3. Technical Assistance. Container Custodians will work any needed technical assistance through the USM. Direct contact with the IPO by the custodian is not authorized.

1.12.4. Container Maintenance/Administration. Custodians will comply with DoDM 5200.01, Volume 3 and AFMAN16-1404 when accomplishing container maintenance, to include use of the OP Form 89 and other required security forms.

1.12.4.1. Maintain and update a record of authorized individuals having access to the container combination IAW DoDM 5200.01, Volume 3. A copy will be maintained in the container and in the USM handbook.

1.12.4.2. Ensure all documents/items stored in the container are properly marked, IAW DoDM 5200.01, Volume 2, AFMAN 16-1404, and this instruction.

1.12.4.3. Ensure the required "clean out" day is conducted as noted in **paragraph 10.8.4** to verify only information needed for specific mission requirements is maintained.

Chapter 2

THE INSTALLATION SECENT ADVISORY GROUP (ISAG)

2.1. ISAG Concept. The Minot AFB ISAG works in conjunction with the Minot AFB ID/AT EC to provide senior-level awareness of SECENT issues and is the local equivalent of the DoD Security Enterprise Executive Committee discussed in DoDD 5200.43. The ISAG specifically ensures compliance with SAF and MAJCOM IP policy, oversight, and training requirements by providing realistic courses of action to Minot AFB senior leaders on emerging threats and policy changes and feedback to MAJCOM on SECENT issues identified at the installation level. The ISAG is a cross-functional forum which brings experts from multiple SECENT-related disciplines together to resolve issues which cross traditional boundaries. This may include (but is not limited to) Cyber Security, COMSEC, Freedom of Information Act (FOIA), Personnel Reliability Assurance Program (PRAP), SAPs, INFOSEC, Computer Security (COMPUSEC), PERSEC, INDUSEC, and various other agencies. Other functional areas may be incorporated into the ISAG as deemed necessary.

2.2. ISAG Charter. The ISAG is chartered by the 5 BW/CC, as outlined in this chapter, to operate as an independent, executive-level group whose primary mission is to ensure the critical information used to accomplish the Minot AFB mission is available to the war fighter when needed. The group coordinates and oversees IP-related SECENT policy issues in direct support of the Minot AFB Wing Commanders. Oversight is provided by the 5 BW/CV through the CIP. This may include requiring members to conduct necessary research and staffing of packages prior to submission to senior leaders for action. The ISAG is separate from, but may work in conjunction with, other established groups such as the Minot AFB ID/ATEC or other formal groups.

2.3. ISAG Objective. The primary objective of the Minot AFB ISAG is to better protect sensitive information by focusing and streamlining oversight and coordination of SECENT policies. The medium used to relay the information (e.g., electronic media, hardcopy, etc.) and the type of the information, (e.g., classified, unclassified, equipment items, SAP, etc.) is considered during the risk management phase but does not exempt it from the IP process. The CIP coordinates with the MAJCOM functional expert on HHQ issues, as required, and receives technical support from the ISAG members, as needed.

2.4. ISAG Goals. The group's overarching goal is to ensure information is available to the war fighter when needed. In today's information rich environment, this may require the group to engage in cross-functional meetings with non-IP functions. This is especially true as SECENT issues often crossover into areas outside the basic IP regulations. For example, if a unit has a mission critical Nuclear Command and Control (NC2) command post, which falls under DoD 5210.41M nuclear security, the same area may also be a certified open discussion and open storage area for classified material and require the use of classified computers. In this case, in addition to the obvious INFOSEC and Cyber Security disciplines, planners must ensure nuclear security experts are included in decisions affecting the area to comply with NC2 physical security standards. This type of scenario requires close and early cooperation between IP, nuclear, operational, and other SECENT disciplines. The ISAG promotes a nontraditional, multi-functional approach, often termed as an enterprise approach and is the cornerstone of the SECENT concept.

2.5. ISAG Leadership. The 5 BW/CV provides oversight and additional direction, as needed, for the Minot AFB ISAG. The CIP is Chairman of the ISAG and is delegated to act for the 5BW/CV during these meetings. Commander appointed members represent and may act on behalf of their respective commander when in attendance.

2.5.1. ISAG Documentation. The CIP will ensure the 5 BW/CV and senior leaders receive the ISAG meeting minutes for review. If items require commander action, the CIP will forward ISAG recommendations to the appropriate commander(s) through their ISAG representative. Senior leaders may be briefed on ISAG action items, recommendations or updates via e-mail, through existing meeting forums or by electronic staffing, as needed. A member of the 5 BW/IPO acts as secretary/recorder for the group.

2.5.2. ISAG Structure. The ISAG consists of voting and advisory (nonvoting) members, as noted in this instruction. Including new members (voting or advisory) or changing advisory member voting status (temporarily or permanently) to enhance the group's capabilities may be accomplished by a majority vote of voting members. The voting members listed in **Table 2.1** may not be removed unless authorized by the 5 BW/CV. General administrative procedures and specific responsibilities for planning/follow-up of ISAG meetings are outlined below.

2.6. ISAG Meetings. The ISAG should meet quarterly, but may meet more or less frequently, as determined by the CIP or 5 BW/CV. Voting members are essential and at least two thirds of voting members must be present to establish a voting quorum for a meeting. Scheduled meetings will be conducted in-person, virtual (audio and/or visual) is also considered as in-person, and absent voting or nonvoting members will be noted in the meeting minutes. Effective operation of the ISAG is directly affected by members receiving information in a timely fashion. The chairman will maintain the group membership/distribution lists for all appointed members. Unit commanders are responsible to ensure the 5 BW/IPO is notified of any changes to unit representatives.

2.6.1. Documenting Meetings/Actions. The Chairman will distribute and track open ISAG action items and ensure meeting minutes are provided to members and senior leaders. Members not present and without an excused absence will be reported to the appointing official.

2.6.2. Working Groups. Subordinate working groups (WGs) may be formed as needed from voting, nonvoting and/or technical experts. They will meet as necessary and provide updates to the Chairman, as determined by their charter, until they are disbanded.

2.6.2.1. The OPSEC WG is considered a subordinate WG to the ISAG and the Minot OPSEC PM will brief the ISAG on OPSEC WG updates during scheduled ISAG meetings.

2.6.3. Voting. Voting may be accomplished during ISAG meetings or completed via e-mail. Meeting announcements, agendas and any required supporting material should be provided, as possible, to members prior to the meeting using the ISAG distribution list. Advisory members may be temporarily designated as voting members if the ISAG voting membership determines an issue directly affects their functional area of expertise.

2.7. ISAG Member Roles And Responsibilities. Commanders provide inputs to the ISAG through their appointed voting or advisory members. Members are appointed in writing to represent and act on behalf of their commander during ISAG meetings. Specific ISAG member roles are defined below:

2.7.1. The ISAG Chairman. The Chairman presides over meetings, provides leadership and guidance during meetings and ensures meetings properly address IP integration, requirements, prioritization, and HHQ requirements. The CIP acts as Chairman at meetings, if the 5 BW/CV is not present. Additionally, the Chairman:

2.7.1.1. Develops and publishes meeting schedules, coordinates agendas, and notifies members of meetings. When a formal forum is needed, Robert's Rules of Order should be used for conduct.

2.7.1.2. Ensures all ISAG responsibilities are executed. This may include requiring assigned members to assist in creation, coordination, prioritization, assessment, and monitoring the status of any identified IP-related issue.

2.7.1.3. Prepares, coordinates, and arranges presentation of ISAG recommendations and requirements to the 5 BW/CV and/or other senior leaders as new IP requirements are identified.

2.7.1.4. Assigns, manages and tracks open ISAG-related action items (e.g., assign tracking numbers, OPR and Office of Coordinating Responsibility (OCR), and suspense dates).

2.7.1.5. Coordinates with senior leaders, ISAG members, steering groups, and WGs, as needed.

2.7.1.6. Coordinates, approves and tracks any ISAG interagency correspondence (e.g., action items, HHQ updates/data calls, local tracking of items, etc.).

2.7.1.7. Coordinates, manages, publishes and approves ISAG-related information or administrative items, such as meeting minutes, public awareness articles, etc.

2.7.1.8. Coordinates with and provides oversight for ISAG subordinate WGs.

2.7.2. The ISAG Recorder. The Recorder will be a 5 BW/IPO member and provides administrative support and assistance to the Chairman for ISAG-related paperwork, meetings, activities, etc.

2.7.3. Voting Members. Voting members are kept to a minimum to enhance progress regarding resolving group issues. The agencies listed in **Table 2.1** below must have a representative appointed in writing by the owning commander. These SECENT subject-matter experts are empowered to vote on the appointing commander's behalf, in regards to SECENT- related issues, during ISAG meetings. Where possible, one POC is listed for agencies which have multiple SECENT-related disciplines. The representative is responsible to ensure proper unit representation is provided if a matter falls outside their primary field of technical expertise. Additional duties of the voting members include, but are not limited to:

2.7.3.1. Providing administrative and or technical support to the Chairman on SECENT- related actions. This may include producing, proofing or staffing correspondence; giving presentations and/or assisting to identify solutions for IP projects in their field of expertise.

2.7.3.2. Providing expert technical opinions on SECENT issues/requirements to help identify, prioritize and solve issues when new IP requirements are established or when vulnerabilities are noted. Support may be required verbally and/or in a written format.

2.7.3.3. Monitoring their area of functional expertise to identify new SECENT requirements. Any new requirements will be forwarded to the Chairman along with ideas for potential solutions or implementation strategies. Valid items will be added to the ISAG agenda for discussion or action, as appropriate. The initiating member is responsible to research issues, provide basic facts on the topic and suggestions for a course of action, prior to proposing agenda items.

2.7.3.4. Participating on designated WGs to identify/resolve new or existing SECENT requirements, as directed by the Chairman. This may include developing briefings on the topic for leaders.

2.7.3.5. Providing agenda items, validating new SECENT requirements and assisting with any resolution of noted issues. The member proposing an agenda item is responsible to provide research and references for an item, to the Chairman, prior to the meeting.

2.7.3.6. Accomplishing assigned action items within the established timeframes.

2.7.3.7. Identifying and providing specific functional experts for OPR/OCR actions.

Table 2.1. ISAG Voting Members.

Chairman (5 BW/CV or Chief, IP)
Information Security (5 BW/IPI)
Personnel Security (5 BW/IPP)
Special Security Office (SSO)/5th Operational Group (OG) representative
Cyber Security (5 CS representative)
Advanced Programs (5 BW/AP)
5 BW OPSEC PM
91 MW Exercises and Planning OPSEC PM
Note: ISAG Recorder is a 5 BW/IPO member

2.7.4. Advisory Members. Advisory members include those shown at **Table 2.2**. They participate in meetings and provide support when their specific functional expertise is needed. Their duties are basically identical to the voting membership with the exception of voting.

Table 2.2. ISAG Advisory Members.

5 BW/IPO - Industrial Security and Installation OPSEC Program Manager
5 BW Personnel Reliability Assurance Program (PRAP) Manager
5 BW Command Post (CP) Representative
5 BW Public Affairs (PA) Representative
5th Maintenance Group (MXG) Representative
5th Medical Group (MDG) Representative
91st Maintenance Group (MXG) Representative
91st Operations Group (OG) NPM/CNWDI/RD/FRD Representative
91 SFG Representative
5th Civil Engineer Squadron (CES) - Base Architect
5th Force Support Squadron (FSS) Representative
5 SFS, Resource Protection (5 SFS/S5R) - Physical/Nuclear Security
705th Munitions Squadron (MUNS) CNWDI/RD/FRD Representative
AF Office of Special Investigation (OSI) Representative

Chapter 3

INFORMATION SECURITY (INFOSEC) PROGRAM

3.1. Policy And Program Management. This chapter establishes guidance for protection of classified information and outlines the responsibilities of Minot AFB personnel in relation to complying with the INFOSEC program as outlined in DoD and AFI governing directives. The Minot AFB INFOSEC program is a part of the overall SECENT program and applies to all assigned units, to include tenant units, as required under support agreements between the tenant unit and 5 BW.

3.1.1. Policy. These policies/philosophies apply to protecting classified information and controlled unclassified information under the purview of relevant statutes, regulations and directives.

3.1.2. Program Management. Unit INFOSEC programs are an integral part of the overall unit SECENT program and will be managed IAW Executive Order (EO) 13526, DoD/AF implementing guidelines, supplements and this instruction. Commanders will consider corrective actions and sanctions as outlined in the basic guidance if individuals are found to have willfully or negligently violated rules of conduct in regards to controlling access, protecting, handling, safeguarding or transmitting material addressed under IP guidance IAW AFMAN 16-1404 to DoDM 5200.01 Volumes 1 and 3.

3.1.2.1. The CIP provides oversight for the INFOSEC program through 5 BW/IPI, which is the primary focal point for INFOSEC issues at Minot AFB. The INFOSEC specialist:

3.1.2.1.1. Acts as the primary AF SECENT activity coordinator for the CIP by coordinating/scheduling joint SECENT program reviews/CCIPs events.

3.1.2.1.2. Coordinates, monitors and validates unit responses in regards to deficiencies noted due to classified security incidents, CCIPs, or HHQ inspections.

3.1.2.1.3. Acts as the primary SECENT training coordinator and develops and distributes local course curriculum, as needed.

3.1.2.2. The USMs act as unit SECENT representatives and then CIP provides oversight to ensure they provide INFOSEC programs management for their commanders.

3.2. INFOSEC Related Programs. The INFOSEC specialist assigned to 5 BW/IPI is the primary focal point for INFOSEC matters at Minot AFB. Additional duties and responsibilities for units are provided in chapters **8 through 12** below which includes handling/storing sensitive information (classified or unclassified); marking, transmitting, safeguarding, training of sensitive information and the classified security incident program. These items are addressed in separate chapters to help clarify specific responsibilities, but are all integral parts of the INFOSEC and overall Minot AFB SECENT program.

Chapter 4

PERSONNEL SECURITY (PERSEC)

4.1. Policy and Program Management. This chapter establishes guidance for completion of PSIs and processing personnel to meet clearance eligibility needs. The Minot AFB PERSEC program applies to all assigned members, including civilian employees, active duty/guard/reserve military and contractors.

4.1.1. Criteria for Application of Security Standards. The criteria for determining eligibility for access to classified are found AFMAN 16-1405 to DoDM 5200.02, as supplemented by Security Executive Agent Directives (SEAD) 4, *National Security Adjudicative Guidelines*, SEAD 3, *Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position* and SEAD 8, *Criteria for Temporary Eligibility* (formerly interim). All commanders must apply these standards when granting access to classified, to include ensuring reporting occurs as outlined in SEAD 3.

4.1.2. Program Management. The Minot AFB PERSEC program is managed by 5 BW/IPP for the CIP, IAW AFMAN 16-1404 to DoDM 5200.01, Volumes 1-3, *Information Security Program*; AFMAN 16-1405 to DoDM 5200.02, *DoD Procedures for the Personnel Security Program (PSP)*; supplementing DoD and AF guidance and this instruction.

4.2. Duties and Responsibilities. The CIP implements and provides oversight of the PERSEC program on behalf of the 5 BW/CC through the 5 BW/IPP. Tenant units must comply with Minot AFB PERSEC program requirements to receive support from 5 BW/IPP.

4.2.1. Commander and Staff Agency Chief Responsibilities. Referred to as commanders for the remainder of this chapter, Commanders and Staff Agency Chiefs implement and provide oversight of the PERSEC program for their units through their appointed USM. This includes completion of required SAs, preparation for SAs and CE monitoring/reporting requirements associated with AFMAN 16-1405 to DoDM 5200.02, Enclosure 2, paragraph 2.13.i. and SEAD 3.

4.2.2. Servicing Security Activity. The IPO PERSEC specialist acts as the Servicing Security Activity for Minot AFB PERSEC on behalf of the CIP.

4.2.3. Authorized Requestor. The 5 BW/IPO is the only authorized requester for Minot AFB PSI Tier 3 and Tier 5 actions. Specific actions and responsibility are outlined in AFMAN 16-1405 paragraph 5.2.

4.2.3.1. If a tenant unit is supported by the 5 BW/IPO, the fact they will comply with local requirements will be outlined in the Base Support Agreement.

4.2.3.2. If a tenant unit performs their own PERSEC functions, no PSI support is provided by the 5 BW/IPO. This does not preclude providing technical assistance on a short-term basis, mission permitting, e.g., allowing use of IPO fingerprint machine if the tenant temporarily loses this capability.

4.2.3.3. The Civilian Personnel Section (CPS) and Human Resources Office (HRO) are designated as the sole submitting agency for Tier 1, 2 and 4 (non-sensitive) PSI cases. As noted above, this does not preclude short-term technical assistance, as mission permits. The IPO is not authorized to routinely conduct initiation, review or submission of PSIs relating to suitability and fitness for military, civilian or contractors, IAW AFMAN 16-1405 to DoDM 5200.02, Section 4, 4.1.b.(5).

4.2.3.4. The CPO or HRO will submit PSI initial civilian hire PSIs for non-critical, special and critical sensitive positions. The servicing IPO is responsible for approval of requested investigations.

4.2.4. Unit Security Managers. The USM is the focal point for management of the unit PERSEC programs;

4.2.4.1. Unit members will route any questions to IPO through their USM, they will NOT contact the IPO directly.

4.2.4.2. Members must complete required training outlined in AFMAN 16-1404 and this instruction before being indoctrinated for access in the database.

4.2.4.3. If derogatory information brings a member’s trustworthiness, loyalty, or honesty into question, commanders will make required Continuous Evaluation (CE) notifications and evaluate whether access should be suspended IAW AFMAN 16-1405, paragraph 9.2.d.(1) and the adjudicative guidelines outlined in SEAD 4. The PERSEC Specialist assists USMs and commanders with review of the adjudicative guidelines when derogatory information is received on members and on determining if reporting is required IAW SEAD 3.

4.2.4.4. Access to special material will be based on the specific rules for the program.

4.3. Management of the Database of Record. The Defense Investigative Service System (DISS) or successor system National Background Investigation Services (NBIS) is the "database of record".

4.3.1. Notifications. Commanders will ensure unit procedures require the USM be notified of any of the following:

4.3.1.1. In/out-processing of unit members or position changes which place assigned military or civilian members in a new UMD position. This ensures the database of record properly reflects status of all assigned unit personnel.

4.3.1.2. Discovery of potential derogatory information concerning assigned unit members. This ensures adjudicative guidelines are reviewed and CE reports are accomplished.

4.3.1.3. Decisions on whether access to classified and/or computer systems will continue if a CE or other report of potential derogatory information is generated. This ensures any access is considered against the applicable adjudicative guideline.

4.3.1.4. Failure to notify the USM of these items may result in unauthorized access to sensitive information, which may cause a classified security incident and, IAW SEAD 3, a CE report on the individual who failed to make the notification.

4.3.2. Unit Management. The USMs are the unit's sole focal point for managing database of record. They must maintain their unit's data IAW AFMAN 16-1405 to DoDM 5200.02, supplemental guidance and in this instruction.

4.3.2.1. The USM is responsible for all requirements AFMAN 16-1405 to DoDM 5200.02, as supplemented and this instruction. This includes, but is not limited to, the following:

4.3.2.1.1. In/out-processing unit personnel into/out of the DISS or successor system NBIS.

4.3.2.1.2. Using the investigation closed date in database of record to determine when unit members are submitted for periodic review (PR) investigations.

4.3.2.1.2.1. Note: If enrolled for Deferred Investigation, the PR due date is based on the Deferred enrollment date. If enrolled for "Other", regardless of the enrollment date, the PR due date is based on the last Investigation Closed Date.

4.3.2.1.3. Updating, monitoring and acting on notifications received in the database of record for assigned personnel (e.g., CE notifications, in/out-processing, completing SF 312 if needed, etc.).

4.3.2.1.4. Recording and removing applicable accesses IAW with database of record requirements, e.g., using the grant access link, including any applicable special access programs.

4.3.2.1.5. Annotating completion of the SF 312, *Classified Information Nondisclosure Agreement* (NdA) in the database of record using the grant access link and mailing completed NdAs on a weekly, monthly or quarterly schedule to: AFPC/DP1ORM, 550 C Street West, JBSA-Randolph TX 78150.

4.3.2.1.6. Tracking visit request notifications in the database of record. This may include sending, receiving or rejecting the visit request, as required.

4.3.2.1.7. The unit commander is responsible for ensuring the USM monitors and updates DISS or successor system NBIS for SEAD 3 Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.

4.3.2.1.8. The USM will not upload CE incidents; the PERSEC specialist will oversee upload of these reports.

4.3.2.2. The USM will protect all information associated with the database of record as PII and report improper release or access as a PII breach.

4.3.2.3. The USM will be responsible to ensure units sponsoring classified mass briefing events use procedures found at **paragraph 4.8** below to allow entry to the briefing.

4.3.3. Controlling Database of Record Information. The database of record is a real-time system which is continuously updated. Printing hard copy products for use in validating access levels defeats the purpose of the system's real-time function and is prohibited, IAW database rules.

4.3.3.1. Hard copy products will NOT be printed to be used by personnel/agencies to verify clearance data. Clearance can only be validated by the USM via the system of record.

4.3.3.2. The USM will ensure personnel not performing USM duties who require access to DISS or successor system NBIS are processed as follows:

4.3.3.3. The commander submit a request letter to 5 BW/IPO stating personnel listed require "read only access." Access will be granted using Security Officer Visit Admin access in DISS or successor system NBIS.

4.3.3.4. The USM will complete the DD Form 2962, Personnel Security System Access Request, and validate appointed individuals have completed required training identified on the USM training tracker for Security Officer Visit Admin access.

4.3.3.5. The USM will maintain a copy of the appointment letter and training certificates in the USM binder. The IPO will maintain a copy of the appointment letter in the unit folder.

4.4. Processing PSIs (e-QIP or successor system eApp). The USM will use the e-QIP or successor system eApp system to submit, track and process security clearances initial or PRs. This requires completion of actions in a timely manner to prevent negative impact on daily mission, TDYs, deployments, etc. The basic guidance in AFMAN 16-1405 to DoDM 5200.02 requires personnel submitted have at least 1 year retainability.

4.4.1. Submission of PSIs. The USM submits Tier 3 and 5 personnel for initial or periodic review PSIs based on assigned UMD SAR codes.

4.4.1.1. Investigative request will not be submitted for eligibility higher than what has been designated for the position or required for the duty to be performed.

4.4.1.2. In the case of civilian employees hired where a UMD SAR code does not yet exist for the job, the PD on file with the civilian personnel office (CPO) may be used to determine authorized access levels until the UMD is updated.

4.4.1.3. If there is a conflict between the UMD and PD, the UMD takes precedence. If the position is term hire the PD is used to grant access.

4.4.2. Individual Responsibilities. Each member must complete paperwork associated with a PSI (e-QIP or successor system eApp) within established timelines, failure to complete reinvestigation requirements could result in a CE incident for Personal Conduct “failure without reasonable cause complete security forms.

4.4.3. Initial Tier 3 and Tier 5 Civilian PSIs. PSIs for civilian employees requiring a Tier 3 or Tier 5 PSI are reviewed and submitted by the Civilian Personnel Flight (CPF) to the IPO, IAW AFMAN 16-1405 to DODM 5200.02, Section 4, paragraph 4.1.b.(3).

4.4.3.1. The CPF will validate the member does not have an existing, valid PSI in the database of record before submitting for an initial PSI.

4.4.3.2. Access to Secret material requires a SAR code 7 on the UMD and a current or submitted TIER-3 PSI.

4.4.3.2.1. Prior service members hired for a SAR code 7 UMD position with an in-scope (less than 10 years old) TIER-3 or TIER-3R or TIER-5 do not require a new PSI unless there was a break in service of over 24 months.

4.4.3.2.2. Members selected for a SAR code 7 UMD position not meeting one of the above requirements must be submitted for a TIER- 3 PSI **before** being eligible for temporary Secret access.

4.4.3.3. Access to TS requires a SAR code 5 on the UMD and the member must be submitted for a TIER-5 PSI.

4.4.3.3.1. Prior service members filling a SAR 5 code UMD position with an in-scope (less than 5 years) SSBI, TIER-5 or TIER-5R do not require a new PSI unless there was a break in service of 24 months or more.

4.4.4. Documentation of PSI Forms. The USM is responsible to ensure required forms and documentation are properly accomplished for submitted PSI requests. This includes:

4.4.4.1. Ensuring all forms (e.g., NdA, AF Form 2587, *Termination of Security Access*, etc.) are accomplished and maintained as required.

4.4.4.2. Use procedures from AFMANs 16-1401 and 16-1404 for completing and maintaining forms. Examples are available on the IP SharePoint.

4.4.5. Unacceptable or Discontinued Cases. The USM will contact 5 BW/IPP immediately for further instructions if a case is returned by Office of Personnel Management (OPM) as unacceptable or discontinued.

4.4.6. Contact with Adjudicators. The 5 BW/IPO is sole the focal point for contacting DoD Central Adjudicative Services (CAS) priority tracking program or making inquiries to OPM. The USM will never contact these agencies unless directed to by 5 BW/IPO in response to requests for information by the agencies.

4.4.7. Timelines for e-QIP or successor system eApp. Failure to comply with local timelines will result in the e-QIP or successor system eApp account being terminated. The 5 BW/IPO may modify these timelines, if verifiable justification is provided by the USM on why an extension is required. The local procedures are:

4.4.7.1. The USM makes the request to 5 BW/IPP for first time establishment of the account.

4.4.7.2. If the initial account terminates, the unit commander must request reopening.

4.4.7.3. The second time an account terminates, the 5 BW/IPP will notify the commander, through the USM, to consider CE actions under the Adjudicative Guideline of "Personal Conduct" for failing to complete/provide security background information.

4.4.7.3.1. Once the commander completes the CE evaluation, a third account will be established.

4.4.7.4. If the third time an account terminates, the 5 BW/IPO will notify the first O-6 in the organizational chain of a negative trend for CE consideration under the noted Adjudicative Guideline and a failure to comply/obey.

4.4.7.5. The noted e-QIP or successor system eApp procedures apply ONLY to accounts which are generated under oversight of the SMO 585G for the 5 BW/IPO.

4.4.7.6. When an initial hire civilians requires a PSI action, it is submitted by CPF using the above procedures and the 5 BW/IPO is the approving official.

4.4.7.7. The USM will use the following rules for submitting PSIs:

4.4.7.7.1. All e-QIP or successor system eApp requests must be submitted NLT 1300 hrs.

4.4.7.7.2. The 5 BW/IPP attempts to create the account on day received.

4.4.7.7.3. Once created, subject has 5 days to enter account or it terminates.

4.4.7.7.4. Once member enters account there are 10 days to complete upload and review by USM.

4.4.7.7.5. Once uploaded the 5 BW/IPP will attempt to submit to National Background Investigations Bureau (NBIB) or defer the investigation, as appropriate, within 2 weeks.

4.4.8. Temporary Clearances. The following procedures for temporary access to classified were reviewed and approved by AFGSC/IP as meeting minimum requirements outlined in SEAD 8 and AFMAN 16-1405 to DoDM 5200.02. The USM will ensure:

4.4.8.1. All temporary clearance requests are coordinated through the 5 BW/IPP prior initiating a commander's risk assessment.

4.4.8.1.1. Note for civilian personnel please review CPO hiring waiver memo, signed by commander prior to subject’s hire.

4.4.8.1.2. The owning unit commander completes a risk assessment based on available information using the Adjudicative Guidelines, SEAD 8 and AFMAN 16-1405 to DoDM 5200.02.

4.4.8.2. A commander's risk assessment is completed and includes a review of the member's completed SF 86, along with the AF Form 2583, until a final adjudication is received.

4.4.8.3. The Minot AFB Temporary Access instruction document, to include the SF 86, the AF Form 2583 Minot instructions document and associated templates (see attachments **9** and **10** of this instruction) is completed and reviewed by the approving commander to ensure all mandatory actions, cautions and concerns are considered.

4.4.8.4. Access will NOT be granted prior to completion of these mandatory actions.

4.4.8.5. Temporary access is documented using the completed SF 86, AF Form 2583 and adding the member to any applicable unit classified access lists.

4.4.8.6. Provide the member a copy of the completed SF 86 and AF Form 2583, regardless of approval or disapproval, as written notification of the decision.

4.4.8.7. Coordinate with any off-installation locations to determine if they will accept the Minot AFB temporary access decision.

4.4.8.7.1. If the gaining site will not accept the temporary access decision, the USM will notify the applicable unit agencies of the decision for their action.

4.4.8.8. If personnel are being sent to Minot AFB from another installation, the gaining unit commander must determine if the sending location's temporary access procedures will be accepted. They should consult with their USM and the 5 BW/IPP if there are questions on this topic.

4.4.8.9. Top secret temporary access is covered in SEAD 8 rules and requires different actions/checks. Specifically;

4.4.8.9.1. Secret (or DoE “L”) access requires a completed SF 86, citizenship verification (by the USM) initiation of the required investigation AND completion of a FAVORABLE FBI fingerprint check. ALL these actions MUST be completed BEFORE the commander can grant temporary access.

4.4.8.9.2. Top secret (or DoE “Q”) access requires all of the above AND completion of an FBI Name Check (may take 3-6 months) and completion of an FBI National Crime Information Center (NCIC) check (may also be 3-6 months, but will run concurrent with the FBI Name Check).

4.4.8.9.3. Regardless of access level, access must be restricted to only information needed for mission essential duties. This must be clearly6 outlined at Block 30 of the 1583. Access beyond what is specified on Block 30 may be considered a security incident.

4.4.9. Suitability, Adjudication and HSPD-12 PSIs. The 5 BW/CC designates 5 FSS/FSC as the agency responsible to process Tier 1, 2 and 4 and background/fingerprint checks for childcare. Where possible, to enhance continuity for USMs, use the rules associated with processing Tier 3 and 5 PSIs.

4.4.10. Child and Youth Program (CYP) PSIs. These investigations are related to suitability and adjudication and conducted by 5 FSS/FSC IAW guidance found in AFI 34-144 for employees and/or volunteers working with/around children.

4.4.11. Suitability Determinations. If OPM or the FBI fingerprint check is returned with derogatory information on an applicant a suitability determination is required.

4.4.11.1. A suitability determination is also required if OPM does not return a favorable adjudication on an investigation.

4.4.11.2. The 5 FSS/FSC will coordinate with units on actions required for suitability cases using procedures as directed by AFGSC/A1C

4.5. CE and Reporting Requirement. (SEAD 3) All personnel must continuously monitor themselves and others and report any potentially derogatory information to the USM, supervisor or commander as soon as possible after the event. Additionally:

4.5.1. Commander Responsibilities. Unit commanders must establish procedures to ensure required notifications are made in the appropriate database as outlined in AFMAN 16-1405 to DoDM 5200.02 Section 11; SEAD 3; SEAD 4 and this instruction. This includes documenting travel outside the US, disclosure of foreign contacts and CE up/down-channel notifications. If potentially derogatory information is reported the commander will:

4.5.1.1. Use the SEAD 3 and SEAD 4 adjudicative guidelines, in collaboration with 5 BW/IPO to determine if a CE report is initiated. This determination must be completed within 72 hours of receipt of unfavorable information (i.e., 3 duty days) if foreign intelligence entity is involved.

4.5.1.2. Determine whether access is formally suspended or not on initial determination. Once access is formally suspended in the database of record, it may only be reinstated by DoD CAS.

4.5.1.2.1. Commanders may locally or formally suspend access at a later date if additional derogatory information is uncovered.

4.5.1.2.2. Access may be locally suspended by the commander IAW AFMAN 16-1405 to DoDM 5200.02, Appendix 7A, 7A.2.a.(1).

4.5.1.3. Notify the 5 BW/IPO to ensure all required CE notifications are accomplished. Also consider coordinating with the 5 BW Judge Advocate (JA) prior to taking formal suspension actions to ensure due process for the member is protected.

4.5.1.3.1. If the member is Sensitive Compartmented Information (SCI) indoctrinated or has access to a Special Access Program (SAP), also notify these program managers of the decision.

4.5.1.4. Include a requirement for other unit agencies, e.g., First Sergeant, supervisors, etc., to notify the USM in the unit’s SECENT OI. This will ensure any potentially derogatory information can be reviewed against Adjudicative Guidelines to determine if CE reporting is required. Also ensure:

4.5.1.4.1. The OI provides USM access, as needed, to personnel records needed to determine eligibility and reliability; it is acceptable for the USM to go through a focal point (e.g., first sergeant) for access to this type of information.

4.5.1.4.2. The OI clarifies reporting of this information within specified CE program timelines is mandatory and failure to report within timelines may generate a CE report on the individual who failed to report.

4.5.1.4.3. The OI clarifies the USM will contact 5 BW/IPO for technical assistance if unsure on actions to take or unclear on whether SEAD 3 and SEAD 4 criteria apply.

4.5.1.5. Ensure procedures are in place to notify the USM for CE reporting purposes when a member is suspected of abuse or misuse of a government issued credit card or spending accounts IAW AFMAN 16-1405 to DoDM 5200.01, Section 11. This should be included in the unit SECENT OI.

4.5.1.6. Ensure procedures are in place to deny access and initiate a CE report for any individual who refuses to sign an NdA. This should be included in the unit SECENT OI.

4.5.2. USM Responsibilities. The USM will:

4.5.2.1. Review derogatory CE information received against SEAD 3 and SEAD 4 adjudicative guidelines and recommend appropriate actions to the commander and assist with up channeling notifications through the 5 BW/IPO to DoD CAS and AF C-InT Cell.

4.5.2.2. Ensure an AF Form 2587 is completed anytime a CE action results in suspension of access to classified information.

4.5.2.3. Notify the 5 BW/IPO when an individual with an open CE report is projected for permanent change of assignment/station or TDY.

4.5.2.3.1. Ensure the 5 BW/IPO receives a memorandum from the commander at least 10 days prior to the member's departure.

4.5.2.3.2. Ensure a copy of orders is received as soon available so the 5 BW/IPO can forward the CE to the gaining base to allow the gaining unit commander to review the CE contents.

4.5.3. Counterintelligence (CI) Reporting. Security professionals at Minot AFB will share potentially derogatory information discovered with each other and with the lead Minot CI agency (AFOSI Detachment 813). The CI agency will share information with the 5 BW/IPP, if sharing the information does not violate the integrity of an on-going investigation.

4.5.3.1. The 5 BW/IPP office will notify the CI agency when potentially derogatory information of a criminal nature is reported on members through the adjudicative process.

4.5.3.2. The 5 BW/IPO will notify the CI agency if a security incident report indicates an unauthorized disclosure occurred due to a member improperly releasing or mishandling classified or sensitive information. Security incident reports will be made available to the CI agency, upon request.

4.5.3.3. If the CI agency takes action on CE notifications provided by the 5 BW/IPP office they should provide a case number, which is required by the DoD CAS.

4.5.3.4. The CI agency will ensure commanders are aware of the need to consider adjudicative guidelines for actions which result in investigation. This may be accomplished by including the CE requirement on the checklist used to brief commanders.

4.6. Granting Access.

4.6.1. Identifying Access Levels for Positions. Commanders determine the level of access necessary for each military and civilian position based on the mission needs. The commander reflects these decisions on the UMD by ensuring position numbers carry the appropriate SAR.

4.6.1.1. Civilian positions also have a position sensitivity identified on their PD which must match the SAR code on the UMD. The USM must work closely with supervisors when position descriptions are created to ensure the proper PS code is reflected on the PD. If there is conflict between the UMD and PD, the UMD takes precedence until the conflict is resolved.

4.6.1.2. Access may never exceed the SAR code for the position. For example, if a unit member has TS eligibility but is assigned to a UMD position allowing only Secret- level access—they may only be granted Secret access. Additionally, reinvestigations for the individual will be based on the current UMD SAR code of Secret—not the previous eligibility of TS.

4.7. Annual UMD Review. Commanders will conduct an annual review of the UMD between 1-15 May and document the review as of 15 May, IAW AFMAN 16-1405 requirements. The USM is the focal point for this review and will inform 5 BW/IPP when it has been completed. They will use guidance provided by 5 BW/IPO to conduct the review. The USM will maintain a signed copy of the commander's review in the USM binder.

4.8. Minot AFB Visit Request/Servicing Plan. When distinguished visitors, inspection teams or other groups are scheduled to visit Minot AFB, and will need access to classified information, use the following procedures to ensure they can gain access to classified.

4.8.1. Inspection Teams. The USM responsible for the organization being inspected will receive the team visit request in DISS or successor system NBIS for the duration of the visit and will validate the DISS or successor system NBIS access matches the access listed on the entry authority list (EAL).

4.8.1.1. If the inspection is wing-wide the 5 SFS and/or the 91 SFG USM, as applicable, will receive the DISS or successor system NBIS Visit Request and conduct the validation.

4.8.1.2. If the inspection is unit-specific (e.g., one specific squadron or group being inspected), the USM for the inspected agency will receive the DISS or successor system NBIS visit request and will conducted the validation.

4.8.2. Special Visits. If a special speaker or event requires mass briefings of classified, the USM for the unit sponsoring the event is responsible for ensuring personnel attending send a Visit Request for the event. The sponsoring USM will validate clearance access for attendees.

4.8.3. Validation Procedures. Find and accept the visit request and verify the individual is indoctrinated and meets minimum requirements outlined on the inspection EAL or the event access list. If issues are noted; DO NOT accept the visit and contact the event sponsor. Examples of issues include:

4.8.3.1. The individual does not have the required investigation for the briefing level.

4.8.3.2. The individual is NOT indoctrinated at the proper level for briefing (e.g., indoctrinated to secret, but briefing is at TS level).

4.8.3.3. A completed SF 312 is not showing in the system for the member.

4.8.3.4. The briefing contains special access information (e.g., NATO, RD, CNWDI, etc.) but the member is not indoctrinated for the needed access.

4.8.4. Mass Briefings of Classified for Local Units. It is acceptable to use the above procedures to generate an access list for allowing entry to local classified briefings.

Chapter 5

INDUSTRIAL SECURITY PROGRAM

5.1. Policy and Program Management. This chapter establishes guidance for implementing the National Industrial Security Program and outlines the responsibilities of Minot AFB personnel in relation integrating contractors into the SECENT program.

5.1.1. Policy. It is AF policy to identify what access industry will have to information or sensitive resources (regardless of classification, sensitivity, physical form, media or characteristics) which must be protected against compromise and/or loss while entrusted to industry in the performance of classified contracts.

5.1.1.1. The primary focus of INDUSEC is to review contracts working with classified (cleared), but technical assistance for contracts not dealing with classified (uncleared) may be provided, as manning allows. The Minot AFB SECENT program applies to all assigned units, to include tenant units, as required under support agreements between the tenant unit and 5 BW.

5.1.1.2. Prior to allowing access to contractors, a valid need-to-know (NTK) requirement must be established. A valid DD Form 254, VAL or visit request, and a VGSA or other local document, is used to verify contractors are authorized access and meet all local access requirements IAW DoDM 2220.22,Volume 2_AFMAN 16-1406, Section 4 & 5.

5.1.2. Program Management. This program is managed IAW DoDM 2220.22_AFMAN 16-1406, as supplemented, and this instruction.

5.1.3. Scope. The security polices, requirements and procedures identified in this chapter apply to all AF personnel and any on-base DoD contractors performing services at Minot AFB under the terms of properly executed contract and DD Form 254 and associated VGSA or similar document as determined appropriate by the installation commander. Access to classified/sensitive material will be denied if it is not clear whether the required contractor has the required investigation; if it is unclear whether the required DD Form 254 has been completed and or if a VGSA (or local document) has not been accomplished per DoDM 2220.22_AFMAN 16-1406.

5.2. Duties And Responsibilities.

5.2.1. The 5th Bomb Wing Commander. The 5 BW/CC responsibilities are outlined in AFMAN 16-1406, Section 2.8.e.

5.2.1.1. The CIP is delegated all duties and responsibilities for the INDUSEC program on the behalf of the commander.

5.2.2. CIP Duties. The CIP implements the Minot AFB INDUSEC program on behalf of the 5 BW/CC. In addition to the above delegated duties, the CIP is responsible for items outlined in AFMAN 16-1406, Section 2, paragraph 2.8.f.

5.2.2.1. The 5 BW INDUSEC specialist oversees and administers the INDUSEC program on behalf of the CIP, IAW AFMAN 16-1406.

5.2.3. Minot AFB Contracting Officers. The contracting officer responsibilities are outlined in AFMAN 16-1406, Section 2, paragraph 2.8.g. and include the following:

5.2.3.1. Negotiate contractual agreements, blanket purchase agreement, modifications, changes, revisions with all contractors assigned to Minot AFB.

5.2.3.2. Notify 5 BW/IPO within 30 days anytime an initial review of an agency's proposed statement of work (SOW) or performance work statement (PWS) indicates a job will require a contractor to have access to classified material. This must be accomplished prior to the award of a contract.

5.2.4. Commander Duties. Commanders will ensure assigned personnel comply with this instruction and the DoD/AF basic directives when allowing contractors access to classified. Management and oversight of the unit program is accomplished through their appointed USMs.

5.2.5. Key Management Officials. These individuals are normally the chief executive officers of the company. Management Officials will:

5.2.5.1. Appoint, in writing, a primary and assistant Facility Security Officer (FSO) for each on- base integrated visitor group (VG) and provide a copy of the appointment letter to the USM and 5 BW/IPO within 30 days after performance start date.

5.2.6. On-Base Security Representatives. If no FSO is present on the installation, a security representative will be designated by management officials to handle routine security needs and they act as liaisons between the company and the 5 BW/IPO. On-base security representative duties include:

5.2.6.1. Providing 5 BW/IPO with a current copy of the SOW or PWS.

5.2.6.2. Providing current visit requests of all contract-related visits via DISS or successor system NBIS to MPGSFDH55. **Note**: If the contractor does not have DISS or successor system NBIS capability, they will submit a hard-copy visit request which meets all requirements in DoDM 5220.32, Volume 1, Section 10.3 and this instruction.

5.2.6.2.1. Ensure the visit request is updated any time there is a change in employees' status, e.g., removal from employment, name change, clearance status changes, etc.

5.2.6.3. Ensuring all employees receive required DoD, AF and local SECENT training.

5.2.6.4. Ensuring all employees are indoctrinated in the database of record for the level of access to classified stated on the DD Form 254 and are debriefed, as required.

5.2.6.5. Conducting an annual review of the VGSA with the USM during the SECENT annual self- assessment.

5.2.7. USM Duties. The USMs are responsible for complying with the AFMAN 16-1406 and this instruction. If new classified contracts are being planned, the USM will ensure the 5 BW/IPO is immediately notified. They will also:

5.2.7.1. Include cleared contractor VGs in the unit SECENT program and ensure.

5.2.7.1.1. Inclusion in unit self-assessments.

5.2.7.1.2. The VG completes all required training for classified access.

5.2.7.1.3. The VG requirements are considered in the unit SECENT OI.

5.2.7.2. Ensure a VGSA is established with each VG performing duties for the unit to cover local security requirements. The VGSA will:

5.2.7.2.1. Clarify, define and expand security and training requirements from SOW and DD Form 254 to ensure all local requirements are included.

5.2.7.2.2. Participation in annual unit self-assessments, CCIP events and/or inspections.

5.2.7.2.3. Be coordinated through the 5 BW/IPO for a technical review prior to formal routing for final signatures.

5.2.7.3. Maintain all VG documentation in the USM handbook IAW **paragraph 1.10.10**.

5.2.7.3.1. If the unit has no industrial contractors the USM will place an Memorandum For Record (MFR) in the Tab stating the "Unit has no industrial contracts."

5.3. Cleared Contractor Access. Prior to allowing access to Minot AFB classified, the USM will take the following actions for cleared contractors to ensure access is authorized:

5.3.1. Database of Record Management. The USM will advise the 5 BW/IPO of visit request changes (i.e., new or terminated employees) and update the Personnel Security Management Network (PSM-net). The USM will use the following procedures to update the PSM-net:

5.3.1.1. Verify the contractor has the correct investigation for the level of access specified in the DD Form 254 and has completed any required training before in-processing to servicing or allowing access to classified material.

5.3.1.2. Input cleared contractors to "owning" status in the PSM-net for the duration of the visit request. This ensures the unit and 5 BW/IPO are notified on any changes to status.

5.3.1.3. When employees are terminated the USM will accomplish the following:

5.3.1.3.1. Remove employee from PSM-net by inputting an effective end-of-visit date.

5.3.1.3.2. Notify 5 BW/IPO of the change.

5.3.1.3.3. Notify personnel where the contractor had access of the change of status and ensure container custodians conduct an inventory of classified.

5.3.1.3.4. Accomplish any other needed actions, e.g., change combinations to containers, update SF 700, etc.

5.3.2. Employee Changes. The USM will ensure the VGSA requires management officials/security representatives to accomplish the following actions when an employee's status changes:

5.3.2.1. The FSO provides updates the visit request any time employees status changes occur.

5.3.2.2. The security representative completes any needed administrative actions if access is terminated, e.g., AF Form 2587, etc.). If the security representative is not available (e.g., small or single-person VGs) the USM performs this function. In either case, the USM will maintain a copy of the documentation.

5.4. Reporting Requirements. The USM will ensure the VGSA covers the following reporting requirements.

5.4.1. Security Incidents. Ensure procedures outlined in **chapter 12** of this instruction are used if a security incident with Minot AFB classified is suspected concerning on-base contractors.

5.4.2. Cleared Contractor Responsibilities. Cleared contractor working at Minot AFB will notify the servicing USM of any classified security incidents and take actions IAW with this instruction.

5.4.3. Reporting Derogatory or CE Information. The FSO will ensure 5 BW/IPO is notified of any incidents or information which is not local, but involves an employee authorized access on the visit request.

5.4.4. HHQ Reporting. The 5 BW/IPO will up-channel local clearedcContractor incidents to HHQ IAW AFMAN 16-1406.

5.4.5. Procedures for Suspicious Contacts. Report any cleared contractor involved in suspicious contacts/events, such as possible espionage, suspected sabotage, acts of terrorism, or subversive activities, IAW DoDM 5220.32, Volume 1, Section 8.2.

5.5. Contractor Release of Information. Contractor's requests for public release of information will be IAW DoDM 52220.12, Volume 1, Section 6.5. Contractors who receive requests for release of public information will follow the requirements outlined on block 12 of the DD Form 254/local requirements.

5.6. Unclassified (Uncleared) Contracts. These are contracts which do not require contractors to access classified information but still require access to the installation, the Air Force Network (AFNET), or special areas. The 5 BW/IPO is not manned to provide support for these contracts. However, technical support may be provided, as manpower allows, at the request of 5th Contracting Squadron (5 CONS). Where possible, a standardized security requirement template for these contracts should be developed jointly by 5 BW/IP and 5 CONS.

5.6.1. Review of Uncleared Contracts. If an INDUSEC review of an uncleared contract is accomplished, it will be based off the requirements in the PWS/SOW provided by 5 CONS.

5.6.1.1. The security review will focus on items such as need for access to CUI material, defining CUI protective requirements, outlining OPSEC requirements and establishing minimum needed security training and/or education, etc.

5.6.2. HSPD-12 Requirements. Any agency other than 5 CONS which solicits contracts at Minot AFB (e.g., Army Corps of Engineers, Army, Air Force Exchange Services (AAFES), Defense Commissary Agency (DECA), etc.) will notify the 5 FSS/FSC if the initial review of the contract appears to require the contractor/company to need access to the installation or CUI material. The agency soliciting the contract will ensure the PWS addresses the fact the contractor must meet the background check requirements outlined in HSPD-12.

5.6.3. Trustworthiness Determinations. If an uncleared contractor requires a Tier 1, 2 or 4 PSI, the USM will process the PSI using procedures noted in **chapter 14** of this instruction.

Chapter 6

CYBER SECURITY

6.1. General Information. Information, regardless of its format, will be protected IAW guidelines established in DoDI 5200.48_DAFI 16-1403 and DoDM 5200.01, Volumes 2 and 3, as applicable.

6.2. Information Processing Equipment Used With Sensitive Data. Refer to DoDM 5200.01, Volume 2, Enclosure 3, Section 18 and Volume 3, Enclosure 3, Section 17. and AFMAN 16-1404 to DoDM 5200.01, Volume 3 for specifics on equipment such as fax machines, copiers, scanners, automated information systems (AIS), etc., used with classified. Comply with Cyber guidance and DoDI 5200.48_DAFI 16-1403 for CUI. All Information Processing Equipment and software procured for use on Minot AFB networks and information systems will be compliant with Common Criteria requirements and certified/approved for use. Visit **https://www.commoncriteriaportal.org** for more information.

6.2.1. CUI Reproduction. All, or almost all, printers, copiers, scanners, or fax machines connected to the NIPRNET retain data. Authorized holders must ensure these devices are sanitized when taken out of service in accordance with NIST SP 800-88, per DoDM 5200.01, Volume 3, Enclosure 2, Section 14—inclusive.

6.2.1.1. Any copier leased through Defense Automation Printing Service (DAPS) has volatile memory and does not maintain an image of information after powered down. These copiers can be turned over to the contractor after they have been powered down.

6.2.1.2. If units purchase copiers/scanners or lease a copier through an agency other than DAPS the unit is responsible to ensure copier hard drives are purged or removed prior to releasing the copier to ANY other agency—even another base agency. In this case the unit may contact Wing Cyber Security Office (WCO) for the necessary steps to clear the device. This may include removing and destroying the hard drive.

6.2.1.3. Failure to complete the purge of a copier/scanner without volatile memory may result in a Privacy Act Breach being reported and prosecution for violation of the Privacy Act. Improper release of other types of CUI may also subject to prosecution under other federal guidance.

6.2.2. Copiers/Scanners Used for Classified. Copy machines/scanners approved for classified must either reside in an area approved for storage of the highest classification approved for reproduction or have a hard drive sanitization kit installed that purges all memory/hard drives after each use. Additionally, a copier must:

6.2.2.1. Have an approval letter which:

6.2.2.1.1. States the copier checklist at **Attachment 4**, developed by the WCO and 5 BW/IP, was used by the USM to determine the copier meets minimum standards.

6.2.2.1.2. Includes clearing instructions, (e.g., minimum number of blanks needed to purge latent images or any other requirements).

6.2.2.1.3. Is signed by the commander approving the copier for use with classified.

6.2.2.2. Copiers/scanners approved for classified use must also be clearly identified with a sign stating "authorized for classified use”.

6.2.2.3. If both classified and unclassified copy machines/scanners are collocated in an area, each device will be clearly identified as either approved or not approved for classified use. Unclassified copiers in a classified processing area will ALWAYS be labeled as "NOT AUTHORIZED FOR CLASSIFIED."

6.2.2.4. If the copier/scanner is networked, it must be marked and protected IAW AIS marking and protection standards discussed in **paragraph 6.3** below.

6.2.3. Use of Nonstandard Devices. Commanders will coordinate the use of any nonstandard processing equipment (e.g., hand-held data devices, flash memory, USB port devices, etc.) through the WCO prior to purchase or use with CUI or classified information. Further guidance can be found in AFMAN 17-1301.

6.2.4. Digital Senders. Digital Senders are considered a Multi-Function Device (MFD) and are only authorized for use with CUI on the NIPRNet if they have the required CAC enabled security and are properly configured IAW the guidance in the Sharing Peripherals Across the Network (SPAN) Security Technical Installation Guide (STIG) and AFMAN 17-1301.

6.2.4.1. If MFDs retain data, and if used with CUI, must be properly handled when retired from service the same as a copier used with CUI (e.g., hard drive wiped or destroyed).

6.2.4.2. The use of MFDs is not authorized on the SIPRNet at Minot AFB, unless authorized by Designated Approval Authority (DAA) approval, addressed in the MFD STIG.

6.2.4.3. Digital Senders must have an appropriate classification label (such as SF 710, *Unclassified* (label) or SF 707, *Secret* (label)) and DD Form 2056, *Do Not Discuss Classified Information* (label).

6.2.5. Collaborative Computer Systems. AFMAN 17-1301, para. 4.13. This term refers to any information system that allows a group to share voice, text or video in order to conduct meetings or exchange information. The use of cameras or microphones in areas where classified information is processed (electronically or hardcopy) is not authorized unless the following considerations are addressed.

6.2.5.1. The computer used is a SIPRNet computer and all personnel in the vicinity of the session are cleared at the appropriate level and have a valid need-to-know.

6.2.5.2. Use of collaborative systems on NIPRNet computers is authorized for text transmission in classified areas, provided the sender does not transmit classified information over the uncleared computer and the following considerations are addressed.

6.2.5.2.1. Peripherals must be Government Furnished Equipment (GFE) and approved through Cyberspace Infrastructure Planning System (CIPS). Peripherals must be external devices. Embedded collaboration equipment must be physically disabled and/or removed. Peripherals are not allowed to be cross shared between networks or classification levels. Peripherals must be wired; no wireless peripherals are allowed.

6.2.5.2.2. Headsets and/or microphones must be GFE and acquired through CIPS. Must be wired. Must be an external device and not embedded in the computer. Must have Push to Talk (PTT) or Positive Disconnection Device (PDD) capabilities. PTT and PDD capabilities must operate through physical means and not software. Must not contain any noise-cancelling functionality.

6.2.5.2.3. Webcams must be GFE and acquired through CIPS. Must be wired. Must be an external device and not embedded in the computer. Must have PDD capabilities. Must only be used in private offices or conference rooms and not face any open doors and/or windows.

6.2.5.3. In areas where classified and unclassified systems are collocated, but where the classified systems are not used on a daily basis, collaborative computer equipment may be authorized, but only if the user provides specific written procedures to the WCO and 5 BW/IPO outlining procedures used to ensure the equipment is not used during classified operations. These procedures would need to include some type of checklist detailing verification that all camera/microphones have been disconnected and secured prior to start of classified operations.

6.2.6. Unclassified Laptops in CPAs. The Cyber Security Liaison (CSL) will ensure the following procedures are met for these devices:

6.2.6.1. Must have a waiver from the WCO.

6.2.6.2. Must be configured IAW local policy and comply with all STIG requirements.

6.2.6.3. If not on the telecommunications and electrical machinery protected from emanations security (TEMPEST) accreditation or specifically waivered, it must be removed prior to the area going to an active CPA.

6.2.6.3.1. Waivered laptops must be clearly identified with a label from an authorized 5 CS agency indicating it is approved for use in the CPA.

6.2.6.3.2. If the laptop is approved, modifications to disable/remove wireless, Bluetooth, cameras, and microphones must be performed to the device.

6.2.6.3.3. Contact the WCO for more information or questions on requirements.

6.2.7. Control of Classified Copiers, Scanners or Printers. If not located in an approved open storage area, these device must be under positive observation/control of a cleared/authorized individual until properly purged.

6.2.7.1. Commanders will establish written procedures for purging of the devices, which may be included on the approval memo or in the unit's SECENT OI. As a minimum the procedures must include:

6.2.7.1.1. Adding the device to the SF 701, *End-of-Day Security Check Sheet*, for the area.

6.2.7.1.2. Keeping a copy of the purging process on or near the device.

6.2.7.1.3. The number of blank pages to clear latent images.

6.2.7.1.4. The need to power the device off to clear its memory anytime it is not in use.

6.2.7.1.5. A check for physical copies after each use and during the end-of-day check with the SF 701.

6.3. Marking AIS Equipment/Media. The minimum markings required for AIS equipment and media used for classified are outlined in DoDM 5200.01, Volume 2 and will be applied as explained in **chapter 8** below. Use rules from DoDI 5200.48_DAFI 16-1403 for CUI.

6.4. Cellphones and Electronic Devices in Classified Processing Areas (CPAs). Unauthorized devices pose a particular threat to sensitive information due their small size and the inherent risk they present to national security information. Any unauthorized government or personal electronic device found in a CPA is subject to the posted installation search and seizure guidelines and failure to surrender the device may result in apprehension by Security Forces and confiscation of the device. Disposition of the device is discussed under classified security incident for CPAs below.

6.4.1. A CPA is defined as an area which contains computer or electronic devices that process classified information, where classified hardcopy material is worked on or where classified conversations routinely occur. Some examples from AFMAN 16-1404 include the use of secure communication devices (e.g., Viper), a work center where classified hardcopy is reviewed, conference rooms where classified meetings are held, SIPRNet computers, aircraft where classified systems or equipment are in use, etc.

6.4.1.1. Failure to comply with CPA requirements WILL result in security incident if an unauthorized device is found in the CPA, unless the items are specifically authorized on the TEMPEST certification package.

6.4.1.2. If the area is a temporary CPA, this only applies if classified material is present, a conversation is in progress or classified equipment with an approved TEMPEST package is active.

6.4.2. Electronic Items in CPAs. Unless specifically authorized on the TEMPEST survey, it is prohibited to introduce any electronic devices which operate on radio frequency (RF) and infrared (IR) bands or which have photographic or audio recording capabilities (e.g., cell phones, wireless keyboard/mouse, etc.) into CPAs.

6.4.2.1. Personal electronic or data devices are never authorized in TEMPEST CPAs.

6.4.2.2. Ensure personnel are reminded prior to CPA entry or CPA activation to check for cellphones, as they are a specific threat and commonly used by all personnel.

6.4.2.3. Hand-held radio transceivers, used with intra-base radios and land-mobile radios, deserve special consideration because of their unique operational applications. A person may carry these devices into a TEMPEST CPA only if they are on the approved CPA's TEMPEST package.

6.4.2.4. Government issued Electronic Flight Bag (EFB) program devices (i.e., iPads) must be removed from TEMPEST CPAS unless they are specifically approved on the area's TEMPEST package. In unit specific open storage areas, they may “transit” a hallway in the “off” position. They are also authorized for transit through flight line areas and for use on aircraft so long as configured IAW the Authority to Operate.

6.4.3. Temporary CPAs. A temporary CPA is a permanent TEMPEST area where a SIPRNet workstation or a secure telephone is used only infrequently. These areas require:

6.4.3.1. The authorized user to properly purge and secure the area of unauthorized devices before classified information is processed/discussed (e.g., SIPR tactical local area network encryptor (TACLANE) keyed with Crypto Ignition Key (CIK)).

6.4.4. Classified Security Incidents Involving Electronics. When a classified security incident involves an unauthorized device, the item will be confiscated and treated as classified (same level as classified involved) until the classified security incident inquiry is complete or until verified it does not contain classified information. Individuals observing the incident will attempt to secure the device from the offender after they report the incident. Additionally:

6.4.4.1. If the USM verifies the device did not come within 3 meters of classified systems, no incident will be declared. If this cannot be established, or if the device was within 3 meters, an incident is declared.

6.4.4.2. If personal electronic devices are involved in a CPA incident, the inquiry official must determine, with advice from JA, IP, WCO and organizational subject matter expert (SMEs), whether a classified data spillage to the personal device occurred or if the device represented only a transitory threat.

6.4.4.2.1. The USM/CSL will assist the inquiry official (IO) in identifying a SME knowledgeable and able to assess if classified information for the area affected is on the device.

6.4.4.3. For data spills consider the following.

6.4.4.3.1. Secret level spills and below, there may be a technology capability to overwrite or sanitize, depending on the device in question. Contact WCO to determine if possible.

6.4.4.3.2. TS spills have no approved overwriting or sanitization procedure.

6.4.4.3.3. If a device cannot be sanitized, destroy it IAW DoDM 5200.01 Volume 3, enclosure 7, section 5.g.(3).

6.4.4.4. If an individual refuses to allow the device (government or personal) to be reviewed, contact law enforcement and have them apprehended for failure to obey. In this case, the device will be confiscated by SFs and treated as evidence until the matter is resolved by the inquiry official, SF Investigations or OSI.

6.4.4.4.1. Store affected devices surrendered or confiscated as a classified items until verified as clear of classified.

6.4.4.4.2. If devices are sent to National Security Agency (NSA) for destruction, follow procedures for mailing classified items.

6.4.4.5. If the device is a government issued item (e.g., cell-phone/two-way radio) and the breach of the zone was momentary while being performed in the course of duties, (e.g., SF responding to unauthorized aircraft run) it is not considered a security incident and does not need to be reported.

6.4.5. Establishing Unit Procedures. Units with CPAs will document written procedures in the unit's SECENT OI to ensure personnel are aware of requirements, to include:

6.4.5.1. Clearly identifying CPAs and prohibited devices is critical; here are a few examples of prohibited devices: cellphones (with or without cameras/microphones), flash memory devices, wireless PEDs, MP3 players with record, transmit/flash drive capabilities, etc.

6.4.5.1.1. Authorization for an item in one CPA **DOES NOT** automatically allow it into another CPA. For example, the Electronic Flight Bag iPads are authorized in some 5 OG CPAs, but not authorized in temporary SIPRNet work stations CPAs.

6.4.5.2. Posting visual aids of prohibited devices at CPA entrances. Visual aids for temporary CPAs need only be posted when classified processing is in progress.

6.4.5.3. Clearly identifying devices authorized for use in a CPAs. The procedures must ensure that owning area personnel and security forces (if applicable) are provided a copy of approval letters and a description of the device. Some devices which might be approved for CPA use are EFB iPads, Bluetooth medical devices, etc. In TEMPEST CPAs, these types of devices are ONLY authorized if approved on the TEMPEST package.

6.4.5.3.1. In the case of Bluetooth medical devices, they are not a risk in CPA where it is only a briefing or review of hardcopy material, so long as the member leaves any linked device (e.g., cellphone or other transmitting device) outside the CPA. In a TEMPEST CPA, these devices will need a TEMPEST review, certified tempest technical authority (CTTA) recommendation, and authorization official (AO) approval before being authorized.

6.4.5.4. If devices are authorized for use in Minot AFB common restricted/controlled areas the unit will coordinate with 5 SFS/S5 so it can be included in the Integrated Defense Plan.

6.4.6. Training Requirements. Commanders will ensure USMs work with unit leadership to identify positions in the unit where personnel work in or are authorized access to CPAs. Training is required even if the member only transits through the area, but does not use the equipment (e.g., flight line, Network Control Center (NCC), etc.). The training will include items from **Attachment 6** to include:

6.4.6.1. Being developed by the USM, unit training manager and/or section leadership of CPAs to tailor training for the CPA owners.

6.4.6.2. Inclusion in the unit's SECENT initial and annual refresher training.

6.4.6.3. Procedures outlined for classified access, as outlined in this chapter and **chapter 11**.

6.4.6.4. This training may be included into on the job training (OJT)-type training, provided the USM can verify completion, track currency (e.g., has a database) and it has been reviewed/approved by the 5 BW/IPO.

6.4.6.5. The requirement for completion of training before member signs the DD Form 2875, *System Authorization Access Request* for SIPRNet access.

6.4.6.5.1. The USM is responsible to validate all training IAW **chapter 11**. This includes the WCO-provided SIPRNet training (see **Attachment 6**) and requirements of this paragraph and those noted in **paragraph 6.5** below.

6.4.6.6. The SIPRNet users to acknowledge understanding of responsibilities and security requirements when they sign the WCO SIPRNet training letter.

6.4.6.7. The fact, a TACLANE and a CIK in the same location makes them classified.

6.4.6.8. The fact users must maintain positive control (i.e., personal observation AND physical control) of the TACLANE and CIK

6.4.6.9. That failure to maintain positive control (personal observation AND control) will result in a security incident.

6.5. Documenting System Access. Use the DD Form 2875 to document system access requests. These forms are processed to grant users specific permission levels on a specified IT system Specifically:

6.5.1. Processing NIPRNet DD Form 2875s. The unit CSL will maintain these forms. Follow the form's instructions and the following steps.

6.5.2. USM Actions. The USM will:

6.5.2.1. Verify investigation meets the minimum of a TIER-1 or higher investigation.

6.5.2.2. Ensure the "IT Level Designation" block is set to "III," unless otherwise specified in the justification block (i.e., block 13). If there is a question on what level is required, the CSL will contact WCO for clarification. The USM does not make this determination.

6.5.3. Cyber Security Liaison Actions. The CSL will ensure the DD Form 2875 and the WCO training form is properly filed until the member leaves the unit.

6.5.3.1. The "IT Level Designation" box (item 28c) will be checked at level III unless another level of access is required. If elevated permissions are required the CSL generating the form must provide specific rationale in Part II, item 13 (Justification for Access) on why the elevated permission is required. Contact the WCO for an explanation of the permission levels.

6.5.4. Contractor Access. If an uncleared contractor is issued a temporary CAC and requires access to NIPRNet, use procedures at **paragraph 14.3.4** to document the DD Form 2875.

6.5.5. Maintaining SIPRNet DD Form 2875s. The unit CSLs and 5 CS/Communication Focal Point (CFP) (SIPRNet Account Manager) will maintain copies of these forms. The Unit CSL will sign block 21 of the DD Form 2875. The 5 CS/CFP will sign block 22 approving access before returning to the squadron CSL.

6.5.5.1. If SIPRNet access is being granted, the USM will annotate block 27 with following statement, "The USM signature below verifies initial cleared, derivative, marking, and WCO SIPRNet training were accomplished and the member was added to the unit's derivative classifier letter."

6.5.5.2. If the USM fails to validate SIPRNet training, or improperly validates an investigation for a member, it may result in a security incident and/or negative derogatory actions on the USM.

6.5.6. Maintaining other DD Form 2875s. Must be maintained on file for one year after termination of user's account.

6.6. Negligent Discharge of Classified Information (NDCI) Handling Procedures. An NDCI occurs when classified data enters an information system for which it is not accredited to process.

6.6.1. Classified Message Incident (CMI). An NDCI may be a CMI when classified information is introduced into an email system approved for a lower classification of information, or a data spillage, when information of a higher classification is stored in the file system approved for a lower classification.

6.6.1.1. The specific details of any NDCI are classified until the affected systems are cleared which requires secure communications be used for all notifications.

6.6.1.2. All computers suspected of being involved in a NDCI will be treated as classified as soon as the incident is declared.

6.6.1.3. Computers will not be sanitized until the declaration authority makes an official declaration.

6.6.1.4. The Minot AFB Communications Focal Point (CFP) is the lead 5 CS agency for NDCIs. The CFP will notify the 5 BW/IPO when they are made aware of an NDCI. If it is weekend, holiday or after hours, notify 5 BW/IPO no later than (NLT) the next duty day.

6.6.2. Declaration Authority. The 5 BW/CC is the declaration authority at Minot AFB. The WCO, in concert with the 5 BW/IPO, and a subject matter expert for unit owning the information, will provide the declaration authority with recommendations, as needed.

6.6.3. Procedures. Due to the dynamic environment associated with cyber-risks, the AF NDCI process is very fluid and requires the CFP to assess each situation, as it occurs, against the current 624th Operations Center tasking orders (TASKORDs) to determine local responses. As a minimum, ensure the following actions are accomplished when a potential NDCI is reported:

6.6.3.1. Personnel will immediately notify the USM or CSL of any potential NDCI.

6.6.3.2. The USM or CSL will immediately notify their commander and then notify their counterpart (CSL or USM) and the CFP (at 723-1241, a secure line).

6.6.3.3. The USM will notify 5 BW/IPO NLT the next duty day.

6.6.3.4. The 5 BW/IPO will verify that the CFP is aware of any NDCI reported to them by USMs or other personnel.

6.6.3.5. When an NDCI is received from another base, the Air Force Mission Assurance Center (AMAC) directs all sanitization actions and is responsible to notify any other bases affected.

6.7. Non-Traditional Work Environments. Use of any secure device in an environment typically considered not the normal work environment (i.e., office, secure area, etc.) constitutes use in a non-traditional work environment and requires consideration of requirements outlined in DoDM 5200.01, Volume 3, Enclosure 7, Section 7. The situations include; use of documents or a non-mobile secure device at a home location (e.g., VIPER phone, SIPRNet or classified documents used in a commander's home), use of a secure portable electronic device (PED) at a home or undesignated location (e.g., ADSV tablet or DMCC-S phone), or establishment of a field expedient temporary TEMPEST area. In all of these cases, a risk assessment by 5 BW/IP and 5 CS Cybersecurity is required. In the case of home or PED use, AFGSC/IP must approve the use after the risk assessment is completed. In the case of a field expedient temporary TEMPEST area, the WCO will approve the area.

6.7.1. Use of Non-mobile Classified Devices/Material in a Residential Environment. A site survey meeting all requirements will be accomplished, IAW DoDM 5200.01, Volume 3, Enclosure 7, before requesting MAJCOM/IP approval for residential use as discussed in DoDM 5200.01, Volume 3, Enclosure 12, Section 2.b.(1). Contact 5 BW/IP to coordinate the needed site survey.

6.7.1.1. Installed devices require a TEMPEST survey and will not be moved without prior coordination through 5 BW/IP and Cybersecurity.

6.7.2. Use of Secure Portable Electronic Devices (PEDs). Consider the following:

6.7.2.1. Regardless of whether the PED will be used in a residential or undesignated setting, a site survey will be accomplished and AFGSC/IP approval is required.

6.7.2.2. The ADSV, DMCC-S or similar PEDs are intended for emergency or contingency situations where other secure devices (e.g., VIPER or SIPRNet) are not available.

6.7.2.3. If the secure PED will be used in a residential setting, a site survey will be conducted and a designated CPA established. The secure PED may only be used at the residence in the designated CPA.

6.7.2.4. If the secure PED is intended for undesignated location use, a site survey of the device will be conducted to establish needed countermeasures.

6.7.3. Establishment of Temporary TEMPEST Sites. If a temporary TEMPEST CPA is required for local exercises or actual deployments, contact WCO to determine actions to be taken.

6.7.3.1. Contingency TEMPEST CPAs are used only in tactical or deployed environments and will comply with AFSSI 7702, Attachment 2.

6.7.3.2. Users will comply with the contingency TEMPEST rules, where possible, even during actual contingency environment. Uses will notify WCO for instances not met.

6.7.3.3. Physical security rules for protection of classified still apply during contingency operations.

6.7.4. Installation Portable Electronic Device (PED) Manager. Per AFI 16-1404_AFGSCSUP, paragraph 5.2.6.1., the 5 BW/CC appoints the 5 CS/CC as the installation PED manager. This delegation may be further delegated.

6.7.5. User Responsibilities. It is the user’s responsibility to ensure any classified equipment is approved for use in the area it is located. If it is unclear whether the device has been approved, DO NOT USE THE DEVICE. Contact the WCO for clarification. Use of unapproved secure equipment will result in a classified security incident.

6.7.6. Storage Requirements. Storage requirements vary with device types. Follow all requirements as outlined in the site survey.

6.7.7. The crypto ignition key (CIK) for a SIPRNet terminal, along with the TACLAN or an access code for a PEDs are considered classified when in proximity of the device. If they are written down and/or left unattended within physical proximity of a secure PED a security incident will be declared.

6.7.7.1. Follow rules outlined in the site survey for storage of CIKs.

6.7.8. Reporting Loss of Device/Compromise. Take the following actions in regards to suspected loss or compromise.

6.7.8.1. If a secure PED is lost, stolen or tampered with, immediately notify the servicing WCO and USM.

6.7.8.2. If the access code or CIK are lost, immediately notify the servicing WCO.

6.7.8.3. If a keyed device (VIPER, PED or SIPRNet) are discovered unattended while keyed, immediately report the incident to the USM.

6.8. Cyber Security Event. A cyber security event is any violation TASKORDS in regard to network policy on NIPRNet or SIPRNet. The CFP is responsible to enforce the current 624th Operations Center TASKORDs and will make any necessary up/down channel reports and accomplish remediation, if necessary. These types of events may include items such as external media violations, unapproved software, cross domain (NIPR/SIPR) violations, improper use of network access.

6.8.1. For all Data Loss Prevention (DLP) violations or incidents which do not involve classified but may involve is not limited to, plugging in unapproved external hard drives, thumb drives, mobile devices, dongles, or adapters, etc. The WCO will work with the unit CSL and USM to decide upon further action. At a minimum, the violating individual will be required to re-accomplish their cybersecurity awareness training before access is renewed to the network. Repeat offenses may result in a CE Incident report and/or loss classified eligibility based on adjudicative guidelines

6.9. Network Access Suspension. This applies when a member’s access is suspended locally or by OPM. Take the following actions if this occurs:

6.9.1. Classified Systems. If the member's eligibility for access to classified is suspended, denied, or revoked the individual’s USM and CSL will ensure the commander and CFP are informed and classified system access is immediately suspended.

6.9.1.1. Access to classified systems will not be restored until the member’s eligibility for access to classified is restored.

6.9.2. Unclassified Systems. When access to classified is suspended or revoked, the USM and CSL will coordinate with their commander to determine if access to NIPRNet will be maintained.

6.9.2.1. If the commander determines NIPRNet access is suspended, the CSL removes access.

6.9.2.2. If commander wishes to reinstate NIPRNet access before classified access is reinstated, they must request NIPRNet reinstatement from the Information System Owner. Contact WCO for more information.

6.10. Controlled Access Area (CAA) Procedures. The following procedures will be used to establish and maintain CAAs.

6.10.1. Defining CAAs. According to AFSSI 7002, a CAA is "The complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance." Use of CAAs applies only to classified computer systems, as outlined in AFSSI 7002 and 7003, and the areas will not be used for other classified assets.

6.10.2. Responsibilities. The following agencies are responsible for actions noted.

6.10.2.1. Commanders will make requests for CAAs through their CSLs to WCO or through their USMs to 5 BW/IP.

6.10.2.2. The 5 BW/IP office will coordinate a Security Enterprise survey for the request and ensure 5 CES, WCO and 5 BW/IP are present at the survey. Additionally, they will ensure:

6.10.2.2.1. The report will be signed by representatives of 5 BW/IP, WCO and 5 CES. It will outline any needed corrective actions for physical security, access controls, reference need for a formal TEMPEST approval and cover general use of the facility.

6.10.2.2.2. The report clearly indicates whether or not lines carrying SIPR signals above a false ceiling/floor need to be in sealed conduit, alarmed and frequency of checks for the lines.

6.10.2.2.3. The 5 BW/IP office will work with the 5 CES Security representative to ensure the standards from AFMAN 16-1404 to DoDM 5200.01, Volume 3 and MILHNDBK 1013/A1 are met.

6.10.2.3. The WCO will ensure any needed TEMPEST requirements are met with a formal TEMPEST survey and validate access control outlined in the survey report meet AFSSSI 7002 and 7003 requirements.

6.10.2.4. The CSL/USM will ensure:

6.10.2.4.1. A copy of the facility survey report is maintained at the facility, in the USM binder.

6.10.2.4.2. The CSL is responsible to ensure any needed checks of wiring are conducted and documented. It is acceptable for the checks to conducted/documented during the semiannual MICT and annual Security Enterprise inspection/CCIP events.

6.10.3. Physical Control. Control of a CAA is established, IAW AFSSI 7002, 4.2.5., through strict enforcement of access controls and physical security measures. This means codes to cipher locks or keys to the facility are strictly controlled and issued only to personnel who are cleared for access.

6.10.3.1. The Security Enterprise risk assessment survey report will identify physical security standards which apply from AFSSI 7003, Chapter 11..

6.10.3.2. The agency owning the CAA will establish formal written entry/access control procedures for the area ensure these:

6.10.3.2.1. Are signed by the owing commander, 6.10.3.2.2. maintained at the facility, in the USM binder and provided to the 5 BW/IP office. It is acceptable to incorporate these procedures into the unit Security Enterprise instruction.

6.10.3.2.3. Ensure all items in this chapter are localized and clearly outlined in the written procedures.

6.10.3.2.4. If the unit intends to allow use of the CAA facility by uncleared personnel, ensure the written procedures outline how the agency controlling keys will purge the room after use by the uncleared personnel. As a minimum the purge will include inspecting all above ceiling/below floor lines used to transmit SIPR signals.

6.11. Portable Wearable Fitness Devices (PWFD) and Electronic Medical Devices (EMD). In Classified Processing Areas (CPAs), Sensitive Compartmental Information Facilities (SCIF) and/or Special Access Program Facilities (SAPF). All PWFD and EMD must be approved by the appropriate AFGSC functional.

6.11.1. Members requesting/needing approval for a PWFD or EMD will contact their USM to obtain either the DAF Form 110, *DAF EMD Request Form & Approval Card*, or DAF Form 111, *DAF PWFD Request Form & Approval Card*.

6.11.2. The requesting member will complete the form and submit the form to their USM who will process/submit the form IAW AFGSC procedures for EMD and PWFD requests.

6.11.3. Requester must maintain a copy of approved request on their person when in approved areas and should reapply for approval 30-days before their current approval expires.

6.11.4. An unapproved PWFD EMD entering a CPA, SCIF, or SAPF may result an administrative action, confiscation of device and/or a classified security incident.

Chapter 7

SPECIAL INFORMATION PROGRAMS (SIPS)

7.1. General Guidelines. The general guidelines for SIPs at Minot AFB are detailed in this chapter and consist of programs requiring special measures (physical security, access control or additional investigative requirements). Additional specific actions may be directed by the basic references for SAP management found in DoD Directive 5205.7, DoDM 5200.01, Volumes 1, 2, 3 and Joint Air Force – Army – Navy (JAFAN) manuals, as well as program-specific guides, manuals and applicable DoD instructions. If a conflict between the guidance for collateral classified information (standard Confidential, Secret and TS) occurs, the guidelines for the SIP will take precedence, unless the collateral requirements are more restrictive.

7.1.1. Defining SIPs. The Glossary at Volume 1 of DoDM 5200.01, defines a SAP as, "A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." Using the DoDM definition, the following programs all have additional safeguarding, access controls or investigative requirements, which meet the definition of a SAP: COMSEC, NATO, RD and CNWDI and NC2. In an effort to reduce confusion between these federal/DoD-created SAPs and more traditional SAPs, we have termed these programs SIPs, but still comply with all DoD requirements. For the purposes of the remainder of this chapter, the terms SIP and SAP are interchangeable.

7.1.2. General Information. Classified information designated as SIP will be handled, transmitted, marked, protected using at least the minimum standards for collateral information. If SIP requirements are more stringent, the SIP standards will be applied.

7.1.3. Units With SIP Material. Unit commanders holding SIP material (e.g., NC2, RD, CNWDI, etc.) will ensure a Minot AFB focal point is appointed. If it is unclear which agency should be the Minot AFB focal point, (e.g., more than one agency has the material, and there is no HHQ guidance), the ISAG will discuss the issue and forward a recommendation to the 5 BW and/or 91 MW commander (as applicable) on which agency should be the primary focal point.

7.2. Inspection Requirements. Most SIPs have their own inspection requirements/processes and 5 BW/IPO is absolved of annual review, assessment responsibilities and technical assistance unless stipulated otherwise in this instruction. The local Program Security Manager (PSM) may request IPO assistance, in writing, if the technical support does not require access to SIP information. Access will not be granted solely for the purpose of technical support.

7.2.1. General Information. The PSM for the SIP will provide the 5 BW/IPO an appointment letter and ensure SAP classified information or material, as a minimum, meets basic classification, declassification and marking requirements outlined in EO 13526 and DoDM 5200.01, Volume 2. Enclosure 3.

7.2.2. SIP Access/Physical Security Controls. Additional access physical security controls above those used for collateral may be justified only when exceptional security measures are required. The level of additional control is based on threat/vulnerability (e.g., sensitivity and/or value of the information. Specific safeguarding, access controls/investigative requirements may be required for specific SIPs. [REF: DoDM 5200.01, Volume 1, Enclosure 3.]

7.2.3. Congressional Reporting. The programs below are not reported to Congress, as they protect purely military operations and do not involve acquisition or intelligence funds. If additional reporting is required, it will be accomplished by the PSM IAW SIP rules.

7.2.4. Annual Inspections. Each SIP has a designated PSM at either the MAJCOM or Installation level who determines if/when annual inspections are required. If there are concerns or questions on a SIP, contact the Minot AFB PSM for assistance or clarification.

7.2.5. MAJCOM Focal Points. Each SIP has an AF and MAJCOM level PSM to provide oversight, coordinate requests and review potential program issues. The installation PSM coordinates with these POCs on SIP for program questions.

7.3. The Personnel Reliability Assurance Program (PRAP). This program is governed under DoDM 5210.42 and AFMAN 13-501 and no specific local program guidance has been established. The 5 BW/CC appoints the 5 BW/PRAP office to act as the Minot AFB focal point.

7.4. The Restricted/Formerly Restricted Data (RD/FRD) Program. Access and dissemination of RD and FRD information is governed under the Department of Energy (DoE) IAW the Atomic Energy Act of 1954, DoD Instruction 5210.02, and AFI 16-1404.

7.4.1. Program Management. Each wing commander will designate a RD Management Official (program manager) to disseminate directives, classification guides, (as needed), and ensure personnel with access are trained IAW AFMAN 16-1404, Volume 1 . The 5 BW/CC designates the 705 MUNS/CC as the 5 BW focal point for CNWDI and the 91 MW/CC designates 91 OSS/CC as the 91 MW focal point. This responsibility may be further delegated, in writing, to another SME for the unit. Provide a copy of the delegation letter to 5 BW/IP.

7.4.1.1. Ensure RD/FRD is stored, marked, protected and destroyed IAW DoDI 5210.02, in the same manner as collateral material of equivalent level. A copy of the each unit's RD certification procedures will be forwarded to the 5 BW/IPO to be included in the unit folder.

7.4.1.2. There are no special access requirements for FRD and the holder must ensure anyone accessing the material has a clearance equal to the equivalent collateral level.

7.4.2. RD Indoctrination. RD access requests are recorded on AF Form 2583, *Request for Personnel Security Action*. Keep the AF Form 2583 in unit files for duration of the individual's access to RD and dispose of IAW RDS.

7.4.3. Accessing RD. Access/dissemination of RD is controlled IAW DoDI 5210.02 and AFMAN 16-1404 to DoDM 5200.01, Volume 1, Enclosure 3, paragraph 13.a.(1). Due to the sensitivity of RD a strict adherence to the "need-to- know" principles will be followed. Each unit holding or with members requiring routine access to RD must establish specific unit procedures.

7.4.4. Electronic Transmission of RD/FRD. There are special requirements for transmitting this material. The electronic transmission of Secret level FRD/RD material is authorized over SIPRNET, only if the sender verifies the receiver has a valid need-to-know the information. The use of distribution groups is not authorized when sending over SIPRNET.

7.4.5. Debriefing from RD. Procedures for ensuring access is terminated when no longer needed for official duties. Record debriefing of RD access using AF Form 2587, *Security Termination Statement*. Maintain the AF Form 2587 IAW RDS.

7.4.6. Unauthorized Access to RD. If there is reasonable doubt on whether a member is properly indoctrinated for RD access, a security incident will be declared.

7.5. Critical Nuclear Weapons Design Information (CNWDI) Program. This program is governed by DoD Directive 5210.2 and AFMAN 16-1404 to DoDM 5200.01, Volume 1, Enclosure 3, and is tied directly to the RD program.

7.5.1. Program Management. The Wing RD program manager will act as the CNWDI program manager. Members may not be indoctrinated to CNWDI without first being indoctrinated into RD. Each commander/staff agency chief having members requiring CNWDI access will establish specific written procedures to ensure only members who have a valid and official need are indoctrinated to RD and CNWDI.

7.5.2. CNWDI Indoctrination. CNWDI access requests are recorded on AF Form 2583. Keep the AF Form 2583 in unit files for duration of the individual’s access to CNWDI and dispose of IAW RDS.

7.5.3. Debriefing from CNWDI. Record debriefing of CNWDI access using AF Form 2587, Security Termination Statement. Maintain the AF Form 2587 IAW RDS.

7.5.4. Transmission of CNWDI. Ensure CNWDI is transmitted IAW current program requirements. Contact the appointed Wing RD PSM for questions on transmitting CNWDI.

7.5.5. Unauthorized Access to CNWDI. If there is reasonable doubt on whether a member is properly indoctrinated for RD/CNWDI access, a security incident will be declared.

7.5.6. Temporary RD or CNWDI Access. If temporary access is required for a TDY, conference or other official reason, the RECEIVING location should accomplish indoctrination and debriefing. If the receiving location cannot accomplish the indoctrination or fails to accomplish the debriefing, the USM will use the following procedures:

7.5.6.1. Process an access request letter through the appropriate certification authority which clearly states the reason the access is required and the duration. The letter will be maintained until the member returns from trip. This method may also be used when all members of unit are in a career-field where access may be needed, but an official need does not exist on a daily basis.

7.5.6.2. Upon return from the TDY location (or completion of the local task) the owning USM will debrief the member using the AF Form 2587 and remove the RD and/or CNWDI access in DISS or successor system NBIS. Maintain paperwork IAW RDS.

7.5.6.3. In-bound TDY personnel coming to Minot AFB who need RD/CNWDI access should be announced on a system visit request and indoctrinated prior to arrival. If access is granted at Minot AFB the sponsoring wing RD program manager accomplishes all actions including the temporary access letter training, administrative paperwork (i.e., AF Forms 2583 and 2587), indoctrination and debriefing. All paperwork for the individual is maintained IAW RDS.

7.6. North Atlantic Treaty Organization (NATO) Program. Security requirements for NATO material is governed by United States Security Authority (USSAN) Instruction I-07 and AFMAN 16-1404 to DoDM 5200.01, Volume 1, Enclosure 3. In addition, NATO material will be marked and controlled IAW DoDM 5200.01, Volume 2. Care must be taken to protect foreign government information at the equivalent of its US level, except as specified in DoDM 5200.01, Volume 3, Appendix to Enclosure 4, or as required by treaties or international agreements. All Minot AFB NATO is COMSEC related material and reviewed under that program's rules. The following procedures also apply for COMSEC-related NATO at Minot AFB.

7.6.1. NATO Sub-Registry and Processing. There is no NATO sub-registry associated with NATO at Minot AFB as it is COMSEC material and controlled IAW that program's access rules. If non-COMSEC NATO material is received at Minot AFB, a NATO sub-registry must be established and a specific NATO program coordinator designated.

7.7. Communications Security (COMSEC) Program. The focal point for this program is 5 CS/SCXSC, COMSEC Account 634039. It is governed by AFMAN 17-1302-O, *Communications Security (COMSEC) User Requirements*. Security classification and declassification policies in DoDM 5200.01 apply to COMSEC information in the same manner as other classified information. DoDM 5200.01, Volume 1, Enclosures 3 and 5 prescribes special procedures for cryptologic information.

7.8. Sensitive Compartmented Information (SCI) Program. This program is managed by the Minot AFB SSO and governed by applicable Director of Central Intelligence Directives (DCID), Intelligence Community Directives (ICD) and DoD 5105.21-Vol 1-3. Security classification and declassification policies in DoDM 5200.01 apply to SCI in the same manner as other classified information. There are special access and physical security controls required for SCI.

7.8.1. Pre-access requirements for SCI. The following actions will be accomplished prior to individuals being granted access to SCI.

7.8.1.1. Squadron CC will complete, sign and return the SCI Access Request form using the template provided by the Minot AFB SSO to the applicable SSR. This is not required if the Minot AFB SSO or an SSR knows of a compelling need.

7.8.1.2. An AF Form 2583, properly routed thru 5 SFS/S5R, must be completed using the Minot AFB SSO template. This form must be completed prior to accomplishing the compelling need memorandum, if it is required.

7.8.1.3. No action to grant access will occur until all required forms are completed and received by the SSO.

7.8.1.4. All forms must be accomplished at least 30 days prior to requested access date.

7.9. Installation Nuclear Command And Control Extremely Sensitive Information (NC2-ESI) Program Management (INPM).

7.9.1. General Information. Because Minot AFB consists of two wings, the host wing (5 BW) provides an INPM to manage the NC2-ESI program IAW CJCSI 3132.01B and AFI 13-502. The Chief, Minot Command Post, is designated as the primary INPM and may delegate NC2-ESI Program Manager (NPM) responsibilities within the Command Post (CP). If delegated, the member must be at least an E-6/O-3 or above and have an appropriate clearance and access levels. The INPM provides oversight for the 5 BW and 91 MW Wing NPM (WNPMs). The

5 OG USM is the 5 BW WNPM and also acts as the assistant INPM. The 91 MW/CC will designate a Primary and Alternate WNPM, who will provide a copy of the appointment letter to the INPM. The 5 BW/IPO provides annual management oversight for the INPM program, normally during the unit's scheduled SECENT inspection.

7.9.2. The INPM Responsibilities. The INPM will:

7.9.2.1. Oversee the NPM program to include NC2-ESI management, safeguarding and access requirements IAW CJCSI 3132.01B and AFI 13-502.

7.9.2.2. Standardize access briefings and training materials for all personnel granted NC2-ESI access. The training plan/materials will include identifying applicable classification guides for the material and special access control requirements associated with the material. The training plan will be coordinated through 5 BW/IPI.

7.9.2.3. Coordinate a self-assessment of the INPM plan in addition to the annual program review conducted by 5 BW/IPO.

7.9.2.4. Conduct and document, in writing, an annual assessment of the installation NC2-ESI program routed to the 5 BW and 91 MW commanders with a courtesy copy to the CIP after wing commander reviews.

7.9.2.5. Act as Installation OPR for consolidating, coordinating and forwarding HHQ directed tasks related to NC2-ESI materials and program management.

7.9.2.6. Develop and distribute NC2-ESI program management checklists to unit NPMs.

7.9.2.7. Coordinate, as required, with 5 BW/IPO for technical assistance (e.g., NC2-ESI material classified security incidents, screening questionnaire “yes” answers not previously adjudicated prior to granting official review, etc.).

7.9.3. Commander Responsibilities. The 5 BW and 91 MW must appoint WNPMs in writing for units with administrative responsibilities for the program or with access to NC2-ESI Material. Responsibilities include:

7.9.3.1. Designating, in writing, a WNPM who will be responsible for completing any required training and administrative actions as detailed in WNPM responsibilities below.

7.9.3.2. Completing procedures IAW AFI 13-502 and AFMAN 16-1404 anytime a loss or compromise of NC2-ESI material is suspected/confirmed.

7.9.4. 5 BW and 91 MW WNPMs Responsibilities. The WNPMs will:

7.9.4.1. Oversee their respective NC2-ESI programs, as directed by the INPM.

7.9.4.2. Ensure required administrative actions are completed IAW checklist provided by the INPM for units under their administrative control.

7.9.4.3. Consolidate and forward the “granting officials” roster to the INPM NLT 10 January and 10 July each CY.

7.9.4.4. Consolidate and forward the NC2-ESI access list rosters to the INPM NLT the last duty day of each CY quarter.

7.9.4.5. Meet access requirements and be properly indoctrinated for access to NC2 materials.

7.9.4.6. Complete all actions required to allow assigned unit personnel access to NC2 material. This includes indoctrination, debriefing, self-assessments, etc.

7.9.4.7. The WNPMs will develop any specific local unit procedures needed for safeguarding materials. These procedures will be established in writing and should be included in the unit's SECENT OI.

7.9.5. USM Responsibilities. The USM does not require access or indoctrination to NC2-ESI material when indoctrinating personnel. For units with personnel indoctrinated to NC2 but which do not control NC2 material, the USM will:

7.9.5.1. Oversee completion of any required administrative actions (e.g., indoctrination, training, debriefing, questionnaire, etc.).

7.9.5.2. Consolidate and forward any required NC2 program management material to their respective WNPM, as required.

7.9.5.2.1. If there are any issues with answers to questions on the NC2 questionnaire the USM will contact 5 BW/IPP for assistance on determining actions required.

7.9.6. Control Procedures. All NC2-ESI material will be classified and marked as TS with the appropriate NC2-ESI indicator. Any NC2-ESI hard copy documents will be separated from other classified material by guide cards, file folders, or separate drawers of multi-drawer security containers.

7.9.6.1. Security classification and declassification policies of DoDM 5200.01 apply to NC2 material in the same manner as other classified information.

7.9.6.2. All specific investigative requirements must be met prior to individuals being granted access to NC2 material.

7.9.7. Investigation Requirements. Members must have a final TS prior to be indoctrinated to NC2-ESI access. Temporary-TS access may be granted ONLY if the AFGSC/CC or CV have provided the needed waiver of access requirements letter.

7.10. Presidential Support Activities (YANKEE WHITE). Although there are no positions assigned for this at Minot AFB, members may need to complete investigative requirements prior to being accepted for some assignments. The 5 BW/IPP is the focal point for investigative actions concerning this program at Minot AFB. It is governed by DoD Directive 5210.55 and has special investigative requirements.

7.11. Other Special Access Programs (SAP). Ensure any access to SAPs not covered in this section is granted only as specified by the SAP instructions. Additional guidance can be found in DoD Directive O-5205.7.

Chapter 8

CLASSIFYING, MARKING AND DECLASSIFYING INFORMATION

8.1. Original Classification. There are no authorized Original Classification Authority (OCAs) at Minot AFB. Any required OCA decisions must be submitted to the appropriate Numbered Air Force. USMs can provide more information on this topic, if required.

8.2. Derivative Classification. The following requirements must be considered when making derivative classification decisions.

8.2.1. Generating Derivatively Classified Documents. Derivative classifiers must be specifically trained and receive refresher annually IAW current DoD directives.

8.2.1.1. Specific training requirements are outlined in **chapter 11**, **paragraph 11.3**, of this instruction. Derivative classification is extremely important to ensure classified information is provided the proper level of protection.

8.2.1.2. Derivative classifiers are responsible to ensure the proper markings are applied to all portions of the document and must understand failure to properly mark a derivative document may constitute a security incident.

8.2.1.3. The unit commander will appoint derivative classifiers in writing and USMs will maintain a compiled listing of unit members identified and trained to act as derivative classifiers, with a copy provided to 5 BW/IPO.

8.2.1.4. The USM will verify members gaining access to SIPRNet have completed required training and annotate the DD Form 2875, block 27, with the statement, shown at **paragraph 6.5.2.2**.

8.3. Marking Classified Information. Derivative classifiers are required to verify documents they use comply with guidelines for marking found in the basic instructions.

8.3.1. Marking Requirements. Specific marking requirements can be found in AFMAN 16-1404 to DoDM 5200.01, Volume 2.

8.3.2. Marking Classified Emails. Information sent/received via approved secure communications systems must be properly marked. The receiver will notify the sender of improper marking issues on receipt. If the sender refuses to correct improper markings, it may be considered a security incident on the sender.

8.3.3. Printing Classified Emails. All printed email documents must be marked IAW DoDM 5200.01, Volume 2, regardless of whether markings show appropriately when printed. It is the holder's responsibility to ensure classified under their control is properly marked.

8.3.4. Special Control and Similar Notices. See DoDM 5200.01, Volume 2 for instructions on special notices for restricted data, formerly restricted data and other types of information.

8.3.5. Marking Special Types of Materials. When marking automated information systems, audiovisual media, hardware, products, etc., use the guidelines described in DoDM 5200.01, Volume 2.

8.3.6. Marking Foreign Government Information in DoD Documents. Use the guidelines described in DoDM 5200.01, Volume 2 to control and mark this information.

8.3.7. Marking Blank Pages in Multi-page Classified Documents. If a document contains blank pages, they must contain banner markings (i.e., top/bottom) using one of the marking conventions outlined in DoDM 5200.01, Volume 2.

8.4. Declassifying, Downgrading or Regrading Information. Use the guidelines in DoDM 5200.01, Volume 2 and AFMAN16-1404 declassify, downgrade or upgrade classified information.

8.5. Classification Challenges. The holder of an improperly marked classified or unclassified document shall contact the document's originator to obtain correct markings. If personnel feel a document needs a higher or lower classification or should be declassified, it is the individual's responsibility to challenge the classification using procedures in AFMAN 16-1404 and DoDM 5200.01, Volume 2.

8.5.1. Mismarked Information. If information is received without proper markings, always attempt to resolve the situation at the lowest level possible. First, contact the sender to verify the markings. If this does not work, ask your USM to contact the agency's USM. If this does not work, your USM should contact the 5 BW/IPO for additional assistance.

8.5.2. Handling/Storing Challenged Information. If there is doubt on the validity of classification authority or level for material, or it is not possible to verify what level information should be protected at, protect the information at the highest suspected level until clarification is received.

8.6. Marking CUI. Follow the guidelines in DoDI 5200.48_DAFI 16-1403, when handling, processing and marking controlled unclassified information when it is NOT included in a classified document. Some specific considerations include:

8.6.1. General CUI Marking Requirements. All CUI documents will have "CUI" on the top and bottom of each page the document and the first page will have the "Dissemination Information" discussed below. It is the responsibility of the originator/writer of the document/e-mail to determine whether the information qualifies for CUI status and to ensure markings are applied as required IAW DoDI 5200.48_DAF 16-1403. Additionally:

8.6.1.1. Do not apply CUI markings to documents or emails unless a specific rule from the CUI Registry is applicable, applied and included in the Dissemination Information block. Improper use of CUI markings may result in administrative or other sanctions.

8.6.1.2. If one paragraph is marked parenthetically, all paragraphs must be marked parenthetically. Use (U) for information which is not CUI in this case.

8.6.1.3. The Dissemination Information will consist of the following:

8.6.1.3.1. Line 1: Controlled By: Service branch of the controlling agency (e.g., USAF)

8.6.1.3.2. Line 2: Controlled By: Enter the office symbol of the agency controlling the information (for example, 5 BW/IP).

8.6.1.3.3. Line 3: CUI Category(ies): Obtain these by reviewing the CUI Registry and choosing those which apply—there may be more than one. For example, PII would be "PRVCY". The Registry is found at **https://www.archives.gov/cui/registry/category-list**

8.6.1.3.4. Line 4: Limited Dissemination Control: Until further notice, use "FEDCON".

8.6.1.3.5. Line 5: POC: Include name, phone and/or email address of the individual to contact if questions are raised on the assigned category.

8.6.1.4. All emails sent over NIPRNet to outside the AF Network to commercial addresses or other government agencies containing any category of CUI must be digitally signed and encrypted. Due to the underlying encryption native to the Outlook tool suite, there is no need to encrypt when sending messages to users on the AF Network.

8.6.2. Considerations for DoD UCNI. Use the normal CUI marking scheme (i.e., CUI top and bottom with Dissemination Information block) and identify any DoD UCNI parenthetically as (DCNI). This information must meet requirements in DoDD 5210.83 before being designated as DoD UCNI.

8.6.2.1. When emailing DCNI over the AF Network, encryption/digital signature are not required but the sender must verify the receiver has valid need. If emailed outside the AF Network to a commercial address or other government agencies the sender must also encrypt and digitally sign the email.

8.6.2.2. If the information will be released outside DoD channels include the expanded statement from DoDD 5210.83, in addition to the Dissemination Information block.

8.6.2.3. If there is CUI comingled with DoD UCNI, identify it in the parenthetical markings as (CUI).

8.6.3. Privacy Act Data. Additional requirements, over those in DoDI 5200.48_DAFI 16-1403, for this type of CUI are found in DODM 5400.11 and AFI 33-332, *Air Force Privacy and Civil Liberties Program*. This includes:

8.6.3.1. Do not apply CUI PRVCY markings to documents or emails unless a specific rule from the CUI Registry is applicable, applied and included in the Dissemination Information block. Improper use of CUI markings may result in administrative or other Privacy Act or notifications.

8.6.3.2. The writer must also identify which paragraphs contain the CUI information by placing (CUI) before the affected paragraph.

8.6.3.3. If the information will be released outside DoD channels include the expanded statement from DoDM 5400.11, in addition to the Dissemination Information block.

8.6.3.4. It is acceptable to use the expanded statement in an e-mail/hardcopy document, even if not going outside DoD channels provided the e-mail or document contains CUI information.

8.6.3.5. When emailing Privacy Act information over the AF Network, encryption/digital signature are not required but the sender must verify the receiver has on official need. If emailed outside the AF to a commercial address or other government agencies the sender must also encrypt/digitally sign the email.

8.6.3.6. Do not send Privacy Act information/PII to distribution lists or group e-mail addresses, unless each member is verified by the sender as having an official need for the information.

Chapter 9

TRANSMISSION/TRANSPORTATION OF SENSITIVE INFORMATION

9.1. General Policy. The DoD/AF general policy on transporting/transmitting classified or CUI is it should be sent electronically or through the US Postal Service unless there are no other options.

9.1.1. Guidance. Personnel will use the procedures outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 4, the AFGSC/CC GM and any other applicable AFGSC/IP GMs when transporting or transmitting classified material. When transmitting CUI use the rules outlined in DoDI 5200.48, Section 4.1.e.(2).

9.1.2. Procedures. Unit Commanders must establish local procedures for sending and receiving classified information.

9.1.2.1. Use the unit's SECENT OI to address specific actions to take when receiving first class, certified or registered mail. These types of packages may contain classified and must be protected (at a minimum) as Secret material until received by the designated office.

9.1.2.2. When transmitting/transporting specialized program information such as COMSEC, NATO, SAPs etc., collateral classified rules apply, in addition to any additional program requirements. If a conflict occurs, use the stricter of the two standards.

9.2. Training. Commanders establish procedures and training in their unit's SECENT OI to ensure personnel tasked to send and/or receive sensitive information (classified or CUI) are properly identified, aware and trained, as needed. As a minimum, ensure the OI identifies:

9.2.1. Specific jobs requiring additional training, for example; secretaries, administrative assistants, receptionists and other personnel who perform administrative duties where US mail is sent or received.

9.2.2. Procedures and training on actions to take when classified or CUI is received or sent. This will include procedures for receipt and protection of first class, registered or certified mail, which may contain classified or CUI information.

9.2.3. Training requirements for AFGSC on-base transport of classified is accomplished using a localized version of the AFGSC/IP Basic Courier Block Training and must be provided in-person. Training requirement for off-base couriers include the on-base requirements and the individual must also complete the CDSE on-line Transmission and Transportation for DoD Training found at **https://www.cdse.edu/Training/eLearning/IF107/**. All AFGSC Courier training (on and off-base) must be completed annually.

9.2.4. Commander's Courier Briefing. This briefing will be documented using a template briefing (**Attachment 11**), which may be pre-signed by the commander. The member signs this briefing to acknowledge understanding of the training and the USM signs to validate the training.

9.3. Standards. Each category of sensitive information (classified or CUI) has specific standards for transporting or transmitting. Consider the following when developing unit procedures for transmitting/transporting sensitive information:

9.3.1. Transporting/Transmitting of US Collateral Classified. Off-base transport of classified is only authorized as a last resort or when other transport methods (i.e. electronic transmission, use of approved carrier service) are not viable. If required, transport will be accomplished using methods outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 4, the AFGSC/CC GM and any applicable AFGSC/IP GMs.

9.3.2. Transporting/Transmitting of Classified to Foreign Governments. Use only the methods outlined in AFMAN16-1404 to DoDM 5200.01, Volume 3, Enclosure 6 when considering how to transport/transmit classified material to foreign governments.

9.3.3. Transporting/Transmitting of CUI. Ensure the appropriate standard from DoDI 5200.48, Section 4.1.e.(2) **paragraph 8.4** (inclusive) of this instruction are applied before sending any unclassified sensitive information.

9.3.4. Improper Electronic Transmission of Information. If information is sent inappropriately over a computer, fax, electronic data device, or other electronic means follow the procedures outlined in paragraph **1.7.2.6**, **1.10.3** and **6.4.4** of this instruction, depending on type and category of information.

9.4. Preparation For Shipment. When preparing classified material for physical shipment ensure the following:

9.4.1. Packaging. Comply with the requirements outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 4 when packaging classified material for shipment/transport.

9.4.1.1. In the case of bulky items or equipment, the outer cover may be a tarp or similar opaque covering to prevent the item from being viewed. The shell of an equipment item (i.e., aircraft part or laptop) may act as the "inner wrapper" provided it does not allow classified information or components to be viewed.

9.4.1.2. As a minimum, items not being mailed, but being shipped or moved as part of a daily operational missions (on or off base), will utilize an inner and an outer cover.

9.4.1.3. Any material outside approved storage will be kept under personal observation and positive control of an authorized individual. Material, will under no circumstances be left unattended while in transport. For example, member may not leave material "locked" in a vehicle, hotel safe or take material to a personal residence.

9.5. Courier Transport of Classified. Transport of classified occurs when an authorized and cleared individual moves classified from one location to another, either on or off an installation. In AFGSC both on and off installation transport require an individual to be appointed and trained as a courier. Courier will comply with the requirements outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 4, the AFGSC/CC GM and AFGSC/IP GMs. Requirements differ for on and off installation courier transport.

9.5.1. Administrative Requirements. Individuals must be cleared for access to the information transported, appointed by the owning commander/director/staff agency chief (hereafter called commander) and have a commander briefing and courier training documented by the USM.

9.5.1.1. Commanders will identify all unit couriers (on or off-base) in writing. The appointment letter will be reviewed and updated at least once every 2-years.

9.5.1.2. Off-base Couriers must also comply with additional requirements, to include:

9.5.1.2.1. An off-base commander appointment and briefing will be documented by the USM. The courier will keep a copy of the off-base courier appointment letter on them while performing off-base courier duties. The DD Form 2501, Courier Authorization Card will not be used for this.

9.5.1.3. Commanders must ensure briefcases and pouches used to transport classified (on or off-base) have an internal locking mechanism and that the exterior are properly marked with the unit's address, phone number, point-of-contact and that the case/pouch is serial numbered.

9.5.2. On-base Transport. This is the most common transport of classified and is defined within AFGSC as a courier activity. It includes movement of classified between offices, buildings or between on-base geographic locations. The AFGSC policy also requires specific administrative and training actions before unit members may move classified on-base. Specifically:

9.5.2.1. The missile field is considered on-base and on-base transport rules will be followed.

9.5.2.2. On-base Couriers will be appointed in writing by the unit commander, director/staff agency chief (called unit commander for the remainder of this publication).

9.5.2.3. An annual Commander's briefing will be accomplished and documented using the template briefing. This document may be pre-signed by the commander, but must be signed by the member to acknowledge understanding of duties and training and signed by the USM to validate completion of the training.

9.5.2.4. In-person completion (IAW AFGSC policy) of the localized AFGSC/IP Basic Courier Block Training. Units may supplement (add to but not replace) this block training with unit/section job-specific or specialized training (e.g., Combat Crews, Missile Electronic Encryption Devices, Aircrews, etc.).

9.5.2.5. Use of POVs is authorized for transport of classified while acting as on-base courier, if GOVs are not available.

9.5.3. Off-base Transport. This occurs when a cleared and authorized member move classified from one installation/activity to another geographically separated installation or activity. Additionally:

9.5.3.1. It may be authorized by the owning commander only as a last resort, only when other authorized methods are not viable. For instance, hand carrying a classified document that could be sent as a secured transmission to the receiving location is not authorized. Additionally:

9.5.3.1.1. Comply with administrative requirements for on-base courier above (i.e., appointment, CC brief, training, etc.).

9.5.3.1.2. A Transport Plan will be completed and must address deviations to travel plans and all other items outlined in the AFGSC/IP Handbook and/or GM to AFMAN 16-1404 to DoDM 5200.01, V3.

9.5.3.1.3. The Security Manager/Assistant, Special Security Office, or other Security Professional will inspect the classified for proper packaging and marking.

9.5.3.1.4. A lockable briefcase/pouch will be used, if possible, but cannot serve as the second layer of the double wrapping requirement.

9.5.3.1.5. The courier and/or escort will receive and acknowledge the commander's off-base courier briefing.

9.5.3.1.6. The courier will use/comply with transportation log, two-person requirement or other requirements for off-base transport of secret, as noted within the AFGSC/IP Handbook and/or GM to AFMAN 16-1404 to DoDM 5200.01, V3.

9.5.3.1.7. If flying the courier will use TSA pre-check.

9.5.3.2. If Top Secret information is being transported the owning commander will ensure compliance with AFGSC specific requirements, such as:

9.5.3.2.1. Approval from AFGSC/CC if commercial travel is used.

9.5.3.2.2. Completion of a transport plan, using the AFGSC template.

9.5.3.2.3. Any other requirements outlined for off-base transport of Top Secret, as noted within the AFGSC/IP Handbook and/or GM to AFMAN 16-1404 to DoDM 5200.01, V3.

9.5.4. Commercial Travel with Classified.

9.5.4.1. Failure to follow procedures in AFMAN 16-1404 to DoDM 5200.01, V3, the AFGSC/CC GM and applicable AFGSC/IP GMs may result in airport officials denying access to the mode of transportation or examining the classified package.

9.5.4.1.1. If airport security officials open the classified package report it as a security incident to the home station USM as soon as possible. Ensure

9.5.4.2. Comply with all AFGSC specific transportation requirements, e.g., waiver for TS to travel on commercial aircraft, use of TSA pre-check, two-person travel, etc.

Chapter 10

SAFEGUARDING SENSITIVE INFORMATION

10.1. General Policy. The AF policy for safeguarding is that each individual granted access to sensitive information (classified or CUI) is responsible to safeguard the material under their care from unauthorized access. This includes complying with special requirements associated with the material. Classified material will be stored only in approved storage containers or areas when not under the personal observation and control of an authorized person as outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 2.

10.1.1. Security Storage Areas. The USM will submit the special security area review checklist (**Attachment 8**) with each work order. This ensures the 5 CES Customer Service section is aware of and identifies any special security needs (e.g., open storage, open discussion, controlled areas, SIP facilities, etc.)..

10.1.1.1. Any work order identified with special security concerns will be forwarded to the 5 CES ISAG member who is the 5 CES security review official. The 5 CES security review official will ensure project details are forwarded to the appropriate security SME (i.e., 5 SFS, 5 CS, 5 BW/IP, local PSM for SIP, etc.).

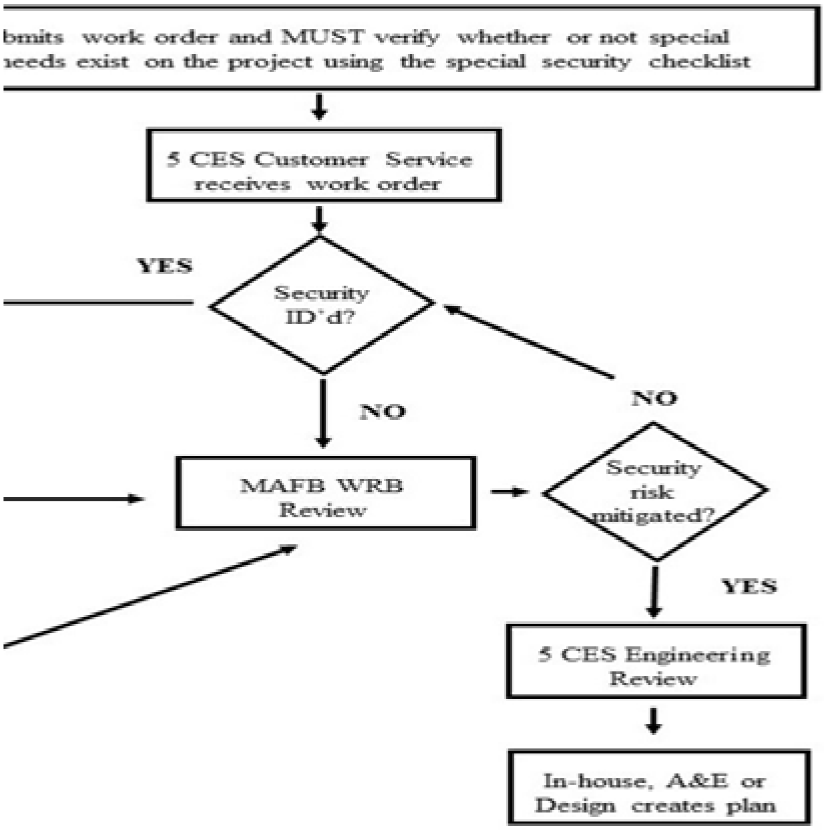
10.1.1.2. The 5 CES security review official liaisons between the security SME and the 5 CES engineering section to ensure completion of needed security reports before it goes to the Work-order Review Board (WRB).

10.1.1.3. The work order will indicate to use the security report and the engineering section will ensure any plans reflect the requirements outlined in the report.

10.1.1.4. The engineering section forwards the initial design plans to the 5 CES security review official who coordinates with the security SME to ensure security requirements.

10.1.1.5. **Figure 10.1** provides the flow for CE construction work orders and the plans developed to implement any required construction.

Figure 10.1. Work Order Submission Flow.


bmits work order and MUST verify whether or not special
ıeeds exist on the project using the special security checklist
5 CES Customer Service receives work order
YES
Security ID'd?
NO
NO
MAFB WRB Review
Security risk mitigated?
YES
5 CES Engineering Review
In-house, A&E or Design creates plan

10.2. Granting Access to Classified. Commanders will ensure the USM applies the standards found at **Chapter 4** of this instruction to ensure compliance with AFMAN 16-1404 to DODM 5200.01 and AFMAN 16-1405 to DoDM 5200.02.

10.2.1. Indoctrination to Database of Record. The USM is responsible for managing the in and out-processing of unit personnel into this database. Do not indoctrinate personnel for access or allow access to classified until all requirements from in **Chapter 4** of this instruction are completed.

10.2.2. Verifying Clearances. Use only the database of record to verify individual clearances, regardless of whether an individual is permanent party, visitor, or an inspector. The database of record reflects changes in real-time which is why entry authority lists are not used to verify clearances.

10.2.2.1. The USM may use procedures discussed at 4.3.3. and 4.8. to generate entry rosters.

10.3. Classified Aboard Aircraft. See AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 3, Section 6.a.(3), for specific rules concerning classified aboard aircraft.

10.3.1. At Minot AFB, Security Forces may conduct required checks **if** notified by the aircrew classified is present and the aircraft is sealed.

10.4. Closed Storage of Classified. Closed storage is defined as use of a GSA-approved security container for storage. Containers used to store classified must meet criteria outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 3. See **paragraph 10.6** for guidelines and procedures for requesting or using OS areas.

10.4.1. General Storage of Classified. The general requirements for storage of classified are discussed in AFMAN 16-1404 to DoDM 5200.01, Volume 3 Enclosure 3.

10.4.2. Courtesy Storage. If classified belonging to one agency is stored in a classified security container controlled by another agency, a memorandum outlining the arrangement should be established. As a minimum it would need to address:

10.4.2.1. The routine protection, accessing, and emergency destruction of the classified.

10.4.2.2. The fact the agency providing storage is responsible only for physical security and access control of the material. All other administrative control/accountability requirements are the responsibility of the owning agency.

10.4.2.3. The measures established to prevent inadvertent or unauthorized access to the material; for example, sealing packages, separate locking drawers, etc.

10.4.3. "In Transit" Storage of Classified. This provision is provided for storage of classified received after duty hours, which cannot be stored in unit containers or for personnel who arrive unexpectedly with classified and require storage.

10.4.3.1. The custodian of the in transit classified will pre-coordinate a drop off with one of the agencies noted below to arrange temporary storage. Failure to pre-coordinate the drop off may result in refusal of the agency to accept the material. The custodian will reclaim the material the next day or arrange for an authorized and cleared member to take control of the material.

10.4.3.2. Base Operations is designated as the repository for overnight storage of classified material up to Secret. The base command post will serve as the repository for TS material. Both locations will develop procedures for the receipt of transitory classified material.

10.4.3.3. The Defense Force Commander will ensure installation entry controllers are aware of the repository locations. The 5 FSS/CC will ensure lodging personnel are aware of the repository locations.

10.4.4. Repairing Approved general services administration (GSA) Containers. The 5 BW/IPO maintains a list of local GSA-approved technicians who may perform lock neutralizations without decertifying a container. Any modification or repair to a GSA-approved container (e.g., lock neutralization, welding, drilling, etc.) which does not comply with the Federal Standard results in it being decertified.

10.4.4.1. If unauthorized work is suspected, immediately contact the 5 BW/IPO to have the issue reviewed. The 5 BW/IPO will determine if the work requires recertification. If the container is decertified, it may not be used for storage of classified until recertified by a GSA-approved technician.

10.4.4.2. It is recommended units project to have a GSA-approved technician conduct a periodic maintenance inspection (PMI) on classified security containers once each 5 years.

10.4.4.3. Use of a non-GSA locksmith to gain entry to locked out containers is authorized, however; the container must be decertified until reviewed by a GSA-certified technician.

10.4.4.4. Document all repairs, maintenance actions and combination changes on the OP Form 89, *Maintenance Record for Security Containers/Vault Doors,* which replaced the AFTO Form 36, *Maintenance Record for Security Type Equipment*. Do not destroy old AFTO Form 36 documents, staple them to the new OP Form 89 as a historical record of maintenance.

10.4.5. Special Purpose Security Containers. These containers are intended only for use during deployed or contingency situations and can be identified by the size/shape and the fact they may have factory-made bolt holes to allow them to be secured to a facility floor. They are not authorized for use during normal operations. In any case, contact the 5 BW/IPO for additional security guidance prior to placing a special purpose container into service. The same rules concerning modifications applies to these containers, so any after-market welding, drilling, etc. will cause it to be decertified for use with classified.

10.5. Open Storage (OS) of Classified. Classified material will not be stored outside an approved security container unless it is maintained in an authorized OS area. Only areas certified in writing by the CIP are considered authorized. Due to the cost involved in establishing OS areas, they will not be approved for convenience. Commanders must notify the CIP, in writing, of any new OS area requirements and of any proposed changes to existing OS areas, prior to changes being made. The USM will ensure all approved OS areas are included on the unit consolidated container listing.

10.5.1. Initial and Recertification Surveys. The 5 BW/IPO will conduct these surveys and provide a written report listing required corrective actions/recommended fixes based on DoDM 5200.01, Volume 3 references. All corrective actions must be addressed before the area will be certified by the CIP for OS.

10.5.1.1. Initial surveys are conducted for facilities which do not currently exist, or which are being completely demolished.

10.5.1.2. Recertification surveys are conducted for existing area where substantial modifications are planned. Substantial modification may include any changes which alter the layout of the interior impacting alarm coverage (e.g., moving furniture) or where the areas physical integrity is impacted (e.g., removal of doors, walls, windows, adding or removing vents, pipes, etc.).

10.5.1.3. The 5 BW/IPI verifies corrective actions identified in the initial/recertification survey are completed and notifies the CIP if the facility meets standards. The CIP will endorse the certification request letter if the 5 BW/IPI confirms standards are met. Facilities which do not meet standards will not be certified.

10.5.1.4. In some circumstances, temporary compensatory measures may be available until mandatory actions noted in the initial or certification surveys are complete. These types of measures are typically intended to be short-term (i.e., 30 days or less).

10.5.1.5. An OS area is not automatically a controlled area. Controlled area designation decisions are made under the Resource Protection (RP) program rules in AFI 31-101.

10.5.1.6. The USM will ensure specific written OS area entry and circulation controls are developed. These procedures may be included in an already existing unit OI.

10.5.2. Intrusion Detection Systems. Utilize the Protection Level 4 alarmed area rules found in Integrated Defense Plan for OS areas; with the following exceptions:

10.5.2.1. If alarms fail on a secret OS area, the owner/user will contact the 5 BW/IPO to determine if a cleared individual must be posted in the facility or if 4 hour checks of the facility by a cleared member (requires entry and walk through) are authorized IAW AFMAN 16-1404, Volume 3, Enclosure 3, Section 3.a. This provision may also be addressed in the facility certification report, but the USM should always contact the 5 BW/IPO prior to implementing this measure.

10.5.2.2. If alarms fail on a TS OS facility, the owner user must post a cleared individual in the facility. Checks of all vulnerable areas (e.g., doors, windows, vents, etc.) will be conducted at least once every two hours until alarms are restored.

10.5.3. Physical Security Checklist. The 5 BW/IPI will conduct OS and/or OD surveys using localized checklists, derived from AFMAN 16-1404 DoDM 5200.01, Volume 3, Appendix to Enclosure 3.

10.5.4. Certification/Recertification of OS Areas. The CIP certifies new OS areas and, if necessary, recertifies existing OS areas where substantial changes have occurred. Specific requirements are detailed below.

10.5.4.1. Commanders will not use areas for OS of classified until certified by the CIP.

10.5.4.2. The CIP will certify OS areas once the 5 BW/IPI survey report indicates all corrective measures are completed.

10.5.4.3. Maintain initial, certification, supplemental and recertification surveys for OS areas at the facility, in the USM's program binder and in the 5 BW/IPO unit folder.

10.5.4.4. The unit commander, through the USM, will notify the 5 BW/IPO of any "substantial" renovation, remodeling work proposed for approved unit OS areas. The notification must be given prior to modifications, preferably 30 days prior. This allows the 5 BW/IPO sufficient time to determine what actions are required and which personnel are needed for the security survey. Include a detailed risk mitigation plan for protecting classified material/operations normally stored in the facility.

10.6. Certifying Open Discussion (OD) Areas. Commanders will notify the CIP, in writing, of proposed new OD or changes to existing OD areas. An OD does NOT authorize classified material to be stored in the area. The general rules noted in **paragraph 10.6** above apply to OD areas, to include including OD areas on the unit consolidated container listing.

10.6.1. Discussing Classified Information. Classified information shall be transmitted IAW DoDM 5200.01, Volume 3, Enclosure 4. This means approved secure communications and approved for specified classification level of the information. When considering classified meetings or conferences, the USM of the sponsoring agency must ensure compliance with all security provisions outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 2, Section 16. Unit members sponsoring a classified conference/meeting will work with the USM to ensure all necessary actions are taken.

10.6.1.1. In-office discussions of classified by personnel must ensure all participants in the conversation are properly cleared and have a valid need-to-know and that any classified conversation cannot be overheard by uncleared/unauthorized individuals.

10.6.2. Certified OD Areas. The CIP is the certification authority for approving/disapproving OD areas. Areas will be certified based on the initial justification from the request letter and completion of corrective actions noted in the physical security survey conducted by 5 BW/IPI and 5 CES/CECNA. These areas will not be approved for convenience.

10.6.2.1. Commanders will not use OD areas prior to the area being certified by the CIP.

10.6.2.2. Maintain initial, certification, supplemental and recertification surveys for OD areas at the facility, in the USM's program binder and in the 5 BW/IPO unit folder.

10.6.2.3. Units will develop specific written entry and circulation controls for the OD area which may be included in an already existing unit OI.

10.6.2.4. Use the guidelines in DoDM 5200.01, Volume 3, Enclosure 2, Section 16 for conducting off-base conferences.

10.6.2.5. Alarms are not required for any OD unless a specific threat is identified by the security survey team.

10.7. Certifying SIP OS/OD Areas. Contact the MAJCOM SSO and/or installation PSM for guidance on SIP facilities.

10.8. Disposition and Destruction of Classified and CUI. Follow the guidelines in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 3 when making decisions to retain and/or destroy sensitive material.

10.8.1. Central Destruction Facility. Minot AFB has no central destruction facility for classified or CUI. Agencies are responsible to obtain approved destruction equipment which meets the DoD guidelines.

10.8.2. Information Technology Related Materials. The National Security Agency (NSA) may assist with destruction of some classified electronic media (e.g., hard drives, etc.). Contact your USM for specific requirements to arrange for destruction of classified electronic media.

10.8.2.1. The primary functional expert and POC for units requiring NSA destruction capabilities is the USM. The USM will ensure unit members comply with any and all mailing and preparation requirements specified by NSA and will ensure all packages comply prior to allowing the package to be mailed.

10.8.3. Destruction of CUI. Units must ensure comply with the standard outlined in DoDI 5200.48_DAFI 16-1403. At **paragraph 4.5**b., it states CUI, "…may be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and unrecoverable. This means any other methods which render the information unreadable, indecipherable, and irrecoverable would be authorized, however; use of a classified shredder is noted as meeting this standard.

10.8.4. Annual Classified Cleanout Day. The annual classified cleanout date for Minot AFB is to be completed on or before 15 Feb of each calendar year. The USM will ensure agencies are complying with this requirement during semiannual self-assessments. It is acceptable to complete this action over an extended period or prior to the 15 Feb deadline.

10.8.4.1. The 5 BW/IPO will review compliance with retention/destruction rules for classified during annual unit inspections/reviews.

10.9. Access Termination to Sensitive Information.

10.9.1. Access Termination to Classified. Refer to **chapter 7**.

10.9.2. Access Termination to CUI. Individuals shall be debriefed with the following topics covered IAW AFMAN 16-1404, Vol 3, enclosure 2

10.9.2.1. Remind individuals of their responsibility to continue to protect controlled unclassified information to which they had access.

10.9.2.2. Discuss procedures for reporting any unauthorized attempt to gain access to such information.

10.9.2.3. Remind individuals of the prohibition for retaining CUI when leaving the organization.

10.10. Alternative/Compensatory Control Measures. AF prohibits use of these measures.

10.11. Classified Process Area Emergency Plans.

10.11.1. Emergency plans are required to be posted in all activity spaces that process or store classified information/material. Refer to AFMAN 16-1404V3, appendix 2 for an emergency plan template that addresses the minimum plan requirements.

10.11.2. Ensure plan procedures also include a requirement to debrief and completion of a non-disclosure agreement if non-clear emergency personnel enter a classified processing area due to an emergency like fire/medical response and classified was present and exposed.

Chapter 11

SECENT EDUCATION AND TRAINING

11.1. General Requirements. The SECENT training described below meets all mandatory requirements outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 5 and also includes mandatory SECENT-related training for INFOSEC, PERSEC, C-InT and addresses CUI and OPSEC installation focus areas. Distinct types of mandatory training are described below and include initial orientation training, annual refresher training, continuing training and specialized training.

11.2. Unit SECENT Training. At Minot AFB, unit SECENT training covers the following programs: PERSEC (DoDM 5200.02), C-InTP (AFI 16-1402) and Privacy (AFI 33-332) with local focus area for CUI (DoDI 5200-48) and OPSEC (AFI 10-701). The Minot AFB training plan was coordinated with the AFGSC functional experts for the noted areas and validated as meeting established training requirements. This training is provided during the initial and refresher training discussed below. Unit commanders use the USM to implement the SECENT education and training program. The USM may require access to unit members' training documentation to validate requirements are completed.

11.2.1. Initial SECENT Training. There are two types of "initial" training to consider. The "cleared" training applies to members with access to classified information and the "uncleared" applies to those with no access to classified. The requirements for cleared training are outlined in AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 5. Both cleared and uncleared training require completion of the DoD Cybersecurity Challenge and contain information from AFMAN 16-1405 to DoDM 5200.02, DoDI 5200.48_DAFI 16-1403, AFI 10-701 and AFI 16-1402 which covers Continuous Evaluation, C-InT and addresses CUI and OPSEC installation focus areas training requirements. Additionally, both categories require annual refresher and continuous training.

11.2.1.1. The USM must document completion of initial cleared training in Database of Record under the non-SCI indoctrination date by verifying completion of SECENT slides and required MyLearning courses.

11.2.1.2. Initial training for uncleared personnel is required for GS civilians or contractor personnel not authorized access to classified (e.g., a UMD SAR code 8 GS employee). The training consists of the noted MyLearning training and the SECENT slides. It is acceptable for commanders to require uncleared personnel to complete initial cleared training. If this is the case, ensure it is addressed in the SECENT OI.

11.2.1.3. The method of delivery for the SECENT slides is determined by the unit in the unit SECENT OI. It may be conducted as a mass briefing, individually or by forwarding slides via e-mail. Whichever case is used, the USM must verify completion and document the training in writing.

11.2.2. Annual Refresher and Continuing Education Training. The SECENT program uses the same method described above to complete annual refresher training. The USM may provide a portion of the SECENT slides on a semiannual (or more frequent) basis to meet INFOSEC, C-InT and CE continuing education training requirements.

11.2.2.1. The USM will ensure the unit method/plan for conducting and tracking annual refresher and continuing education training is reflected in the unit's SECENT OI.

11.2.2.2. The USM must maintain written documentation of who took the training and how/when it was distributed and completed.

11.2.2.3. The USM will verify members have completed the required MyLearning training. A quarterly (or more frequent) roster from the unit training manager is acceptable.

11.2.2.4. If continuing education training is not conducted by sending out SECENT slides semiannually (or more frequently) the USM will outline how the training is accomplished and documented in the unit's SECENT OI.

11.2.2.5. The USM ensures cleared contractors are integrated into the unit's SECENT training program and ensures they complete needed SECENT . The actual training may be conducted by the contractor, USM, or other training personnel. This should be specified in the VGSA.

11.2.2.6. The USM is responsible to ensure any uncleared contractors assigned to the unit complete required SECENT training. Documentation of completion will be maintained in the USM binder.

11.2.3. Additional SECENT Related Training. The USM will ensure any additional SECENT training is documented in the SECENT OI (e.g., unit has alarms, controlled area, etc.). The USM will ensure locally created lesson plans for this training are coordinated through the 5 BW/IPO.

11.2.4. Pre-Deployment Training. The USM will ensure pre-deployment enhanced security training, if required by the unit, is included in the SECENT OI. This training is required for deploying personnel supporting operational contingencies as outlined in DoDM 5200.01, Volume 3, Enclosure 5.

11.2.4.1. This training should build on the information already included in SECENT Initial/Annual Refresher Training.

11.2.4.2. Ensure any members deploying receive refresher training on INFOSEC. As a minimum include: use of NATO information, how to handle/protect US collateral/CUI/foreign government information where foreign allies are present and rules for sharing US information with allies.

11.2.4.3. Ensure all deploying personnel receive mission-oriented OPSEC education. Ensure members are familiar with potential threats related to the organization, critical information for the mission it supports, job specific OPSEC indicators and the OPSEC measures unique to that specific event/AOR.

11.2.5. Documenting/Tracking SECENT Training. The USM is responsible to document and track all required SECENT training. Also:

11.2.5.1. Cleared/Uncleared training should be completed within 90 days of arrival.

11.2.5.2. The USM must be able to provide proof training, for example a unit training roster with training, names, dates. Computer databases, sign-in rosters which identify topics covered and members who attended from commander's calls/roll call training or e-mail read receipts are acceptable methods of tracking SECENT Annual, Refresher or continuing training.

11.2.5.3. Initial Cleared Training MUST be completed prior to member accessing classified or CUI. Record initial training for cleared personnel in the "non-SCI Indoctrination" section of the database of record.

11.2.5.4. Initial Uncleared Training MUST be completed prior to NIPR access or allowing access to CUI documents.

11.3. Derivative Training. Unit commanders identify unit derivative classifiers and ensure they are trained annually IAW AFMAN 16-1404 to DoDM 5200.01, Volume 3, Enclosure 5, Section 7.c. Volume 3, Enclosure 5, Section 7.c. The USM provides oversight at the unit level and will ensure:

11.3.1. Appointing Derivative Classifiers. A Unit Derivative Classifier Appointment letter signed by the Commander is provided to 5 BW/IPO. Do not add derivative classifiers to the letter until required training is complete.

11.3.2. Unit Guidance on Derivative Actions. Any unit specific procedures concerning derivative classification will be outlined in the unit's SECENT OI. As a minimum, include the training/appointment requirements and the fact failure to complete annual refresher training will result in removal from the Derivative Classifiers Appointment letter.

11.3.3. Administrative Items. The USM will provide the 5 BW/IPO with a copy of the Derivative Classifiers Appointment letter and also maintain one in the USM binder. The USM will maintain copies of training records and must be able to provide them on request

11.3.4. Initial Derivative Classifier Training: Derivative classifiers will complete the Defense Security Service (DSS) Derivative Classification and the Marking Classified Information web-based courses located on the DSS website. These are the only courses which meets the requirements outlined in of DoDM 5200.01, Volume 3, Enclosure 5. Contact your USM if you are having issues accessing the website.

11.3.5. Refresher Derivative Classifier Training. Derivative classifiers must accomplish derivative refresher training **annually.** The Marking Classified course is a one-time requirement and is not required for the derivative refresher training.

11.3.6. SIPRNet Access. All SIPRNet users are inherently derivative classifiers and the USM will validate required training from **chapter 6** of this instruction is completed prior to completing block 27 of the DD Form 2875.

11.3.7. Oversight. The 5 BW/IPO provides oversight by validating completion of training during scheduled inspections.

11.4. Container Custodian Training. See **paragraph 1.12.2** for requirements.

11.5. Combining Security-Related Disciplines with SECENT Training. Annual SECENT training may be combined with other security disciplines, such as SCI, alarm operations, controlled area, Force Protection, etc. so long as the following items are considered:

11.5.1. Responsibilities for Combined Training. The 5 BW/IPO and USMs are not responsible for developing, conducting or tracking of non-IP training.

11.5.2. Review of Material. If a combined security approach is used for training, the USM must ensure all refresher/continuing training from SECENT training curriculum is included. The IP-related portions of the course material will be reviewed by the 5 BW/IPO.

11.6. The 5 BW/IPO Training Responsibilities. The 5 BW/IPO provides oversight and assists USMs, if requested, in developing localized IP-related SECENT training.

11.6.1. USM Training. As security professionals USMs must complete training outlined in DoDM 5200.01, Volume 1 and Volume 3 to properly performing duties. Commanders should consider setting aside funding for USMs to attend in-residence DSS courses. As a minimum, USMs will:

11.6.1.1. Complete the DSS, MyLearning and other site course as identified by 5 BW/IPOwithin 60 days of appointment. This training also includes courses required to perform CUI and OPSEC coordinator duties.

11.6.1.2. Attend the USM initial training course conducted by the 5 BW/IPO.

11.6.1.3. Commanders may request one-on-one USM training on a case-by-case basis if extraordinary situations prevent a USM from attending the local USM training course. Due to amount of time required to conduct the class for one person, this option is only approved on a case-by-case basis

11.6.1.4. The 5 BW/IPO will document USM training with a certificate of completion. A copy will be maintained in the 5 BW/IPO unit folder and in the USM binder. The USM is responsible for ensuring this training is documented in any other needed systems (e.g., AF Form 1098, etc.).

11.6.1.5. If a USM fails to accomplish required training within the specified timelines, the CIP will notify the commander the individual is unqualified for USM duty and must be replaced.

11.6.2. Security Officer Visit Admin DISS or successor system NBIS Access. If individuals are appointed by the commander, in writing, they may be granted Security Officer Visit Admin access in DISS or successor system NBIS.

11.6.2.1. The USM will provide a copy of the appointment letter and verify required training is completed using the USM training tracker (provided by 5 BW/IPO).

11.6.2.2. The USM is responsible to maintain copies of applicable training and to ensure currency of the noted courses is also maintained.

11.6.3. Other Specialized Training. The 5 BW/IPO is available to assist units in developing unit specific localized IP training plans, on request. The USM will ensure the 5 BW/IPO coordinates on any localized unit training plans covering IP topics (e.g., container custodian training, derivative training, etc.).

11.7. The USM Recognition Program. The 5 BW/IPO uses the following procedures to recognize primary USMs who consistently exceed standards.

11.7.1. USM of the Month. The 5 BW/IPO selects the USM with the least PSI submission errors for the USM of the Month. If multiple USMs tie for the least PSI errors, other factors are considered to break the tie (i.e., least inspection finds, assistance rendered etc.).

11.7.2. USM of the Quarter/Year. The USM of the quarter is selected from the monthly winners and the annual winner is selected from quarterly winners. The criteria for quarterly/annual winners is the same as monthly winners, but includes any data over the period under consideration (e.g., quarter/year).

11.7.3. USM Program of the Year. Use aggregate data from PSIs, completion of taskers (monthly priority listing responses, etc.), inspection results, etc.

Chapter 12

SECURITY INCIDENTS

12.1. General Information. All personnel will comply with DoDM 5200.01, Volume 3, Enclosure 6 and AFMAN16-1404, when accomplishing requirements for actual/potential compromises of classified information. If possible, report classified security incidents using secure communications.

12.2. Conducting Incident/Investigation Reports. The commander having control of the individual(s) involved will act as the appointing official (AO) for the inquiry or investigating official (IO). If the individual who would normally act as the appointing official is involved in the incident, the next level of command will act as the AO. The report goes directly from the IO to the CIP and will not to be routed through unit channels prior to CIP/JA review.

12.2.1. Time Limits. The AO will ensure the IO is appointed within 2-duty days of the notification. The required briefings by 5 BW/IPO and the 5 BW Legal Office (JA) should also be completed within this timeframe.

12.2.1.1. The initial suspense will be established by the 5 BW/IPO and will be within 10 duty days of the incident being reported.

12.2.1.2. The CIP may grant up to a 10-day extension on a case-by-case basis. If the IO is prevented or delayed from accomplishing the report for an extended period (e.g., 5 or more consecutive days), the AO should consider reassigning the inquiry to a new official.

12.2.1.3. The USM will not be appointed as the IO.

12.2.2. Report Format. The IO will use the report format provided by 5 BW/IPI when completing IO reports. Failure to use this format will result in the report being rejected. Mark and handle the IO report as CUI, at a minimum.

12.2.3. Statements. Formal statements (i.e., AF Form 1168, *Statement of Suspect, Witness, Complainant*) are not mandatory for inquiries, but will be used when the report is part of an investigation.

12.2.3.1. When conducting an inquiry, the IO may quote personnel within the body of the IO report, and collect statements using a memorandum format via e-mail or with an AF Form 1168.

12.2.4. COMSEC Related Incidents. When a security incident involves COMSEC material, the USM will ensure both 5 CS/SCXSC (723-1301), and 5 BW/IPI are notified. The circumstances and specific information surrounding the incident may be classified, use secure means to report.

12.2.4.1. If the situation generates a COMSEC report, a collateral inquiry report is not required.

12.2.5. Inquiry/Investigating Officials. Use AFI 90-301 as a guideline for selecting inquiry or IOs. Specifically:

12.2.5.1. The IO must be objective, unbiased, and not in the direct chain-of-command of those being investigated.

12.2.5.2. The IO must be of sufficient experience, maturity, have sound judgement and not be less in rank or grade than the person(s) involved with the incident.

12.2.5.3. In order to meet the intent of **paragraph 12.2.5.2** above, as a minimum, IOs must be an officer, E-7, GS-9 or above.

12.3. Incidents with Electronic Devices in Classified Processing Areas. Electronics in classified processing areas represent an extraordinary threat to security, see **paragraph 6.4** of this instruction for specific actions.

12.4. CMI/Data Spillage Incidents/NDCI. If classified information is improperly transmitted over unapproved systems, follow the procedures outlined in **paragraph 6.6** of this instruction.

12.5. Closing Incidents. The AO will close incidents with a memorandum validating corrective actions have been completed or stating they non-concur with the findings.

12.5.1. Actions if an AO Non-Concurs. An appointing official may challenge all or part of the findings/conclusions, but must provide specific reasons in the memorandum. In no case will the IO be required to revise their findings.

12.5.1.1. If the non-concur is reviewed by the CIP and 5 BW/JA and they continue to support the IO's findings/conclusions, the report will be returned to the AO for reconsideration of the original findings.

12.5.1.2. If the AO still non-concurs a second review will be completed with the entire package being reviewed by the next level of command for final resolution.

Chapter 13

COUNTER-INSIDER THREAT PROGRAM (C-INTP)

13.1. Purpose. This Air Force C-InTP is implemented through this instruction, as a part of the overall SECENT, IAW AFPD 16-14 and AFI 16-1402. It is:

13.1.1. The C-InTP Concept. The C-InTP is implemented through and managed in conjunction with the SECENT program. C-InTP requirements are integrated into existing programs and specific training is provided for portions of SECENT, through IP annual training, and includes specific C-InTP and continuous evaluation topics. The C-InTP program ensures:

13.1.1.1. AF personnel are continuously evaluated using enhanced technical capabilities to monitor and audit user activity on information systems.

13.1.1.2. Leveraging the SECENT portfolios associated with Information, Industrial, and Personnel Security to improve existing installation insider threat detection and taking actions to mitigate noted deficiencies.

13.1.1.3. By integrating and standardizing processes and procedures across the SECENT to help detect, mitigate and respond to insider threats, while ensuring civil liberties and privacy rights are safeguarded.

13.2. C-InTP Governance. The key directives for the C-InTP are DoDI 5200.43, AFPD 16-14 and AFI 16-1402.The Minot AFB ISAG and ID/ATWG coordinate with Minot AFB Intelligence Community (IC) via the assigned members to ensure timely sharing of information to ensure that pertinent information reaches AF C-InTP personnel so they can take appropriate action.

13.3. C-InTP Objectives. In general, the functions of identifying strategic goals, approving program implementations, integrating policy and procedures and developing prioritized resource recommendations is accomplished through the normal course of the ID/ATWG and ISAG meetings then forwarded to leadership for approval. The overarching goal of the Minot AFB C-InTP is to mitigate the threat represented by insiders through the following objectives:

13.3.1. Network Monitoring and Auditing. This C-InTP function is accomplished through mandated AF Cyber Security actions. Emerging cyber-threats and risks are also discussed in the ISAG and forwarded to affected agencies, as needed.

13.3.2. Information Sharing. The Minot AFB C-InTP community of SMEs includes, but is not limited to: AFOSI, Force Protection, Security Forces Investigations, Cyber Security, the IFC members and the 5 BW/IPO.

13.3.2.1. Any derogatory information received by any reporting agencies, i.e., PRAP, SAP, IP will be shared between offices.

13.3.3. Physical Security. This objective is accomplished through on-site reviews conducted by 5 BW/IPO, Resource Protection and the WCO. The goal is to prevent physical access to information. The executive groups provide any needed local guidance in their publications and Minot AFB commanders ensure mandated security controls are in place and verify unit members routinely use them to protect assets (i.e., information, people and/or equipment).

13.3.4. Training and Awareness. This objective is accomplished by incorporating C-InTP principles into already existing security training (e.g., SECENT initial/refresher training) to ensure all members are trained and aware of insider threat principles and reporting responsibilities.

13.3.5. Insider Threat Reporting and Response. This goal is met through existing reporting procedures and the noted training. Response to specifically identified threats will be assessed by the IFC, who will forward information to agencies affected or which need to take specific actions (e.g., AFOSI CI, 5 BW/IPP, unit commanders, etc.).

13.4. Responsibilities. The responsibilities and duties of the Minot AFB C-InTP program are outlined in the guidance of the various agencies that monitor the insider threat. The 5 BW/IPO responsibilities are essentially the same as those outlined in **chapter 1** of this instruction. Additionally:

13.4.1. Oversight. The 5 BW/CV has general oversight for the Minot AFB C-InTP and executes this oversight through this instruction to ensure the following actions:

13.4.1.1. Development of policy and checklists to provide needed compliance and management oversight for the Minot AFB C-InTP. This is accomplished primarily through this instruction.

13.4.1.2. Identifying and coordinating recommend courses of actions to senior leaders as needed. This will be accomplished through the ID/ATEC or the ISAG, as necessary. The IFC will forward any needed guidance changes to the appropriate executive group.

13.4.1.3. Coordinating and integrating needed local policy changes which result from changes to the DoD or AF C-InTP. This is done through the appropriate executive group.

13.4.1.4. Written procedures are established as needed. This instruction serves as the base for the written guidance; however, specific agencies may need to develop agency specific guidance on insider threat response.

13.4.2. ID/ATEC. The ID/ATEC is responsible for most traditional security responses to identified insider threat risks. Where the threat is primarily to information assets or crosses multiple functional organizations, the ID/ATEC should refer the issue to the ISAG.

13.4.3. Installation SECENT Advisory Group. The ISAG is a cross-functional security group which is responsible for non-traditional security issues to information assets. They require notification of potential derogatory information discovered as the result of insider threat reviews to be sent to the 5 BW/IPP, ensuring commanders are notified of the need to review members for CE.

13.4.4. IFC. This group is the primary agency which receives insider threat warning information. The AFOSI CI section is the primary action agency for the IFC. When information is received by members of the IFC, they will:

13.4.4.1. Ensure appropriate CI agencies are notified. Other security agencies will be notified, as authorized, once active investigations are concluded. Ensure the personnel security office is notified when final reports of investigations are sent to commanders to ensure proper CE notifications are also provided.

13.4.4.2. Ensure notifications are made in a timely manner to potentially impacted security agencies to ensure danger from insider activity is mitigated. These notifications are primarily accomplished through the Minot AFB IFC with AFOSI CI acting as the lead for determining whether information may be released.

13.4.4.3. Ensure information reviewed is forwarded to appropriate security agencies to ensure all mitigation actions needed are accomplished. If AFOSI CI or 5 SFS Investigations are notified of unauthorized or criminal activity involving classified information, they will notify 5 BW/IPP, so long as the notification does not jeopardize any on-going investigation. Additionally, once on-going investigations are completed, they will notify 5 BW/IPP when the commander receives the report.

Chapter 14

COMMON ACCESS CARD (CAC) FOR UNCLEARED PERSONNEL

14.1. Policy And Program Management. This chapter establishes guidance for issuance of a CAC to "uncleared" contractor or volunteer personnel in accordance with HSPD-12, DoDM 1000.13, Volume 1, DoDI 5200.46 and DoDM 5200.02. It also locally implements the Trusted Associate Sponsorship System (TASS). The 5 BW/CC appoints the 5 MSG/CC as the Minot AFB Installation Point of Contact (IPOC) to manage and oversee the TASS process. This responsibility may be delegated no lower than the 5 MSG/CD.

14.2. Duties and Responsibilities. The IPOC implements the Minot AFB TASS program on behalf of the 5 BW/CC through the TASS Security Manager (TASM). Tenant units must comply with Minot AFB TASS program requirements or 5 FSS will deny the issue of a CAC to the uncleared personnel.

14.2.1. IPOC. In lieu of SAF guidance, the IPOC provides local guidance for actions required in DoDM 1000.13, Volume 1 through this instruction. Issuance of a CAC to uncleared contractors is requested, documented and tracked through TASS.

14.2.1.1. The IPOC will ensure the TASM maintains the AF program MICT checklists to validate compliance during self-assessments and CCIP events.

14.2.1.2. The IPOC appoints 5 CONS to provide a primary and at least one assistant TASM from 5 CONS, in writing, to manage TASS.

14.2.2. TASM. The TASM manages and monitors requests and issuance of CACs through TASS. They are also responsible to provide needed program oversight and ensure unit trusted associates (TAs) are identified and trained IAW DoDM 1000.13, Volume 1. The training material provided by the DoD TASS program manager will be used to comply with any required training.

14.2.2.1. The primary TASM will ensure the appropriate MICT/CCIP checklist is loaded against their MICT/CCIP program to validate compliance during self-assessments and IG CCIP events.

14.2.2.2. The TASM will maintain a continuity book which has a listing of current TAs (contact information, training completion dates), TA appointment letters and copies of IPOC and TASM appointment letter and TASM training certificates.

14.2.3. TAs. Unit commander requiring contractor support will appoint a primary TA, in writing, with a copy of the appointment letter provided to the TASM. The commander should consider appointing at least one assistant, but must do so if the primary TA's uncleared contractor population is 90 or more. The TA is the most critical part to the TASS program and it is imperative for them to be fully trained and comply with all duties noted below. The commander and unit TA will ensure the appropriate MICT/CCIP checklist is loaded against their MICT/CCIP program to ensure the compliance during self and IG assessments.

14.2.3.1. Commanders are highly encouraged to use their the USM to act as TAs. This is due to the fact USMs are already familiar with PSI requirements and have access to the database of record, which can show if an individual already has a "cleared" PSI, alleviating the need to submit a new PSI. The TA will use the checklist at **Attachment 8** as a guide to help when requesting PSIs for contractors.

14.2.3.2. If the TA is not the USM, the TA "MUST" specifically verify with the USM whether or not an applicant already has a suitable PSI for CAC issuance.

14.2.3.3. If a contractor must be submitted for a PSI, the TA will ensure the USM makes the needed e-QIP or successor system eApp request. DO NOT approve the individual for a CAC in TASS until the USM confirms the TIER-1 is returned as favorable. If an temporary CAC is needed, see **paragraph 14.3.3** for requirements.

14.2.3.4. The Primary TA will maintain a continuity book which has copies of the noted checklists, a list of all current contractors issued CACs, a copy of their commander appointment letter, copies of completed "Contractor CAC Issue Checklist" for current contractors, and a copy of the TA training certificate for themselves and any assistant TAs.

14.2.3.5. Failure to properly execute TA duties/responsibilities may be considered abuse of computer systems and/or purposeful violation of security requirements and may result in loss of access to the network and/or classified information.

14.2.4. Actions Required by the TA. The unit TA will ensure the following actions are accomplished in regards to their unit TASS program:

14.2.4.1. Validate the contractor has a requirement for CAC issue against the PWS and run the checklist at **Attachment 7** to ensure all actions are accomplished.

14.2.4.2. Verify contractor has continued affiliation every 180 days.

14.2.4.3. Ensure contractor CACs are revoked in TASS upon termination of affiliation of the contractor or contract.

14.2.4.4. Retrieve CACs upon contractor or contract termination.

14.2.5. Human Resource (HR) Offices. The HR for Minot AFB resides in the CPF and NAF. They will use the already established procedures outlined in **chapter 4** above for submitting, monitoring and tracking initial-hire, uncleared federal government employees.

14.3. Requirements for PSI. Anyone requiring long-term (6 months or more) access to the installation, an installation facility or the local area network (LAN) is required to have, as a minimum, a TIER-1 investigation. This includes APF, NAF, contractors or volunteers (who require installation entry or LAN access). If there is a conflict between this instruction and a 31-series AFI, the AFI will take precedence.

14.3.1. Installation Entry Only. If an individual already has a valid form of identification for installation entry (e.g., Dependent ID card) and does not require LAN access, IAW DoDM 1000.13, Volume 1, they do NOT require a PSI.

14.3.2. Designated Uncleared PSI Office. The 5 BW/CC designates the 5 FSS/FSC as the agency which will process Tier 1, 2 and 4 PSIs.

14.3.2.1. Use procedures in **chapter 4** of this instruction to process these PSIs.

14.3.3. Issuing Temporary CACs. An temporary CAC may be approved for an uncleared contractor by the sponsoring unit commander prior to completion of the TIER-1 ONLY if the FBI fingerprint check has been returned to OPM without derogatory information.

14.3.3.1. If the TA is not the USM, the TA will contact the USM if they need assistance in determining status of the TIER-1 or to get an update on the FBI fingerprint checks for consideration of an temporary CAC. The TA will NOT make direct contact to 5 BW/IP, AFGSC/IP, AF, DoD or OPM directly.

14.3.4. If temporary CaC issuance is used for NIPRNet access, the USM will annotate the DD Form 2875 with the following statement, "Temporary CaC authorized IAW DoDM 1000.13, Volume, Enclosure 2, Section 3.b., based on favorable fingerprint check, pending final Tier completion."

14.4. Tracking Uncleared Contractor PSIs. The Central Verification System (CVS) is the system of record for uncleared access PSIs, to include Child and Youth Program (CYP) cases. Although the database of record may be used to validate if previous PSI exists, it does not track uncleared cases or show status of uncleared PSIs.

14.4.1. Monitoring Uncleared Contractor PSIs. It is the requesting USM's responsibility to monitor status of and/or request updates to these cases from 5 FSS/FSC. This includes tracking any state repository checks submitted for CYP cases.

14.4.2. Suitability Determinations for Uncleared Contractor PSIs. See **paragraph 4.4.11**.

14.5. Network Access Suspension. See **chapter 6** of this instruction for actions to take if network access must be suspended for uncleared contractors.

Chapter 15

OPERATIONS SECURITY (OPSEC) PROGRAM

15.1. Purpose. The Air Force OPSEC program is implemented at Minot AFB through this instruction, as a part of the overall SECENT program, IAW AFI 10-701.

15.2. OPSEC Overview. OPSEC is an information-related capability that preserves friendly essential information by using a process to identify, control and protect critical information and indicators.

15.2.1. OPSEC supports 5 BW and 91 MW local planning, preparation, execution and post execution phases of all activities, operations and programs across the entire spectrum of operations. Enhanced operational effectiveness occurs when decision-makers apply OPSEC from the earliest stages of planning. Unit OPSEC Coordinators assist commanders and directors with implementing and practicing effective OPSEC.

15.2.2. OPSEC is a commander's/director's responsibility and is established, managed and implemented at all levels (wing, group, unit, agency, tenant unit, etc.) throughout Minot AFB.

15.2.2.1. Management of OPSEC at Minot AFB resides in the 5 BW/IP (OPSEC PM) and in each organization/agency (OPSEC Coordinators).

15.3. Roles and Responsibilities.

15.3.1. 5th Bomb Wing Commander and 91st Missile Wing Commander will:

15.3.1.1. Appoint in writing, a primary OPSEC Signature Manager at grades no lower than O-3, E-7 or GS-12 and appoint in writing an alternate OPSEC Signature Manager at grades no lower than O-1, E-6 or GS-9.

15.3.1.2. Directs unit-/agency-level OPSEC Coordinators (dual-hatted as USMs) be appointed in all subordinate organizations and on the commander's/director's staff to implement and enhance the effectiveness of OPSEC within the organization and support the installation OPSEC Program Manager.

15.3.1.3. Approve and issue an installation CIIL. Ensure measures are taken to manage signatures, prevent disclosures of critical information and indicators and maintain essential secrecy.

15.3.1.4. Ensure annual OPSEC inspection/reviews are conducted. These events will be arranged and conducted by the OPSEC PM in coordination with 5 BW/IP and respective IG Office (5 BW and/or 91 MW).

15.3.2. 5th Bomb Wing Commander:

15.3.2.1. Ensure OPSEC considerations are included in Minot AFB Public Affairs reviews and all other public information release processes.

15.3.2.2. Ensure contract requirement owners coordinate with OPSEC Coordinators and the OPSEC PMs, the contracting office and other stakeholders to ensure mission critical information and indicators are not placed in publicly available contract documents.

15.3.2.3. Ensure An installation-level OPSEC Working Group is established and integrated with similar protection/security related working groups.

15.3.2.4. Approve the Minot AFB Annual OPSEC Report; OPSEC PM submits report to the AFGSC/OPSEC PM per AFI 10-701.

15.3.3. Commanders and Directors.

15.3.3.1. Appoint, in writing, an OPSEC Coordinator(s) (dual-hatted as USMs) to enhance the effectiveness of OPSEC within the organization and support the installation's OPSEC Program Manager.

15.3.3.2. Approves and issues a unit-level CIIL. Ensure measures are taken to manage signatures, prevent disclosures of critical information and indicators and maintain essential secrecy.

15.3.4. Chief, Information Protection. Provides oversight of the Minot AFB OPSEC Program and Program Manager.

15.3.5. Minot AFB OPSEC PM. Serve as the 5 BW commander's representative regarding OPSEC requirements and the point of contact for all Minot AFB OPSEC-related issues between the installation and AFGSC/OPSEC PM and the organization's subordinate units from both wings and tenant organizations.

15.3.5.1. Chairs the Minot AFB OPSEC WG. Primary OPSEC WG representative to the Minot AFB ISAG (Minot AFB OPSEC executive council).

15.3.5.2. Maintains and manages Minot AFB OPSEC budget and program expenditures.

15.3.5.3. Leads, plans and conducts OPSEC assessments, visits and inspections for all Minot AFB organizations and agencies. Performs as the lead OPSEC representative to the 5 BW and 91 MW IGs for integration into the CCIP process.

15.3.5.4. Oversees the OPSEC chapter of the Minot AFBI 16-1401, OPSEC Implementation Plan and Base Profile.

15.3.5.5. Authors the Minot AFB Annual OPSEC Report.

15.3.5.6. Submits candidates for the AF OPSEC Course, other OPSEC-related training courses and related events.

15.3.5.7. Establish, maintain, review and confirm at least annually, the currency of the Minot AFB CIIL.

15.3.5.8. Annually, review and assess the effectiveness and efficiency of OPSEC within all organizations and agencies in the 5 BW, 91 MW and tenant organizations.

15.3.5.9. Conduct Staff Assistance Visits as requested by subordinate units (5 BW, 91 MW and tenant organizations) for OPSEC program management, planning and assistance in operationalizing OPSEC.

15.3.6. Unit OPSEC Coordinators will:

15.3.6.1. Fulfill duties as referenced in AFI 10-701, Para 2.24.

15.3.6.2. Complete the required OPSEC training outlined in Chapter 4 of AFI 10-701 and training locally directed by the OPSEC PM and 5 BW/IP.

15.3.6.3. Conduct OPSEC reviews of organizational documents and photographs in coordination with 5 BW Public Affairs prior to public release, as required.

15.3.6.4. Assist in reviewing unit-related contracting documents to ensure unit CIIL information and indicators are not publically available in solicitations and other contract documents; complete the OPSEC sections of the 5 CONS "Coordination Requirements for Contracts/Purchase Orders" checklist, as required (more details provided in **paragraph 15.5** below).

15.3.7. 5th Contracting Squadron will achieve requirements as referenced in AFI 10-701, Para 2.25. Will ensure squadron personnel complete the AFI 10-701, OPSEC training requirements for contracting.

15.4. OPSEC Working Group.

15.4.1. Concept of Operations: The OPSEC WG is responsible for assisting the ISAG in the implementation of the installation's OPSEC Program. The OPSEC PM will chair the OPSEC WG and report directly to the ISAG who reports to the Commander.

15.4.2. This group also oversees the implementation of the OPSEC Program, develops and refines OPSEC plans and addresses emergent or emergency OPSEC program issues.

15.4.3. The OPSEC WG will ensure the timely and efficient review of activities and future plans.

15.4.4. The OPSEC WG will integrate OPSEC into all organization planning and operational processes through unit OPSEC coordinators and unit planners.

15.4.5. The OPSEC WG composition will vary, depending on various projects or activities being performed. All members of the OPSEC WG will, as a minimum, possess a secret clearance.

Table 15.1. OPSEC WG Members.

5 BW/OPSEC Program Managers	5 BW/CCT
91 MW/OPSEC Program Managers	5 CS/SCXSI (Cyber Office)
5 OSS/IN	AFOSI-DET 813
91 OSS/IN	5 SFS/AT
5 BW/PA	91 SFG/AT
5 BW/JA	Select OPSEC Coordinators
5 BW/SE	
NOTE: At a minimum, the OWG should include a representative from each exercise or operation, as well as any direct units associated with an exercise or operation.	

15.4.6. The OPSEC WG recommends COAs to the ISAG; develops OPSEC-related policy, TTPs and guidance; clarifies OPSEC roles and responsibilities; conducts long-range planning and recommends resourcing requirements; and addresses emergent or emergency requirements OPSEC funding channels.

15.4.7. The OPSEC WG works in concert with the ISAG and other security/protection-oriented bodies to review security policies for protection of critical information, operations, resources, assets and personnel. It will ensure the timely and efficient examination of the planning, preparation, execution and post execution phases of any activity across the entire spectrum of Installation actions and operational environments to include on and off-base (missile complex).

15.4.8. The OPSEC WG will integrate OPSEC into all organization planning and operational processes.

15.4.9. The OPSEC WG standards, guidance and procedures shall be executed pursuant to AFI 10-701, Operations Security.

15.4.10. The OPSEC WG will use the formal OPSEC process as an integral process of force protection to help protect service members, civilian employees, family members, facilities, and equipment at all locations and in by denying targeted information to terrorists and other adversaries. Since force protection safeguards an organization’s most precious asset (i.e. people), it is critical that OPSEC be applied throughout all organizations.

15.5. OPSEC Education and Training. All Minot AFB personnel (military, Department of the Air Force Civilians and DoD Contractors) are required to complete the DAF OPSEC Awareness Training annually through MyLearning. Additional local focus OPSEC training is present through the SECENT training.

15.5.1. Minot AFB Unit OPSEC Coordinators. Unit OPSEC Coordinators will complete initial and refresher training IAW AFI 10-701 and also IAW local training requirements identified in this instruction and as illustrated on the 5 BW/IP USM Training Course Tracker. Training for OPSEC coordinators includes, but is not limited to, the OPSEC Fundamentals Course-OPSE 1301, OPSEC Contract Requirements-CLC-107 Course, Air Force Identity Management Course (CRS: J3O P-US1322) and other curriculum and courses.

15.6. Evaluating/Inspecting OPSEC. The Minot AFB OPSEC PM, as part of the Installation Security Enterprise Team and Wing Inspection Teams (5 BW and 91 MW) during CCIPs, will inspect every organization annually to verify OPSEC training, policies and procedures are in place to protect critical information and indicators.

15.6.1. All organizations and agencies will utilize the Security Enterprise Management Internal Control Toolset (MICT) checklist to conduct self-assess the OPSEC program IAW MICT rules in identified in DAFI 90-302.

15.6.2. Results from OPSEC-related inspections will be loaded into IGEMS and must be addressed and mitigated by the inspected organization.

15.7. OPSEC Requirements Within Contracting and Acquisitions. Organizations requesting contract support will determine and communicate the OPSEC measures required for each contract and ensure they are included in requests for proposal, statements of work, performance work statements, statement of operations, or other contract documents.

15.7.1. Document Reviews.

15.7.1.1. Minot AFB OPSEC Program Managers, in coordination with unit OPSEC Coordinators from the contract requirement owners, are responsible for the review of contract documents to ensure critical information and/or indicators are not made available to the public. An approved Minot AFB CIIL and/or unit CIIL will be used as a reference when conducting reviews.

15.7.1.1.1. The unit OPSEC Coordinator assigned to the unit with the contract requirement conducts the actual review of the contract documents and the Minot AFB OPSEC Program Manager provides technical guidance, if needed, and final approval.

15.7.1.1.2. If it is determined that a contract document contains critical information and/or indicators associated with the performance of the contract, the requesting organization’s OPSEC Coordinator will develop an OPSEC Plan to protect the critical information and/or indicators associated with the contract from cradle to grave if the critical information can’t be removed.

15.7.1.1.3. Both the unit OPSEC Coordinator assigned to the unit with the contract requirement and the Minot AFB OPSEC PM will coordinate on the OPSEC review on the 5 CONS “Coordination Requirements for Contracts/Purchase Orders” checklist.

15.7.2. Public Release of Information. The Minot AFB OPSEC PMs will work with unit coordinators when notified by 5 BW/PA of a need to conduct a review for public release of information. If there is a question on whether the information can be released due to FOIA exemptions, the OPSEC official reviewing the information will forward it to the INFOSEC office for further review.

DANIEL S. HOADLEY, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 5200.43, *Management of the Defense Security Enterprise,* 1 October 2012, Change 3 - 14 July 2020

DoDI 5200.1, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI),* 21 April 2016, Change 2 - 1 October 2020

DoDI 5200.02, *DoD Personnel Security Program (PSP),* 21 March 2014, Change 3 - 24 September 2020

DoDI 5200.8, *Security of DOD Installations and Resources and the DoD Physical Security Review Board (PSRB),* 10 December 2005, Change 3 - 20 November 2015

DoDI 5200.48, *Controlled Unclassified Information,* 6 March 2020

DoDI 8500.01, *Cybersecurity*, 14 March 2014 – Change 1 – 7 October 2019

DoDM 1000.13, Volume 1, *DoD Identification (ID) Cards: ID Card Life-Cycle,* 23 January 2014, Change 1 - 28 July 2020

DoDM 5200.01, Volume 1, *DOD Information Security Program: Overview, Classification, and Declassification*, 24 February 2012, Change 2 – 28 July 2020

DoDM 5200.01, Volume 2, *DoD Information Security Program: Marking of Information,* 24 February 2012, Change 3 - 14 May 2019

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information,* 24 February 2012, Change 3 – 28 July 2020

DoDM 5200.02, *Procedures for the DoD Personnel Security Program (PSP),* 3 April 2017

DoDM 5220.32, Volume 1, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* Change 2 - 10 December 2021

AFPD 10-7, *Information Operations,* 21 June 2021

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

AFPD 33-3, *Information Management,* 8 September 2011, Change 1 – 21 June 2016

AFPD 35-1, *Public Affairs Management,*23 December 2020

AFI 10-701, *Operations Security,* 24 July 2019, Change 1 – 9 June 2020

AFI 16-1401, *Information Protection,* 28 July 2019

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

AFI 16-1403, *Controlled Unclassified Information (CUI),* 5 October 2021

AFI 34-144, *Child and Youth Programs,* 2 July 2019

DAFI 90-302, *The Inspection System of the Department of the Air Force, 15 Mar 2023*

AFMAN 16-1404, Volume 1, *Information Security Program: Overview, Classification, and Declassification*, 6 April 2022

AFMAN 16-1404, Volume 2, *Information Security Program: Marking of Information*, 7 January 2021

AFMAN 16-1404, Volume 3, *Information Security Program: Protection of Classified Information,* 12 April 2022

AFMAN 16-1405, *Air Force Personnel Security Program,* 1 August 2018 – AFGM2022-01 – 8 Feb 2022

AFMAN 16-1406, Volume 2, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* 8 May 2020

Prescribed Forms

None

Adopted Forms

AF Form 2583, *Request for Personnel Security Action*

AF Form 2587, *Security Termination Statement*

AF Form 847, *Recommendation for Change of Publication*

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

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

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

Abbreviations and Acronyms

AAFES—Army Air Force Exchange Services

AFB—Air Force Base

AFMAN—Air Force Manual

AFNET—Air Force Network

AFOSI—Air Force Office of Special Investigations

AFI—Air Force Instruction

AFRIMS—AF Records Information Management System

AFSEC—AF Security Enterprise

SECENT—AF Security Enterprise Concepts

AFTO—Air Force Technical Order

AIS—Automated Information Systems

AO—Appointing Official

CAC—Common Access Card

CAS—Central Adjudications Services

CARL/NARL—Classified Authorization Receipt Listing and Nuclear Weapons Related Material (NWRM) Authorization Receipt Listing

CCIP—Commander's Inspection Program

CE—Continuous Evaluation

CFP—Communications Focal Point

C-InTP—Counter-Insider Threat Program

CI—Counterintelligence

CIK—Crypto Ignition Key

CIP—Chief, Information Protection

CMI—Classified Message Incident

CNWDI—Critical Nuclear Weapons Design Information

COMSEC—Communications Security

COMPUSEC—Computer Security

CP—Command Post

CPA—Classified Processing Area

CPF—Civilian Personnel Flight

CPO—Civilian Personnel Office

CSL—Cyber Security Liaison

CUI—Controlled Unclassified Information

CVS—Clearance Verification System

CYP—Child and Youth Program

DAA—Designated Approval Authority

DAPS—Defense Automation Printing Service

DCID—Director of Central Intelligence Directives

DEERS—Defense Enrollment Eligibility Reporting System

DISS—Defense Investigative Service System

DLP—Data Loss Prevention

DoE—Department of Energy

DoD—Department of Defense

DoDI—Department of Defense Instruction

DSS—Defense Security Service

EAL—Entry Authority List

EFB—Electronic Flight Bag

EO—Executive Order

e-QIP—Electronic Questionnaires for Investigations Processing

FOIA—Freedom of Information Act

FRC—Family Readiness Center

FRD—Formerly Restricted Data

HHQ—Higher Headquarters

HR—Human Resource

IAW—In Accordance With

IC—Intelligence Community

ICD—Intelligence Community Directives

ID—Identification

ID/ATEC—Integrated Defense/Antiterrorism Executive Committee

ID/ATWG—Integrated Defense/Antiterrorism Working Group

IFC—Intelligence Fusion Cell

IG—Inspector General

IGEMS—Inspector General Enterprise Management System

INDUSEC—Industrial Security

INFOSEC—Information Security

INPM—Installation NC2-ESI Program Manager

InTWG—Insider Threat Working Group

IO—Inquiry/Investigating Official

IP—Information Protection

IPOC—Installation Point of Contact

IS—Information System

ISAG—Installation SECENT Group

ISOO—Information Security Oversight Office

JA—Legal Office

KCCC—Keys and Codes Control Center

KMO—Key Management Officials

NTK—need-to-know

LAN—Local Area Network

LO5—Classified Receiver Listing

MINOT AFB—Minot Air Force Base

MAJCOM—Major Command

MICT—Management Information Communicator Toolkit

MFD—Multi-Function Device

MSC—Missile Security Control

NACI—National Agency Check with Written Inquires

NACLC—National Agency Check, Local Agency Check and Credit Check

NAF—Nonappropriated Funds

NATO—North Atlantic Treaty Organization

NBIB—National Background Investigations Bureau

NBIS—National; Background Investigation Services

NC2—Nuclear Command and Control

NCC—Network Control Center

NdA—Non-disclosure Agreement

NIPERNet—Non-secure Internet Protocol Router Network

NLT—Not Later Than

NPM—NC2 Program Manager

NSA—National Security Agency

NWRM—Nuclear Weapons Related Material

OCA—Original Classification Authority

OD—Open Discussion

OI—Operating Instruction

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

OPSEC—Operations Security

OPSEC PM—Operations Security Program Manager

OS—Open Storage

PED—Portable Electronic Devices

PERSEC—Personnel Security

PD—Performance Document

PDA—Personal Data Assistants

PII—Key Infrastructure

PKI—Key Infrastructure

POV—Personally Owned Vehicle

PRAP—Personnel Reliability Assurance Program

PSI—Personnel Security Investigations

PSM—Program Security Manager

PSM—Net—Personnel Security Management Network

PWS—Performance Work Statement

RAPIDS—Real-time Automated Personnel Identification System

RD—Restricted Data

RDS—Records Disposition Schedule

RP—Resource Protection

SA—Self-assessment

SAO—Senior Agency Official

SAR—Security Access Requirement

SAP—Special Access Program

SCI—Sensitive Compartmented Information

SCG—Security Classification Guide

SIPRNet—Secret Internet Protocol Router Network

SIP—Special Information Program

SME—Subject Matter Expert

SOI—Security Office Identifier

SON—Security Office Number

SOW—Statement of Work

SPAN—Sharing Peripherals Across the Network

STIG—Security Technical Installation Guide

SF—Security Forces

SSAN—Social Security Account Number

SSO—Special Security Officer

TA—Trusted Associate

TASM—TASS Security Manager

TASS—Trusted Associate Sponsorship System

TDY—Temporary Duty

TS—Top Secret

TSCA—Top Secret Control Assistant

TSCO—Top Secret Control Officer

TSCP—Top Secret Control Program

UCNI—Unclassified Controlled Nuclear Information

UMD—Unit Manning Document

US—United States

USM—Unit Security Manager (aka, Unit Security Assistant)

USAF—United States Air Force

VG—Visitor Group

VGSA—Visitor Group Security Agreement

WCO—Wing Cyber Security Office

WG—Working Group

WNPM—Wing NPM

WRB—Work-order Review Board

Terms

Access—The ability or opportunity to obtain knowledge of classified information.

Activity Head—See “heads of DoD activities.”

Activity Security Manager—The individual specifically designated in writing and responsible for a group or squadron's Security Enterprise program and performing duties as outlined in DoDM 5200.01, Volume 1 and Volume 3. This term is also called the unit security assistant in AFMAN 16-1404.

Authorized/Cleared Person—An individual with a favorable determination of eligibility for access to the specified level of classified information, with a signed a SF 312, and showing a valid need-to-know for the specific classified information in the performance of official duties.

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.

Classified Processing Area (CPA)—An area where classified information is processed using electronic devices, review of hardcopy information or through conversation. If computers are used, TEMPEST rules must also be considered. Rules are different between temporary CPAs and temporary TEMPEST areas, contact WCO for clarification.

Collateral Information—All national security information classified Confidential, Secret, or TS under the provisions of an E.O. for which special systems of compartmentation (such as SCI or SAP) are not formally required.

Compromise—An unauthorized disclosure of classified information.

Controlled Unclassified Information—Information which requires special handling or protection, but which is not classified. For example, PII, and UCNI are all types of CUI.

Critical Information—Specific facts (or evidence) about friendly intentions, capabilities, and activities needed by adversaries to plan and act effectively against friendly mission accomplishments.

Critical Information and Indicators List—That part of an OPSEC program or plan that conveys the organization or mission specific critical information and indicators to personnel as a reference of what information that must be protected via secure means or indicators that must be hidden from adversary collection methods.

Data Spillage—Classified information or CUI is transferred onto a 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.

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.

Essential Secrecy—The condition achieved from the denial of critical information and indicators to adversaries through the combined efforts of traditional security programs and the operations security process.

FRD—Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data.

Heads Of DoD Activities—Heads, either military or civilian, of organizations, commands, and staff elements subordinate to a DoD Component, with jurisdiction over and responsibility for the execution of the organization's mission and functions, including its information security program. The official may variously carry the title of commander, commanding officer, or director, or other equivalent title.

Indicator—In operations security usage, data derived from friendly detectable actions and open-source information that an adversary can interpret and piece together to reach conclusions or estimates of friendly intentions, capabilities, or activities.

Information Protection—Information Protection is a subset of the Air Force Security Enterprise consisting of the core security disciplines (Personnel, Industrial, and Information Security).

Information Security—The system of policies, procedures, and requirements established in accordance with Reference (d) to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures and requirements established to protect controlled unclassified information, which may be withheld from release to the public in accordance with statute, regulation, or policy.

Infraction—Any knowing, willful, or negligent action contrary to the requirements of Reference (d), its implementing directives, or this Manual that does not constitute a "violation," as defined herein.

Inquiry—The initial fact-finding and analysis process to determine the facts of any security incident.

Investigation—An in-depth, comprehensive examination of the facts associated with a security violation.

Loss—The inability to physically locate or account for classified information.

Need-To-Know—A determination prospective recipients require access to specific classified information in order to perform/assist in a lawful and authorized governmental function. Need-to-know for contractors is determined by the requirements outlined in DD Form 254.

Negligent Discharge of Classified Information—A spillage or unauthorized disclosure of classified information while using an information system.

Observation and Control of Classified—Is the requirement for an authorized/cleared individual to be able to see classified material **and** be able to physically prevent unauthorized access IAW AFMAN 16-1404 and DoDM 5200.01, Volume 3, Enclosure 2.

Open Storage Area—An area constructed in accordance with the requirements of the Appendix to Enclosure 3 of Volume 3 to DoDM 5200.01 and authorized for open storage of classified information.

Operations Security—A capability that uses a process to preserve friendly essential secrecy by identifying, controlling and protecting critical information and indicators that would allow adversaries or potential adversaries to identify and exploit friendly vulnerabilities.

OPSEC Coordinator—An individual trained in OPSEC located at a subordinate level, who works in coordination with the OPSEC program manager or primary representative.

OPSEC Program Manager—A full-time appointee or primary representative assigned to develop and manage an OPSEC program.

OPSEC Review—Methods to determine an organizations compliance with established OPSEC standards or measures of performance. Inspector General Inspections, or higher headquarters reviews that specifically address OPSEC are considered OPSEC Reviews.

OPSEC Working Group—Designated body representing a broad range of line and staff activities within an organization that provides advice and support to leadership and all elements of the organization. This can be an OPSEC, USM, threat, or public affairs working group that addresses OPSEC concerns).

Original Classification—Initial determination information requires, in the interests of national security, protection against unauthorized disclosure.

Portable Electronic Devices—As defined in paragraph 1.2 of the OSD policy memo, U.S. Government Portable Electronic Devices (PEDs) with classified capability (e.g. DoD Mobile Classified Capability and SecureView) offer a unique ability to support the Department of the Air Force mission.

PII—Unique information about an individual that can be used to distinguish or trace his or her identity. It includes, but is not limited to, name, social security number, date and place of birth, mother's maiden name, home address and phone number, personal e-mail address, biometric records, financial transactions, medical history, criminal or employment history, and other information to which a security manager may have access. PII does not include an individual’s name when it is associated with work elements, such as duty phone number, duty address, and

U.S. Government e—mail address.

Practices Dangerous to Security—Incidents which are not reportable as security incidents, but have the potential to jeopardize the security of classified information and material if allowed to perpetuate. These practices, when identified, must be promptly addressed by security management and appropriate changes made, actions taken, or training provided, to ensure the security of classified information.

RD—All data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but not data declassified or removed from the Restricted Data category pursuant to section 2162 of

The Atomic Energy Act of 1954, as amended (Reference (cj)).

Safeguarding—Measures and controls that are prescribed to protect classified information.

Self-Inspection—The internal review and evaluation of activities with respect to the implementation of the program established in accordance with DoDM 5200.01, Volume 1-Volume 3 or other referenced guidance. This is accomplished locally through use of MICT and CCIP events.

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. Oversight of installation level duties requiring SAO action are delegated to the installation commander in AFMAN 16-1404, 1.3..3.

Security-in-Depth—Determinations 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. Determinations outside the ones discussed above are made locally for storage of TS, Secret, and Confidential information.

Unclassified-—Information not requiring control, but requiring review before public release.

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.

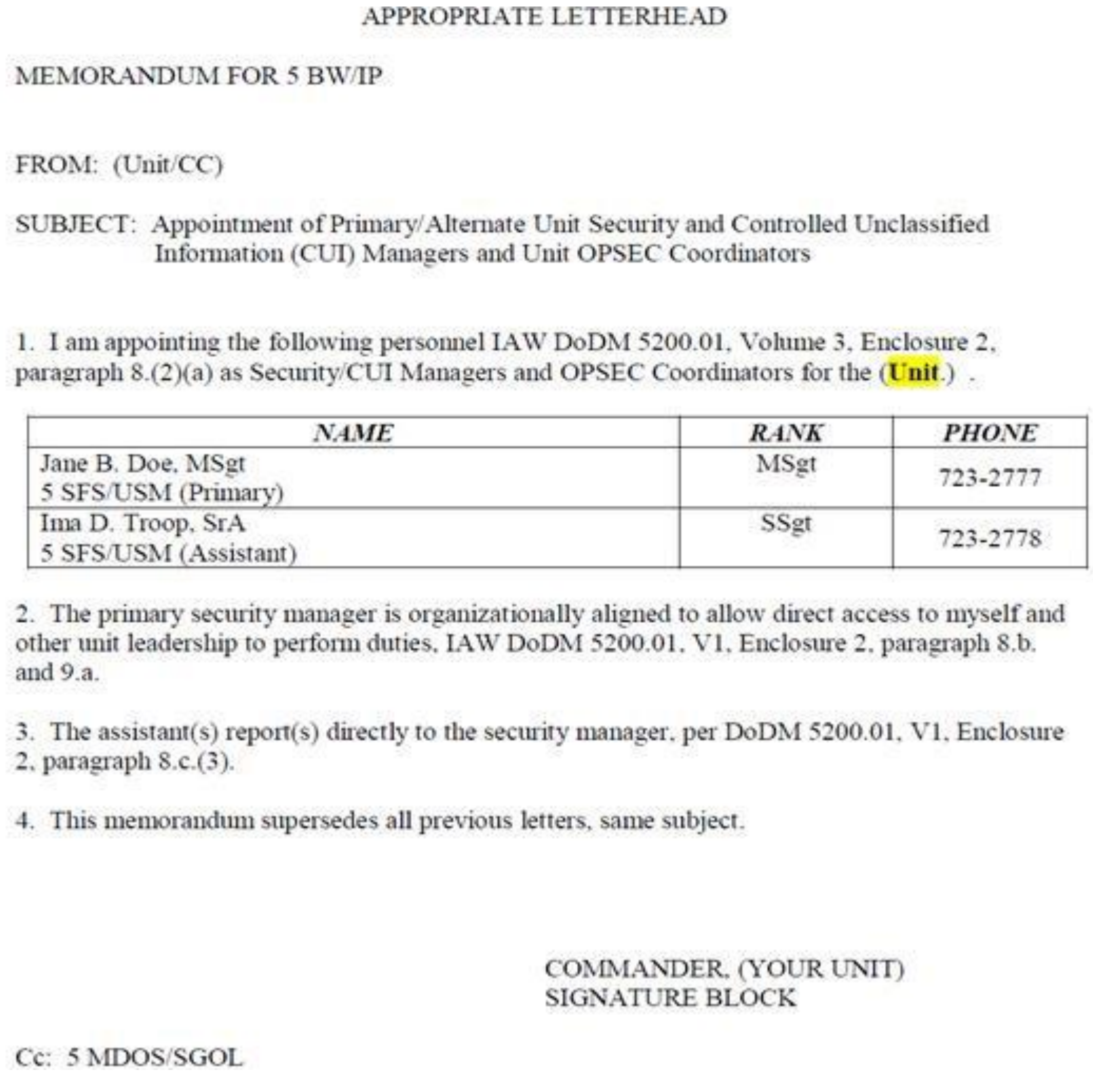
Vault—An area designed and constructed IAW DoDM 5200.01, Volume 3 to provide protection against forced entry and which is equipped with a GSA-approved vault door and lock. The term may also be applied to a modular vault approved by the GSA.

Violation—Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information or which meets criteria established in DoDM 5200.01, Volume 3.

Attachment 2

SAMPLE MEMORANDUM FOR APPOINTMENT OF SECURITY MANAGER

Figure A2.1. Sample Memorandum for Appointment of Security Manager.



APPROPRIATE LETTERHEAD

MEMORANDUM FOR 5 BW/IP

FROM: (Unit/CC)

SUBJECT: Appointment of Primary/Alternate Unit Security and Controlled Unclassified Information (CUI) Managers and Unit OPSEC Coordinators

1. I am appointing the following personnel IAW DoDM 5200.01, Volume 3, Enclosure 2, paragraph 8.(2)(a) as Security/CUI Managers and OPSEC Coordinators for the (**Unit**.) .

NAME	*RANK*	*PHONE*
Jane B. Doe, MSgt 5 SFS/USM (Primary)	MSgt	723-2777
Ima D. Troop, SrA 5 SFS/USM (Assistant)	SSgt	723-2778

2. The primary security manager is organizationally aligned to allow direct access to myself and other unit leadership to perform duties, IAW DoDM 5200.01, V1, Enclosure 2, paragraph 8.b. and 9.a.

3. The assistant(s) report(s) directly to the security manager, per DoDM 5200.01, V1, Enclosure 2, paragraph 8.c.(3).

4. This memorandum supersedes all previous letters, same subject.

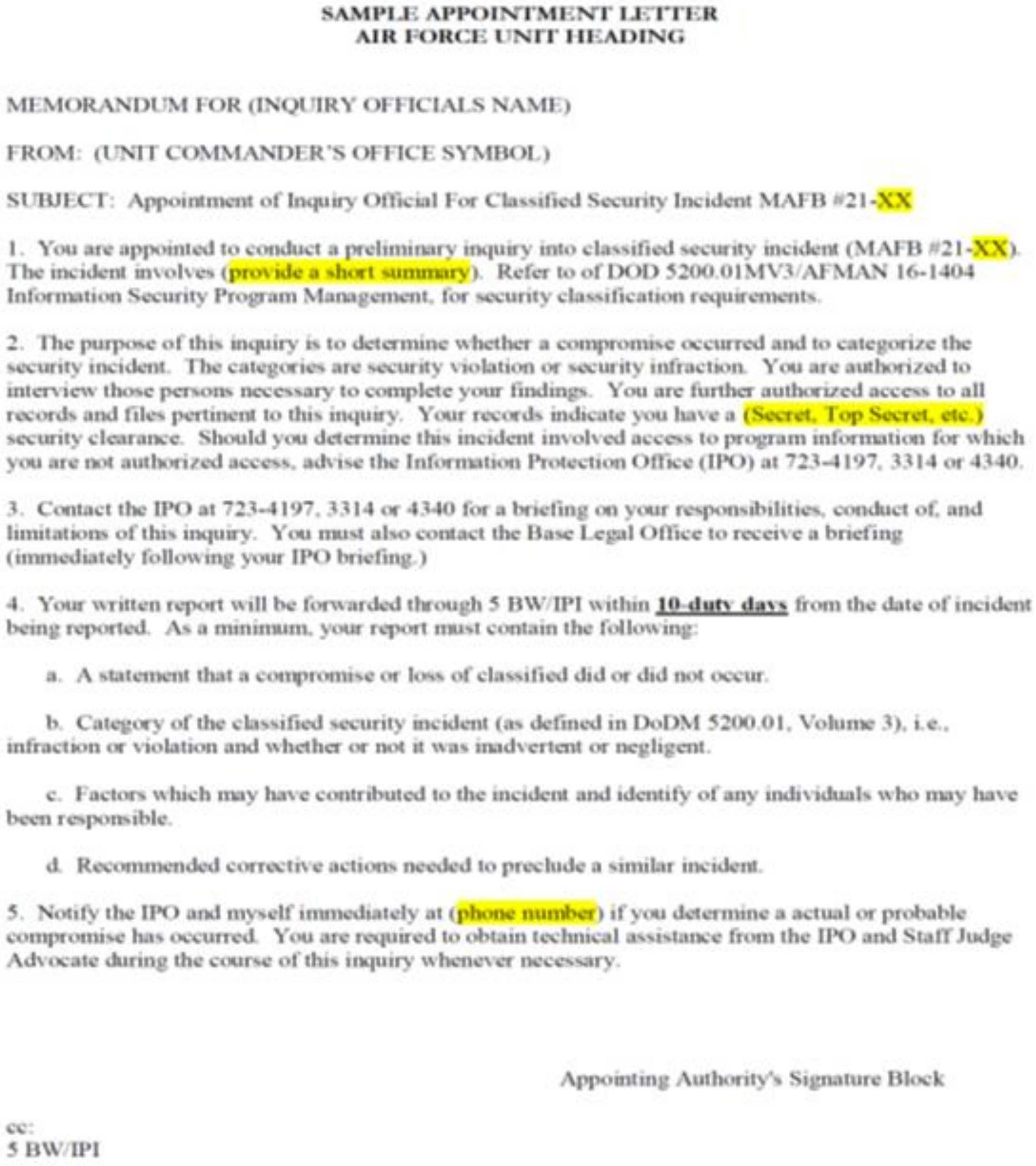
COMMANDER, (YOUR UNIT)
SIGNATURE BLOCK

Cc: 5 MDOS/SGOL

Attachment 3

SAMPLE APPOINTMENT LETTER

Figure A3.1. Sample Appointment Letter.



SAMPLE APPOINTMENT LETTER
AIR FORCE UNIT HEADING

MEMORANDUM FOR (INQUIRY OFFICIALS NAME)

FROM: (UNIT COMMANDER'S OFFICE SYMBOL)

SUBJECT: Appointment of Inquiry Official For Classified Security Incident MAFB #21-XX

1. You are appointed to conduct a preliminary inquiry into classified security incident (MAFB #21-XX). The incident involves (provide a short summary). Refer to of DOD 5200.01MV3/AFMAN 16-1404 Information Security Program Management, for security classification requirements.

2. The purpose of this inquiry is to determine whether a compromise occurred and to categorize the security incident. The categories are security violation or security infraction. You are authorized to interview those persons necessary to complete your findings. You are further authorized access to all records and files pertinent to this inquiry. Your records indicate you have a (Secret, Top Secret, etc.) security clearance. Should you determine this incident involved access to program information for which you are not authorized access, advise the Information Protection Office (IPO) at 723-4197, 3314 or 4340.

3. Contact the IPO at 723-4197, 3314 or 4340 for a briefing on your responsibilities, conduct of, and limitations of this inquiry. You must also contact the Base Legal Office to receive a briefing (immediately following your IPO briefing.)

4. Your written report will be forwarded through 5 BW/IPI within **10-duty days** from the date of incident being reported. As a minimum, your report must contain the following:

a. A statement that a compromise or loss of classified did or did not occur.

b. Category of the classified security incident (as defined in DoDM 5200.01, Volume 3), i.e., infraction or violation and whether or not it was inadvertent or negligent.

c. Factors which may have contributed to the incident and identify of any individuals who may have been responsible.

d. Recommended corrective actions needed to preclude a similar incident.

5. Notify the IPO and myself immediately at (phone number) if you determine a actual or probable compromise has occurred. You are required to obtain technical assistance from the IPO and Staff Judge Advocate during the course of this inquiry whenever necessary.

Appointing Authority's Signature Block

cc:
5 BW/IPI

Attachment 4

CHECKLIST FOR USE OF COPIERS/SCANNERS WITH SENSITIVE INFORMATION

Table A4.1. All Purpose Checklist.

<table>
<tr><td colspan="2"><b>ALL PURPOSE CHECKLIST</b></td><td colspan="4"><b>PAGE 1 OF 2 PAGES</b></td></tr>
<tr><td colspan="2"><b>TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA
Unit Purchase/Use of Classified Copiers or Scanners references are to DOD 5200M.01/AFI 16-1404/AFGSC supplement 1.</b></td><td><b>OPR
5 BW/IP</b></td><td colspan="3"><b>DATE</b></td></tr>
<tr><td><b>NO</b></td><td colspan="2"><b>ITEM</b></td><td><b>YES</b></td><td><b>NO</b></td><td><b>N/A</b></td></tr>
<tr><td>1</td><td colspan="2">The following checklist was developed by the 5 BW/IP and approved by Wing Cyber Security Office using the noted references. You must contact your USM to ensure all requirements for your classified copier or scanner are properly addressed in your unit's local procedures.</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td colspan="2">Are classified copiers/printers/scanners clearly identified, to include:
a. Having a copy of the commander's designation/approval letter which includes the device manufacturer and model, posted near the device? [REF: DoDM 5200.01, Volume 3, E2, 15—inclusive.]
b. Has the equipment received TEMPEST approval from the WCO, and been coordinated through the Unit CSL, to include number of blanks needed to clear latent images? [REF: DoDM 5200.01, Volume 3, E2, 14—inclusive.]
c. Have procedures been developed and posted near the device which address copying, clearing, control, individual security responsibilities and who is authorized to reproduce classified material [e.g., CC policy letter or in unit OI)? [REF: DoDM 5200.01, Volume 3, E2, 14.b.]
d. Is a "Cleared for Classified" sign and equipment marked with SF 706, SF 707, SF 708, SF 710, as applicable, posted at the device? [REF: DoDM 5200.01, Volume 3, E2, 15.b(7).]
e. IF the device is connected/part of an Information Technology (IT) system (i.e. a networked e-device), is the equipment marked with the SF 706, SF 707, SF 708, SF 710 as applicable? [REF: DoD 5200.1M Vol 2, Enclosure 3, 18. g(1).]</td><td></td><td></td><td></td></tr>
<tr><td>3</td><td colspan="2">Do classified devices:
a. Meet volatile memory requirements? [REF: DoDM 5200.01, Volume 3, E2, 14—inclusive.]
b. Has equipment received Certification and Accreditation (C & A) if connected to a network? [REF: DoDM 5200.01, Volume 3, E2, 14.e.]</td><td></td><td></td><td></td></tr>
</table>

Table A4.2. All Purpose Checklist.

ALL PURPOSE CHECKLIST		**PAGE 2 OF 2 PAGES**		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA **Unit Purchase/Use of Classified Copiers or Scanners references are to DOD 5200M.01**	**OPR** **5 BW/IP**	**DATE**		
NO	**ITEM**	**YES**	**NO**	**N/A**
	COPIER/SCANNER RULES FOR TS MATERIAL			
4	Units possessing TS <u>must have</u> a TS Control Program (TSCA) and a designated TS Control Officer (TSCO.) The TSCO must authorize and log any TS copies a unit produces. Specific TSCA and TSCO requirements may be obtained from the unit security manager. The following items are taken from the locally produced TSCO checklist. [REF: AFGSC, GM to AFMAN 16-1404			
5	TS CONTROL- Is the proper annotation made on the AF Form 143, TS Register Page when copies of TS information are made? [REF: AFGSC, GM to AFMAN 16-1404, 5.4.1.2.]			
6	TS CONTROL- Does the AF Form 143 reflect the following: [REF: AFGSC, GM to AFMAN 16-1404, 5.4.1.1. through 5.4.1.3 (inclusive).] a. Sufficient information to adequately identify the TS document or material; to include title or appropriate short title, date of the document, and the originator's identity? b. The date the document or material was received? c. The number of copies received and/or later reproduced? d. The disposition of the TS document or material and all copies of such documents or material? e. Are register pages with active entries recontrolled on an annual basis? (AF Form 143.]			
7	TS CONTROL- Is an AF Form 144, *Top Secret Access Record* and Cover Sheet, attached to each copy of the TS document? [REF: AFGSC, Sup 1 to AFGSC, GM to AFMAN 16-1404, 5.4.1.4.]			
8	TS CONTROL-Are TS facsimiles processed as another copy of the main TS document in the TSCA? [AFGSC, GM to AFMAN 16-1404, 5.4.1.3.1.]			

Attachment 5

CHECKLIST FOR CLASSIFIED MESSAGE INCIDENTS (CMI)/ NEGLIGENT DISCHARGE CLASSIFIED INFORMATION (NDCI)

Table A5.1. Checklist for Classified Message Incidents (CMI)/ Negligent Discharge Classified Information (NDCI).

ALL PURPOSE CHECKLIST		**PAGE 1 OF 3 PAGES**		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA POTENTIAL CMI/DATA SPILLAGE References: DODM 5200.01/AFGSC GM to AFMAN 16-1404.		**OPR: 5 BW/IP**	**DATE**	
NO.	**ITEM**	**YES**	**NO**	**N/A**
	SECTION 1 – INITIAL ACTIONS			
1	When the USM/CSL is notified of a potential CMI or NDCI they will ensure: a. The individual reporting is aware that any specific information on the incident is classified until the systems are sanitized. [REF: Minot AFBI 16-1401, Chapter 6.] b. If the USM receives the notification they will ensure the unit CSL is notified. If the CSL receives they will ensure the USM is notified. [REF: Minot AFBI 16-1401, Chapter 6.] c. The USM/CSL will verify the classification of the information against an approved security classification guide (SCG) or a properly classified source. (1) The USM will contact 5 BW/IP if there is any doubt on the classification of the material. [REF: Minot AFBI 16-1401, Chapter 6.) d. The USM/CSL will notify CFP in person or via secure telephone (723-1241) of the incident. The CFP will need specific information on the incident which is classified until sanitization is complete. Be prepared to provide the following information USING A SECURE SYSTEM: [REF: DoDM 5200.01, Volume 3, E6, 3.a. and Minot AFBI 16-1401, Chapter 6.] (1) Names of users that received Email or location of classified. (2) Systems affected (3) Specific time, date, subject line and attachment name for the message. (4) Location of affected systems (5) Verification of security for affected systems (i.e., under positive control of cleared personnel OR in an approved storage container/area). e. The CFP will ensure the WCO is notified as soon as possible (preferably immediately, but within 24 hours). [REF: AFMAN 17-1301, 4.5. and Minot AFBI 16-1401, Chapter 6.]			

Table A5.2. Checklist For Classified Message Incidents (CMI)/ Negligent Discharge Classified Information (NDCI).

ALL PURPOSE CHECKLIST		**PAGE 2 OF 3 PAGES**		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA POTENTIAL CMI/DATA SPILLAGE References: DODM 5200.01/AFGSC GM to AFMAN 16-1404.		**OPR: 5 BW/IP**	**DATE**	
NO	**ITEM**	**YES**	**NO**	**N/A**
	SECTION 1 – INITIAL ACTIONS (continued)			
2	The USM will ensure the Wing Information Protection (IP) Office is notified NLT the next duty day and also: [REF: DoDM Volume 3, E6, 3.a. and Minot AFBI 16-1401, Chapter 6.] a. Ensure the systems are protected as classified until a determination is made. Secure in an approved security container, vault or ensure computer is placed under guard by appropriately cleared personnel. b. Ensure a copy of the message in question is printed and maintained for review. DO NOT print classified data using an unapproved printer, instead save data in question to a properly marked CD and transfer to an appropriate network for printing.			
	SECTION 2 – FOLLOW ON ACTIONS			
1	The CFP will lock out all TIER-2 and below accounts once classification is verified. [REF: Minot AFBI 16-1401, Chapter 6.]			
2	The CFP will wait to initiate sanitization actions until the WCO and/or 5 BW/IP Office have validated the information is classified against the SCG or a valid classified source and briefed the owning unit commander. [REF: Minot AFBI 16-1401, Chapter 6.]			
3	If the information is validated (using an SCG or valid source) as classified: a. The WCO and 5 BW/IP Office will make a recommendation to the Minot AFB Declaration Authority (5 CS/CC) on whether sanitization is required. [REF: Minot AFBI 16-1401, Chapter 6.] b. The CFP will initiate an incident report. c. If a data spill has occurred, the USM will make formal notifications to the original classification authority (OCA) once the classification has been determined. [REF: DODM 5200.01, Volume 3, E7.5.e.] d. If there is a question on the classification of the material, the USM will contact the OCA's POC to obtain the needed clarification. [REF: DoDM 5200.01, Volume 3, E6, 10.a.(3).]			

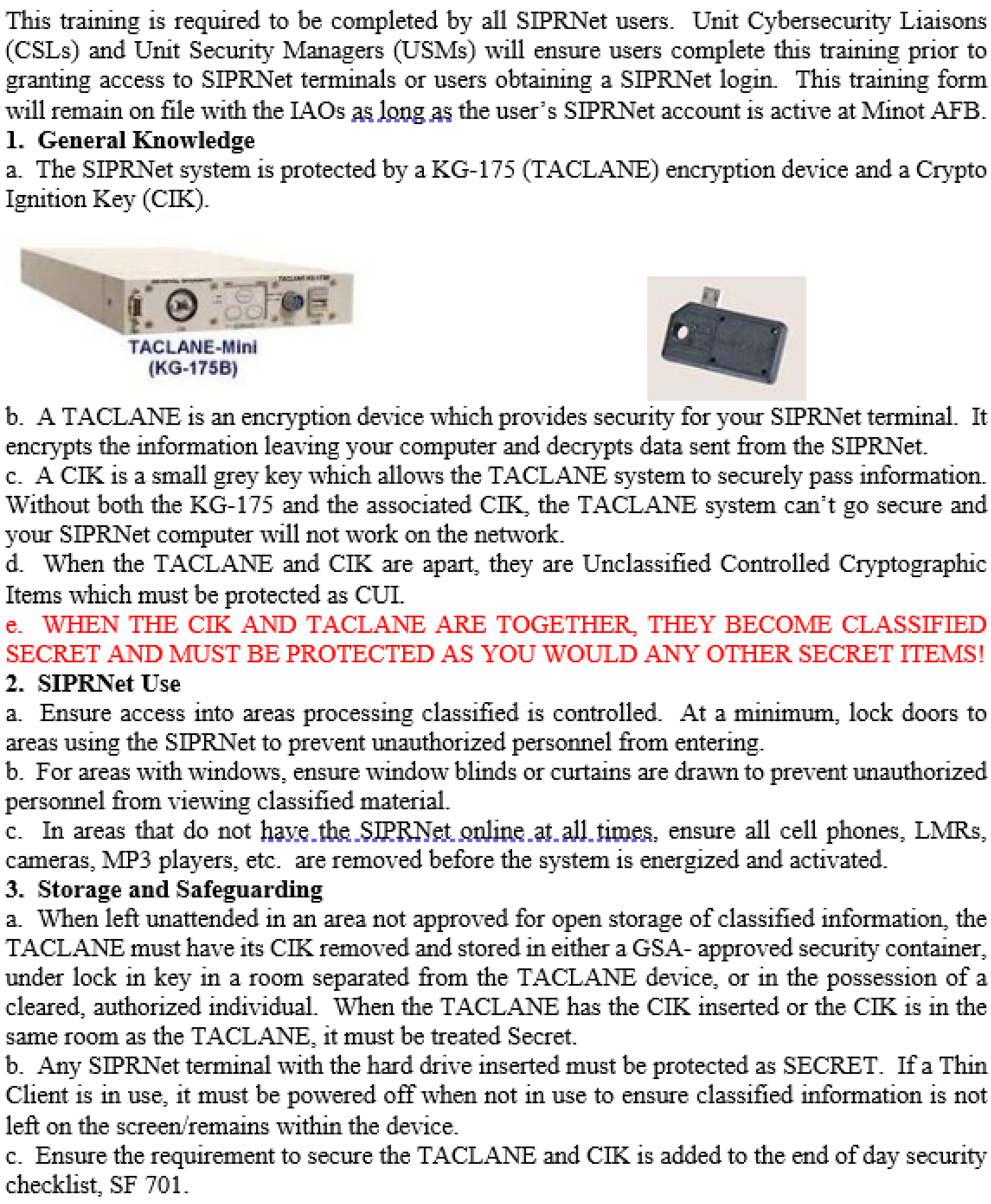
Table A5.3. Checklist For Classified Message Incidents (CMI)/ Negligent Discharge Classified Information (NDCI).

ALL PURPOSE CHECKLIST		**PAGE 3 OF 3 PAGES**		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA POTENTIAL CMI/DATA SPILLAGE References: DODM 5200.01/AFMAN 16-1404/AFGSC supplement 1.		**OPR: 5 BW/IP**	**DATE**	
NO	**ITEM**	**YES**	**NO**	**N/A**
	SECTION 3 – SANITIZATION ACTIONS			
1	The CFP will track sanitization of systems. [REF: Minot AFBI 16-1401, Chapter 6.]			
2	The USM/CSL will ensure all affected systems are protected at the level of classification of the message until the CFP receives verification the system is sanitized.			
3	The CSL will ensure the individual causing the security incident re-accomplishes IA training. [REF: 24 AF/NOTAM.] a. The first O-6 in the individual's chain must submit the training certificate to the CFP before the account can be unlocked. b. If the individual causing the security incident is an O-6 or above, the 5 BW/CC must submit the training certificate to the 24 AF/CC for the account to be unlocked.			

Attachment 6

SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) USER TRAINING

Figure A6.1. SIPRNET User Training.



This training is required to be completed by all SIPRNet users. Unit Cybersecurity Liaisons (CSLs) and Unit Security Managers (USMs) will ensure users complete this training prior to granting access to SIPRNet terminals or users obtaining a SIPRNet login. This training form will remain on file with the IAOs as long as the user's SIPRNet account is active at Minot AFB.

1. General Knowledge

a. The SIPRNet system is protected by a KG-175 (TACLANE) encryption device and a Crypto Ignition Key (CIK).

TACLANE-Mini
(KG-175B)

b. A TACLANE is an encryption device which provides security for your SIPRNet terminal. It encrypts the information leaving your computer and decrypts data sent from the SIPRNet.

c. A CIK is a small grey key which allows the TACLANE system to securely pass information. Without both the KG-175 and the associated CIK, the TACLANE system can't go secure and your SIPRNet computer will not work on the network.

d. When the TACLANE and CIK are apart, they are Unclassified Controlled Cryptographic Items which must be protected as CUI.

e. WHEN THE CIK AND TACLANE ARE TOGETHER, THEY BECOME CLASSIFIED SECRET AND MUST BE PROTECTED AS YOU WOULD ANY OTHER SECRET ITEMS!

2. SIPRNet Use

a. Ensure access into areas processing classified is controlled. At a minimum, lock doors to areas using the SIPRNet to prevent unauthorized personnel from entering.

b. For areas with windows, ensure window blinds or curtains are drawn to prevent unauthorized personnel from viewing classified material.

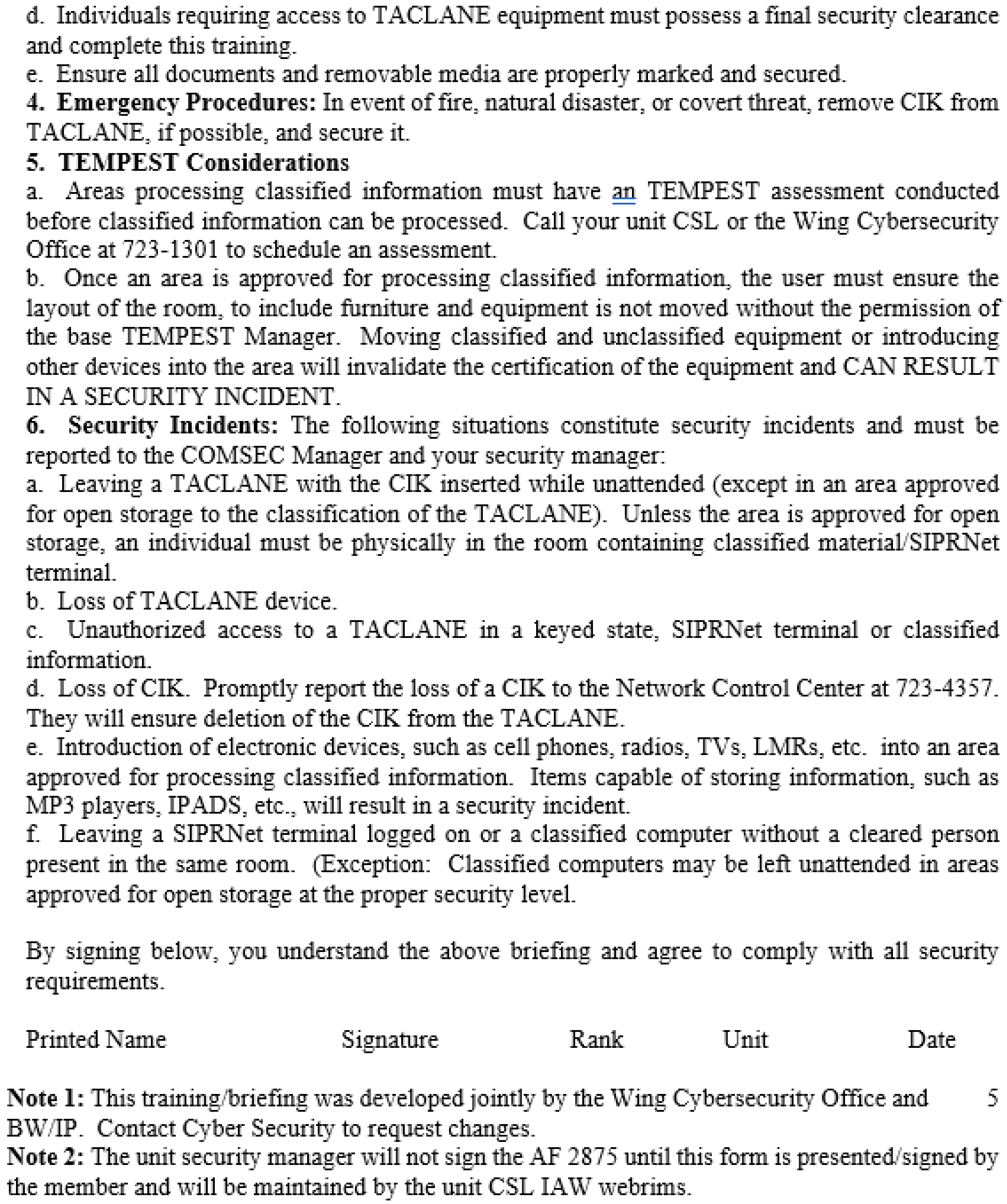
c. In areas that do not have the SIPRNet online at all times, ensure all cell phones, LMRs, cameras, MP3 players, etc. are removed before the system is energized and activated.

3. Storage and Safeguarding

a. When left unattended in an area not approved for open storage of classified information, the TACLANE must have its CIK removed and stored in either a GSA- approved security container, under lock in key in a room separated from the TACLANE device, or in the possession of a cleared, authorized individual. When the TACLANE has the CIK inserted or the CIK is in the same room as the TACLANE, it must be treated Secret.

b. Any SIPRNet terminal with the hard drive inserted must be protected as SECRET. If a Thin Client is in use, it must be powered off when not in use to ensure classified information is not left on the screen/remains within the device.

c. Ensure the requirement to secure the TACLANE and CIK is added to the end of day security checklist, SF 701.



d. Individuals requiring access to TACLANE equipment must possess a final security clearance and complete this training.
e. Ensure all documents and removable media are properly marked and secured.
4. Emergency Procedures: In event of fire, natural disaster, or covert threat, remove CIK from TACLANE, if possible, and secure it.
5. TEMPEST Considerations
a. Areas processing classified information must have an TEMPEST assessment conducted before classified information can be processed. Call your unit CSL or the Wing Cybersecurity Office at 723-1301 to schedule an assessment.
b. Once an area is approved for processing classified information, the user must ensure the layout of the room, to include furniture and equipment is not moved without the permission of the base TEMPEST Manager. Moving classified and unclassified equipment or introducing other devices into the area will invalidate the certification of the equipment and CAN RESULT IN A SECURITY INCIDENT.
6. Security Incidents: The following situations constitute security incidents and must be reported to the COMSEC Manager and your security manager:
a. Leaving a TACLANE with the CIK inserted while unattended (except in an area approved for open storage to the classification of the TACLANE). Unless the area is approved for open storage, an individual must be physically in the room containing classified material/SIPRNet terminal.
b. Loss of TACLANE device.
c. Unauthorized access to a TACLANE in a keyed state, SIPRNet terminal or classified information.
d. Loss of CIK. Promptly report the loss of a CIK to the Network Control Center at 723-4357. They will ensure deletion of the CIK from the TACLANE.
e. Introduction of electronic devices, such as cell phones, radios, TVs, LMRs, etc. into an area approved for processing classified information. Items capable of storing information, such as MP3 players, IPADS, etc., will result in a security incident.
f. Leaving a SIPRNet terminal logged on or a classified computer without a cleared person present in the same room. (Exception: Classified computers may be left unattended in areas approved for open storage at the proper security level.

By signing below, you understand the above briefing and agree to comply with all security requirements.

Printed Name Signature Rank Unit Date

Note 1: This training/briefing was developed jointly by the Wing Cybersecurity Office and 5 BW/IP. Contact Cyber Security to request changes.
Note 2: The unit security manager will not sign the AF 2875 until this form is presented/signed by the member and will be maintained by the unit CSL IAW webrims.

Attachment 7

CAC ISSUE FOR UNCLEARED PERSONNEL

Table A7.1. CAC Issue for Uncleared Personnel.

ALL PURPOSE CHECKLIST				**PAGE 2 OF 2 PAGES**		
TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA COMMON ACCESS CARD FOR UNCLEARED PERSONNEL References are to HSPD-12, DoDM 1000.13, Volume 1, DoDI 5200.46 and DoD 5200.02, unless otherwise indicated.				**OPR** **5 BW/IP**	**DATE** **01 Feb 21**	
Unit:		**Rank/Name:**		**Date:**		
NO.	**ITEM** **(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph)**			**YES**	**NO**	**N/A**
	Use this checklist to help determine whether a civilian/contractor employee requires a personnel security investigation (PSI) for cleared (classified)/uncleared access (e.g., computers, CUI, base access, etc.) NOTE: The 5 FSS USM conducts this check for all new NAF/CPO employees. The sponsoring USM conducts this check for uncleared contractors or periodic reviews (PR) of current GS/NAF employees. It does NOT apply to cleared contractors.					
1	Does the individual have a prior PSI? a. If yes, the unit security manager (USM) must verify whether there was a two year or greater break in service: (1) If 2-year break—go to item 2 below (2) If there was over a 2-year break—see item 3 below b. If no—see item 3 below.					
2	If the individual had a prior PSI, without a 2-year break, the USM uses the following guidelines to determine if the existing clearance is sufficient: a. If the position is Non-Sensitive (SAR code 8—no classified access) the member must have a TIER-1, TIER- 2, TIER-3/3R, TIER-4, SSBI or TIER-5. b. If the position is Non-Critical Sensitive (SAR Code 7—secret access) they must have a TIER-3/3R (conducted within last 10 years) or an SSBI or TIER-5 (conducted within last 10 years). EXCEPTION: If position is PRAP/SAP the investigation must be in last 5 years. c. If the position is Critical Sensitive (SAR Code5—TS access) the member must have an SSBI or TIER-5 (conducted within last 5 years).					

Table A7.2. CAC Issue for Uncleared Personnel.

ALL PURPOSE CHECKLIST	**PAGE 02 OF 02 PAGES**

TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA COMMON ACCESS CARD FOR UNCLEARED PERSONNEL References are to HSPD-12, DoDM 1000.13, Volume 1, DoDI 5200.46 and DoD 5200.02R, unless otherwise indicated.	**OPR** **5 BW/IP**	**DATE** **01 Feb 21**

Unit:		**Rank/Name:**		**Date:**	

NO.	**ITEM** **(Assign a paragraph number to each item. Draw a horizontal line between each major paragraph)**	**YES**	**NO**	**N/A**
	d. A NACLC (military secret) IS NOT usable for ANY type of GS/NAF access but may be used for uncleared contractor secret access. e. Does the existing PSI meet the current job requirement? (1) If YES, go to 4 below (2) If NO, go to 3 below			
3	If the individual has had no prior PSI, there was a two year or greater break in service OR if the current PSI does not meet the job sensitivity requirements then: a. The USM will need to initiate the needed PSI and have the member complete the e-QIP paperwork for the needed PSI. In the case of uncleared contractors—DO NOT sign off on the TASS form until the needed PSI is initiated. If there is a question on whether the current PSI is valid, the USM will contact the 5 BW/IPO to discuss needed actions.			
4	No further PSI action is required, the member's clearance meets requirements.			

Attachment 8

SPECIAL SECURITY AREA REVIEW CHECKLIST

Table A8.1. Special Security Area Review Checklist.

<table>
<tr><td colspan="5"><b>ALL PURPOSE CHECKLIST</b></td><td colspan="5"><b>PAGE 01 OF 01 PAGES</b></td></tr>
<tr><td colspan="5"><b>TITLE/SUBJECT/ACTIVITY/FUNCTIONAL AREA
SPECIAL SECURITY AREA REVIEW CHECKLIST</b></td><td><b>OPR 5 CES</b></td><td colspan="4"><b>DATE
01 Feb 21</b></td></tr>
<tr><td colspan="2"><b>Requesting Unit:</b></td><td></td><td><b>Rank &amp; Name of Requestor:</b></td><td colspan="3"></td><td><b>Date:</b></td><td colspan="2"></td></tr>
<tr><td><b>Item</b></td><td colspan="6"><b>Item description</b></td><td><b>YES</b></td><td><b>NO</b></td><td><b>N/A</b></td></tr>
<tr><td>1</td><td colspan="6">Does the area where the construction will be occurring currently, or is it projected to be, a:</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">a. processing area for classified information?</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">b. funds, weapons, ammunition or explosives storage area?</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">c. classified storage area?</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">d. an alarmed area using an intrusion detection system (IDS) or duress alarm?</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td colspan="6">Is the area proposed an area currently or projected to be:</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">a. an area where access is limited?</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="6">b. On the flight line or in a restricted area?</td><td></td><td></td><td></td></tr>
<tr><td colspan="10">I am the unit security manager for the______________________and I confirm the above statements are correct according to my unit leadership's stated plans for the area discussed in the work order.
Printed Name and Rank:____
Office Symbol:________________________
Signature:____</td></tr>
</table>

Attachment 9

AF FORM 2583 INTERIM ACCESS CHECKLIST

A9.1. The USM will ensure the following steps are accomplished for the AF Form 2583 when requesting interim access. Input the following data for the member on the form.

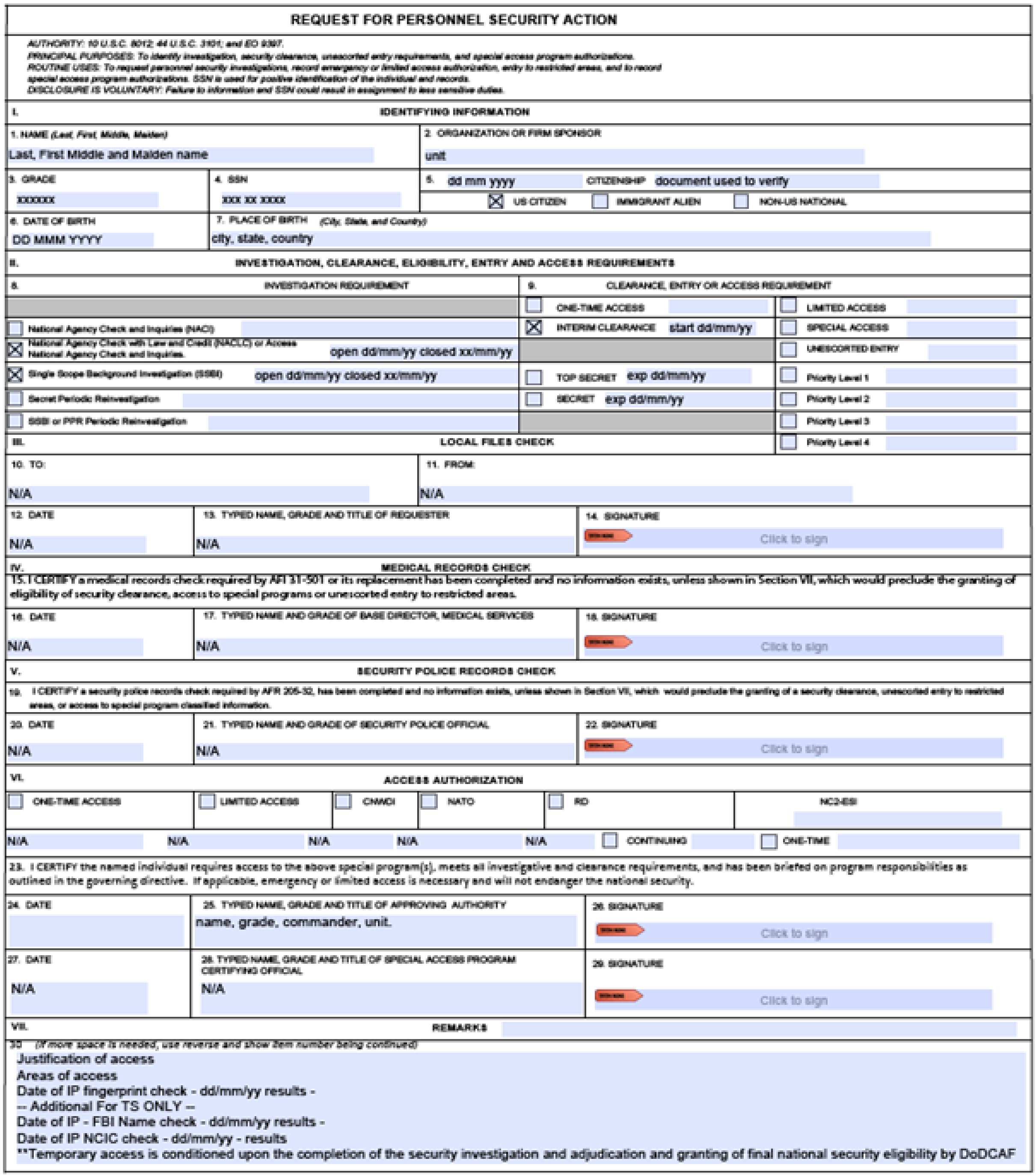
Figure A9.1. AF Form 2583 Interim Access Checklist.

SECTION I
BLOCK 1. Full name BLOCK 2. Current unit BLOCK 3. Grade BLOCK 4. Input member's SSN BLOCK 5. Verification of citizenship a. Date (of document reviewed) b. Type of document reviewed (see examples below) If a US citizen born outside US, must also verify SD form 240 **in addition to** birth certificate or passport. If member's US citizenship previously validated, check member's UPRG, SF 86 and DISS or successor system NBIS. BLOCK 6. Date of Birth (from document reviewed in block 5) BLOCK 7. Place of Birth (from document reviewed in block 5)
SECTION II
BLOCK 8. Investigation Requirement a. Select ONE investigation type (use ONLY NACLAC for secret /SSBI for TS) b. Add the open/closed dates using DD/MM/YY format BLOCK 9. Clearance, Entry or Access Requirement a. Check "Interim Clearance" and add the start date using DD/MM/YY format b. Select either TS or secret and add the expiration date (1 year from start date)
SECTION III, IV, V, VI – Items 10-22
Not used at Minot AFB.
SECTION VII
BLOCK 24. Input date approving authority makes decision BLOCK 25. Self-explanatory BLOCK 26. Approving authority signs. BLOCKS 27-29. Not applicable Block 30. Include the following item a. Areas where access will occur (e.g., flight line, WSA, office SIPR terminal/safe, etc.) b. Date/results of fingerprint check (e.g., DD/MM/YY- favorable **OR** no determination) c. **ADDITIONALLY:** All TS interim access MUST also have the following (1) Date/results of FBI Name check (2) Date/results of NCIC check (3) NOTE: **TS interim access is NOT authorized without these checks**
SECTION V – Items 12-14
Not used at Minot AFB

Attachment 10

REQUEST FOR PERSONNEL SECURITY ACTION

Figure A10.1. Request For Personnel Security Action.



REQUEST FOR PERSONNEL SECURITY ACTION

AUTHORITY: 10 U.S.C. 8012; 44 U.S.C. 3101; and EO 9397.
PRINCIPAL PURPOSES: To identify investigation, security clearance, unescorted entry requirements, and special access program authorizations.
ROUTINE USES: To request personnel security investigations, record emergency or limited access authorization, entry to restricted areas, and to record special access program authorizations. SSN is used for positive identification of the individual and records.
DISCLOSURE IS VOLUNTARY: Failure to information and SSN could result in assignment to less sensitive duties.

I. IDENTIFYING INFORMATION

1. NAME *(Last, First, Middle, Maiden)*: Last, First Middle and Malden name

2. ORGANIZATION OR FIRM SPONSOR: unit

3. GRADE: XXXXXX

4. SSN: XXX XX XXXX

5. dd mm yyyy CITIZENSHIP document used to verify
☒ US CITIZEN ☐ IMMIGRANT ALIEN ☐ NON-US NATIONAL

6. DATE OF BIRTH: DD MMM YYYY

7. PLACE OF BIRTH *(City, State, and Country)*: city, state, country

II. INVESTIGATION, CLEARANCE, ELIGIBILITY, ENTRY AND ACCESS REQUIREMENTS

8. INVESTIGATION REQUIREMENT		9. CLEARANCE, ENTRY OR ACCESS REQUIREMENT			
		☐ ONE-TIME ACCESS		☐ LIMITED ACCESS	
☐ National Agency Check and Inquiries (NACI)		☒ INTERIM CLEARANCE	start dd/mm/yy	☐ SPECIAL ACCESS	
☒ National Agency Check with Law and Credit (NACLC) or Access National Agency Check and Inquiries.	open dd/mm/yy closed xx/mm/yy			☐ UNESCORTED ENTRY	
☒ Single Scope Background Investigation (SSBI)	open dd/mm/yy closed xx/mm/yy	☐ TOP SECRET	exp dd/mm/yy	☐ Priority Level 1	
☐ Secret Periodic Reinvestigation		☐ SECRET	exp dd/mm/yy	☐ Priority Level 2	
☐ SSBI or PPR Periodic Reinvestigation				☐ Priority Level 3	
III. LOCAL FILES CHECK				☐ Priority Level 4	

10. TO: N/A

11. FROM: N/A

12. DATE: N/A

13. TYPED NAME, GRADE AND TITLE OF REQUESTER: N/A

14. SIGNATURE: Click to sign

IV. MEDICAL RECORDS CHECK

15. I CERTIFY a medical records check required by AFI 31-501 or its replacement has been completed and no information exists, unless shown in Section VII, which would preclude the granting of eligibility of security clearance, access to special programs or unescorted entry to restricted areas.

16. DATE: N/A

17. TYPED NAME AND GRADE OF BASE DIRECTOR, MEDICAL SERVICES: N/A

18. SIGNATURE: Click to sign

V. SECURITY POLICE RECORDS CHECK

19. I CERTIFY a security police records check required by AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.

20. DATE: N/A

21. TYPED NAME AND GRADE OF SECURITY POLICE OFFICIAL: N/A

22. SIGNATURE: Click to sign

VI. ACCESS AUTHORIZATION

☐ ONE-TIME ACCESS	☐ LIMITED ACCESS	☐ CNWDI	☐ NATO	☐ RD		NC2-ESI
N/A	N/A	N/A	N/A	N/A	☐ CONTINUING	☐ ONE-TIME

23. I CERTIFY the named individual requires access to the above special program(s), meets all investigative and clearance requirements, and has been briefed on program responsibilities as outlined in the governing directive. If applicable, emergency or limited access is necessary and will not endanger the national security.

24. DATE:

25. TYPED NAME, GRADE AND TITLE OF APPROVING AUTHORITY: name, grade, commander, unit.

26. SIGNATURE: Click to sign

27. DATE: N/A

28. TYPED NAME, GRADE AND TITLE OF SPECIAL ACCESS PROGRAM CERTIFYING OFFICIAL: N/A

29. SIGNATURE: Click to sign

VII. REMARKS

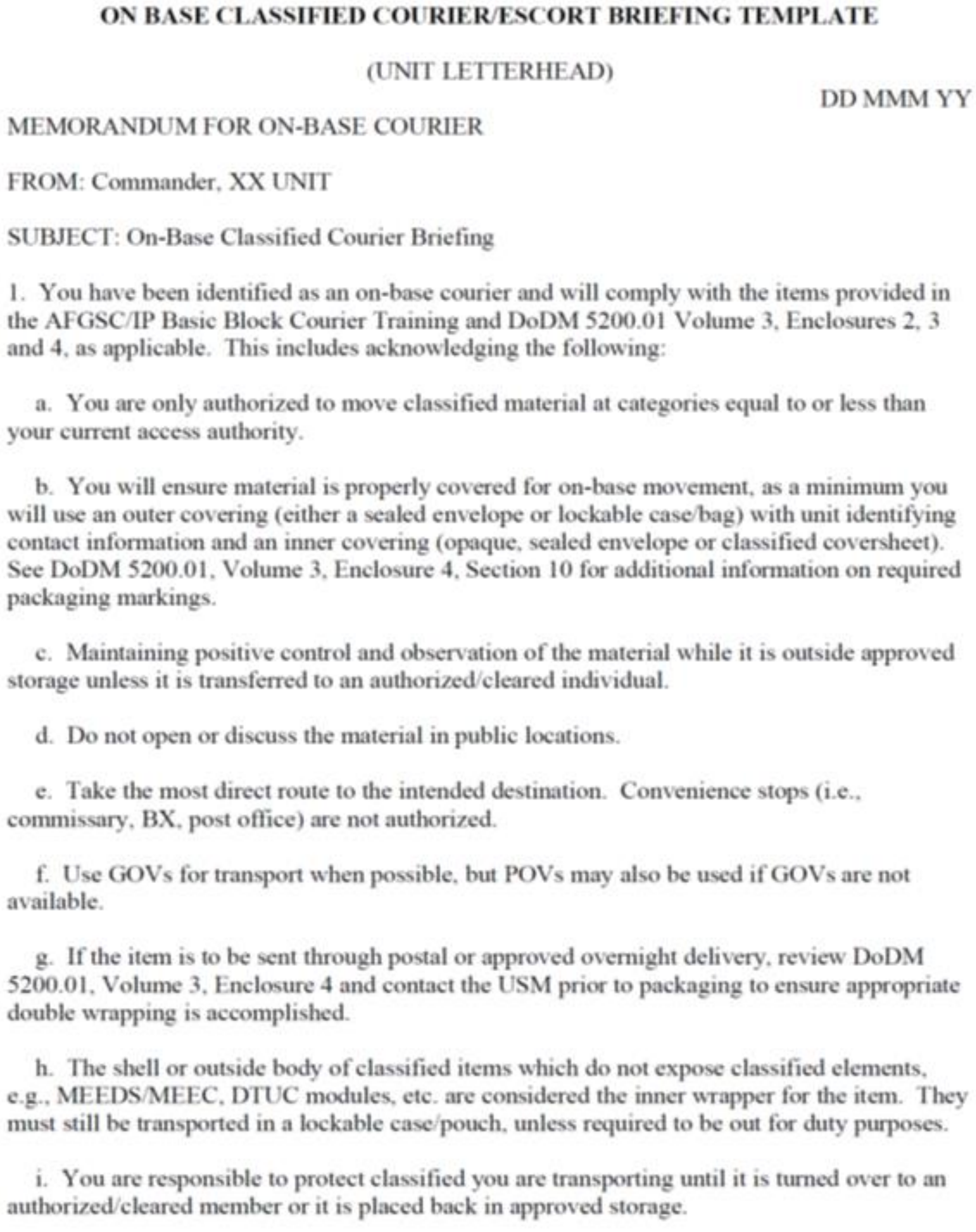
30 *(If more space is needed, use reverse and show item number being continued)*

Justification of access
Areas of access
Date of IP fingerprint check - dd/mm/yy results -
-- Additional For TS ONLY --
Date of IP - FBI Name check - dd/mm/yy results -
Date of IP NCIC check - dd/mm/yy - results
**Temporary access is conditioned upon the completion of the security investigation and adjudication and granting of final national security eligibility by DoDCAF

Attachment 11

ON BASE CLASSIFIED COURIER/ESCORT BRIEFING TEMPLATE

Figure A11.1. On Base Classified Courier/Escort Briefing Template.



ON BASE CLASSIFIED COURIER/ESCORT BRIEFING TEMPLATE

(UNIT LETTERHEAD)

DD MMM YY

MEMORANDUM FOR ON-BASE COURIER

FROM: Commander, XX UNIT

SUBJECT: On-Base Classified Courier Briefing

1. You have been identified as an on-base courier and will comply with the items provided in the AFGSC/IP Basic Block Courier Training and DoDM 5200.01 Volume 3, Enclosures 2, 3 and 4, as applicable. This includes acknowledging the following:

a. You are only authorized to move classified material at categories equal to or less than your current access authority.

b. You will ensure material is properly covered for on-base movement, as a minimum you will use an outer covering (either a sealed envelope or lockable case/bag) with unit identifying contact information and an inner covering (opaque, sealed envelope or classified coversheet). See DoDM 5200.01, Volume 3, Enclosure 4, Section 10 for additional information on required packaging markings.

c. Maintaining positive control and observation of the material while it is outside approved storage unless it is transferred to an authorized/cleared individual.

d. Do not open or discuss the material in public locations.

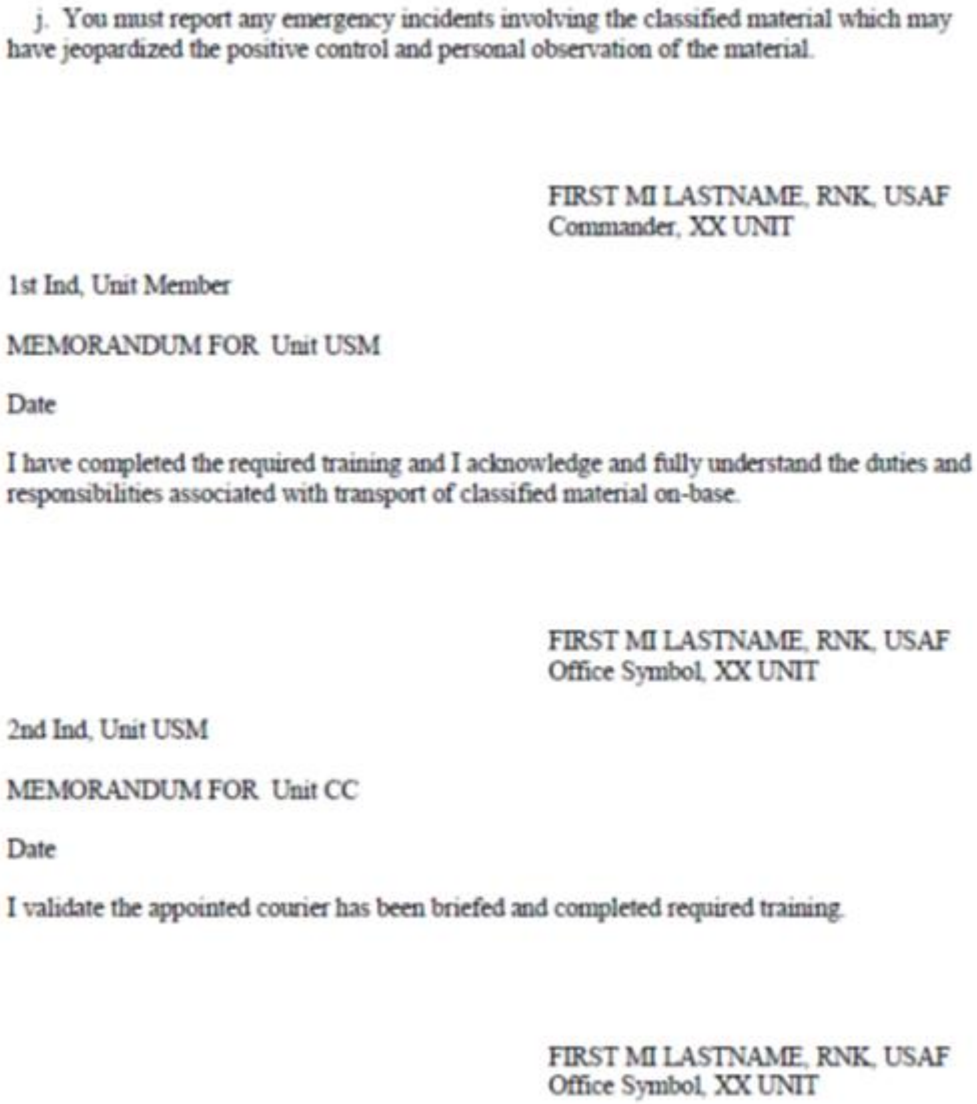
e. Take the most direct route to the intended destination. Convenience stops (i.e., commissary, BX, post office) are not authorized.

f. Use GOVs for transport when possible, but POVs may also be used if GOVs are not available.

g. If the item is to be sent through postal or approved overnight delivery, review DoDM 5200.01, Volume 3, Enclosure 4 and contact the USM prior to packaging to ensure appropriate double wrapping is accomplished.

h. The shell or outside body of classified items which do not expose classified elements, e.g., MEEDS/MEEC, DTUC modules, etc. are considered the inner wrapper for the item. They must still be transported in a lockable case/pouch, unless required to be out for duty purposes.

i. You are responsible to protect classified you are transporting until it is turned over to an authorized/cleared member or it is placed back in approved storage.



j. You must report any emergency incidents involving the classified material which may have jeopardized the positive control and personal observation of the material.

FIRST MI LASTNAME, RNK, USAF
Commander, XX UNIT

1st Ind, Unit Member

MEMORANDUM FOR Unit USM

Date

I have completed the required training and I acknowledge and fully understand the duties and responsibilities associated with transport of classified material on-base.

FIRST MI LASTNAME, RNK, USAF
Office Symbol, XX UNIT

2nd Ind, Unit USM

MEMORANDUM FOR Unit CC

Date

I validate the appointed courier has been briefed and completed required training.

FIRST MI LASTNAME, RNK, USAF
Office Symbol, XX UNIT

Attachment 12

DISTRIBUTION LISTING (E-COPIES ONLY)

Table A12.1. Distribution Listing (e-copies only).

DISTRIBUTION	NO. COPIES		DISTRIBUTION	NO. COPIES
HQ AFGSC/IP	1		91 MW/CC	1
5 BW/CC	1		91 OG/CC	1
			91 OSS/CC	
5 BW/CP	1		740 MS/CC	1
5 BW/PA	1		741 MS/CC	1
5 BW/IG	1		742 MS/CC	1
5 BW/DS	1			
5 BW/SE	1		91 MXG/CC	1
5 BW/JA	1		91 MMXS/CC	1
5 CPTS/CC	1		791 MXS/CC	1
5 MSG/CC	1		91 SFG/CC	1
5 CES/CC	1		91 MSFS/CC	1
5 CONS/CC	1		91 SSPTS/CC	
5 CS/CC	1		791 MSFS/CC	1
5 FSS/CC	1		891 MSFS/CC	1
5 LRS/CC	1			
5 SFS/CC	1		219 SFS/CC	1
5 MXG/CC	1		582 HG	1
5 AMXS/CC	1		54 HS/CC	1
5 MXS/CC	1			
5 MUNS/CC	1		DeCA	1
705 MUNS/CC	1			
			DET 813/AFOSI	1
5 OG/CC	1			
5 OSS/CC	1		AAFES	1
23 BS/CC	1			
69 BS/CC	1			
5 MDG/CC	1			
Note: This instruction will only be provided electronically				