BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-401

1 NOVEMBER 2001

SPACE AND MISSILE SYSTEMS CENTER Supplement 1

24 FEBRUARY 2003

Security

INFORMATION SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ USAF/XOFI (Deborah Ross)

Certified by: HQ USAF/XOF (Brig Gen Richard A. Coleman)

Supersedes AFI 31-401, 17 September 2001

Pages: 149

Distribution: F

It contains Air Force (AF) unique guidance needed to supplement Air Force Policy Directive (AFPD) 31-4, *Information Security*; Executive Order (EO) 12958, *Classified National Security Information*, 20 Apr 95; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information*, 13 Oct 95; and, Department of Defense (DOD) 5200.1-R, *Information Security Program*, 17 Jan 97, for the management of the Air Force Information Security Program. Additional references include DOD Instruction (DODI) 5240.11, *Damage Assessments*, 23 Dec 91; and, DOD Directive (DODD) 5210.83, *Unclassified Controlled Nuclear Information (UCNI),* 15 Nov 91. All these references are listed at the end of each paragraph where applicable. HQ USAF/XOF is delegated approval authority for revisions to this AFI.

(SMC) The OPR for this supplement is SMC/AXPI (Ms Suzanne Rowland). This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-401, dated 1 Nov 01, Information Security Program Management. This supplement describes SMC's procedures for use in conjunction with the basic AFI.

SUMMARY OF REVISIONS

This change is necessary to incorporate IC 2000-1 and 2000-2 which were inadvertently deleted when the last revision incorporated IC 2001-1. This revision incorporates Interim Change IC 2001-1. This change updates the table of contents to reflect new attachments for Original Classification Authorities, an Appointment of Inquiry Official Memorandum, and a Preliminary Inquiry of Security Incident Report; updates the office of primary responsibility for this Air Force Instruction (AFI); clarifies Standard Form (SF) 311, ***Agency Information Security Program Data***, reporting requirements; clarifies authority for nuclear weapon security classification policy and how to obtain the policy; adds guidance for command-

ers and/or staff agency chiefs to process administrative sanctions; adds the requirement for HQ USAF/XOFI to conduct program reviews; completely replaces **Chapter 9**, Actual or Potential Compromise of Classified Information, to implement additional reporting and investigative procedures concerning security incidents; implements automatic declassification extensions; incorporates guidance on systematic declassification reviews; clarifies safeguarding requirements for secure rooms; and, updates handcarrying classified information policy to include laptops. See the last attachment of the publication, IC 01-3, for the complete IC. A bar (|) indicates revision from the previous edition.

(SMC) This change updates paragraphs **2.4.1.**, **5.11.3. (Added)**, **5.12.1. (Added)**, **5.29.1.1. (Added)**, **6.1.7. (Added)** and **7.1.1.**; adds paragraphs **1.3.5.1.**, **1.4.2.3. (Added)**, **1.7.1.**, **2.1.2.3.3. (Added)**, **4.8.2.**,**4.12. (Added)**, **5.5.**, **5.6.9.**, **5.7.**, **5.10.1.**, **5.11.4. (Added)**, **5.15.**, **5.15.2.**, **5.15.3.**, **5.25.1. (Added)**, **5.28.3.1. (Added)**, **8.11.1.**, **8.14.4. (Added)**, **8.16.3.**, and **9.7.2.2.**; deletes paragraphs 1.3.5.2., **4.11. (Added)**, 5.20.7., and 8.9. Removed all references to AFMC.

Chapter 1—POLICY AND PROGRAM MANAGEMENT **8**

1.1. Policy. 8
1.2. Philosophy. 8
1.3. Program Management. 8
1.4. Oversight. 10
1.5. Special Types of Information. 11
1.6. Exceptional Situations. 12
1.7. Reporting Requirements. 12
1.8. Administrative Sanctions. 12
1.9. Self-Inspection. 13
1.10. Forms Prescribed. 13

Chapter 2—ORIGINAL CLASSIFICATION **14**

2.1. Original Classification Authority: 14
2.2. Classification Prohibitions and Limitations 14
2.3. Classification Challenges. 14
2.4. Classification Guides. 15
2.5. Nuclear Weapons Classification Policy. 16

Chapter 3—DECLASSIFYING AND DOWNGRADING INFORMATION **17**

3.1. Declassification and Downgrading Officials. 17
3.2. Automatic Declassification. 17
3.3. Mandatory Declassification. 18
3.4. Systematic Review for Declassification. 18

3.5. Policy. 18

Chapter 4—Marking **19**

Section 4A General Provisions 19

4.1. General. 19

Section 4B Specific Markings on Documents [Reference DoD 5200.1-R, Chapter 5, Section 2] 19

4.2. Reason for Classification. 19

4.3. Declassification Instructions. 19

4.4. Marking Waivers. 19

4.5. Special Control and Similar Notices. 19

4.6. Audio and Video Tapes. 19

4.7. Removable AIS Storage Media. 19

4.8. Intelligence. 20

Chapter 5—SAFEGUARDING **22**

Section 5A Control Measures 22

5.1. General. 22

5.2. Reserve Component Participation In Security Planning. 22

5.3. Working Papers. 22

Section 5B Access 22

5.4. Granting Access to Classified Information. 22

5.5. Nondisclosure Agreement (NdA). 22

5.6. Access by Persons Outside the Executive Branch. 23

5.7. Access by Visitors. 26

5.8. Preventing Publication of Classified Information in the Public. 27

5.9. Access to Information Originating in a Non-DoD Department or Agency. 27

5.10. Administrative Controls. 27

Section 5C Safeguarding 29

5.11. Care During Working Hours. 29

5.12. End-of-Day Security Checks. 29

5.13. Residential Storage Arrangements. 29

5.14. In-Transit Storage. 30

5.15. Classified Meetings and Conferences. 30
5.16. Protecting Classified Material on Aircraft. 31
5.17. Information Processing Equipment. 32
5.18. General Safeguarding Policy. 33
5.19. Standards for Storage Equipment. 33
5.20. Storage of Classified Information. 34
5.21. Use of Key Operated Locks. 35
5.22. Procurement of New Storage Equipment. 35
5.23. Equipment Designations and Combinations. 35
5.24. Repair of Damaged Security Containers. 35
5.25. Maintenance and Operating Inspections. 36
5.26. Reproduction of Classified Material. 36
5.27. Control Procedures. 36

Section 5D Disposition and Destruction of Classified Material 36

5.28. Retention of Classified Records. 36
5.29. Methods and Standards. 37

Section 5E Alternative or Compensatory Control Measures 37

5.30. General. 37

Chapter 6—TRANSMISSION AND TRANSPORTATION 39

Section 6A Methods of Transmission or Transportation 39

6.1. General Policy. 39
6.2. Transmitting Top Secret Information. 40
6.3. Transmitting Secret Information. 40
6.4. Transmitting Confidential Information. 40
6.5. Transmission of Classified Material to Foreign Governments. 41

Section 6B Preparation of Material for Transmission 41

6.6. Envelopes or Containers. 41

Section 6C Escort or Handcarrying of Classified Material 42

6.7. General Provisions. 42
6.8. Documentation. 42

6.9. Handcarrying or Escorting Classified Material Aboard Commercial Passenger Aircraft. 43

FIGURE 6.1 (Added-SMC)SAMPLE COURIER LETTER 44

FIGURE 6.2 (Added-SMC)EXEMPTION NOTICE 45

Chapter 7—SPECIAL ACCESS PROGRAMS 46

7.1. Control and Administration. 46

7.2. Code Words and Nicknames. 46

Chapter 8—SECURITY EDUCATION AND TRAINING 47

Section 8A Policy 47

8.1. General Policy. 47

8.2. Methodology. 47

8.3. Roles and Responsibilities. 47

Section 8B Initial Security Orientation 48

8.4. Cleared Personnel. 48

8.5. Uncleared Personnel. 49

Section 8C Special Requirements 49

8.6. Original Classification Authorities (OCAs). 49

8.7. Declassification Authorities Other Than Original Classification Authorities. 49

8.8. **Derivative Classifiers, Security Personnel and Others.** 50

8.9. **Professional Security Personnel and Security Managers.** 50

8.10. Other Program Related Training Requirements. 50

Section 8D Continuing Security Education/Refresher Training 52

8.11. **Continuing and Refresher Training.** 52

Section 8E Access Briefings and Termination Debriefings 52

8.12. Access Briefings. 52

8.13. **Termination Debriefings.** 53

8.14. Refusal to Sign a Termination Statement. 54

Section 8F Program Oversight 54

8.15. **General.** 54

Section 8G Coordinating Requests for Formal Training 54

8.16. Coordinating Requests for Training. 54

Chapter 9—ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION 56

9.1. Policy. 56

9.2. Definitions. 56

9.3. Automated Information System (AIS) Deviations. 56

9.4. Sensitive Compartmented Information (SCI) Incidents. 56

9.5. Classification. 56

9.6. Public Release. 57

9.7. Reporting and Notifications. 57

9.8. Preliminary Inquiry. 58

9.9. Damage Assessment. 59

9.10. Formal Investigation. 59

9.11. Management and Oversight. 59

9.12. Unauthorized Absences. 60

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 61

Attachment 2—LIST OF AIR FORCE OFFICIALS AUTHORIZED TO CERTIFY ACCESS TO RESTRICTED DATA 66

Attachment 3—CONTROLLED UNCLASSIFIED INFORMATION 69

Attachment 4—DEPARTMENT OF THE AIR FORCE EXECUTIVE ORDER (EO) 12958 25-YEAR AUTOMATIC DECLASSIFICATION PLAN 71

Attachment 5—PHYSICAL SECURITY STANDARDS 77

Attachment 6—TRANSMISSION TO FOREIGN GOVERNMENTS 78

Attachment 7—AIR FORCE INFORMATION SECURITY PROGRAM TRAINING STANDARD 79

Attachment 8—APPOINTMENT OF INQUIRY OFFICIAL MEMORANDUM DEPARTMENT OF THE AIR FORCE AIR FORCE UNIT HEADING 90

Attachment 9—PRELIMINARY INQUIRY OF SECURITY INCIDENT REPORT DEPARTMENT OF THE AIR FORCE AIR FORCE UNIT HEADING 91

Attachment 10—AIR FORCE ORIGINAL CLASSIFICATION AUTHORITIES 92

Attachment 11—IC 2000-1 TO AFI 31-401, INFORMATION SECURITY PROGRAM MANAGEMENT 101

Attachment 12—IC 2000-2 TO AFI 31-401, INFORMATION SECURITY PROGRAM MANAGEMENT 125

Attachment 13—IC 2001-1 TO AFI 31-401, INFORMATION SECURITY PROGRAM MANAGEMENT 129

Chapter 1

POLICY AND PROGRAM MANAGEMENT

1.1. Policy. It is Air Force policy to identify, classify, downgrade, declassify, mark, protect, and destroy its classified information and material consistent with national policy. This general policy statement also applies to unclassified controlled information under the purview of relevant statutes, regulations and directives. *[Reference DoD 5200.1-R, Chapter 1, Section 1]*

1.2. Philosophy. Protecting information is critical to mission accomplishment. The goal of the Information Security Program is to efficiently and effectively protect Air Force information by delegating authority to the lowest levels possible; encouraging and advocating use of risk management principles; focusing on identifying and protecting only that information that requires protection; integrating security procedures into our business processes so that they become transparent; and, ensuring everyone understands their security roles and responsibilities and *takes them seriously*.

1.3. Program Management. The strength of the Air Force Information Security Program is in its infrastructure. The infrastructure is important because it facilitates effective communication of our security policies and procedures to those performing the Air Force mission. With the support of commanders at all levels, this is accomplished predominantly through our Information Security Program Manager (ISPM) and security manager system. Both play an integral role in ensuring unit personnel know and understand their role in protecting classified information against unauthorized disclosure. *[Reference DoD 5200.1-R, Chapter 1, Section 2]*

1.3.1. Senior Security Official. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is designated the Air Force Senior Security Official responsible for ensuring implementation of the Information Security Program.

1.3.2. Air Force Program Manager. The Chief, Information Security Division (HQ USAF/XOFI) is responsible for policy, resource advocacy, and oversight of this program.

1.3.3. Commanders of Major Commands (MAJCOM), Direct Reporting Units (DRU), Field Operating Agencies (FOA), and Installations. These commanders are responsible for:

1.3.3.1. Establishing information security programs.

1.3.3.2. Identifying requirements.

1.3.3.3. Executing their programs to comply with this policy.

1.3.4. Information Security Program Managers (ISPM). The Chief of Security Forces, senior security forces official or Director/Chief of Acquisition Security is designated the ISPM at every level of command, as appropriate. ISPMs:

1.3.4. (SMC) The Director, Acquisition Systems Protection (SMC/AXP) is SMC's Information Security Program Manager (ISPM) for all SMC organizations and other organizations supported by SMC on Los Angeles AFB or in the Los Angeles area.

1.3.4.1. Manage Information Security Program implementation.

1.3.4.2. Provide oversight within their jurisdiction.

1.3.4.3. Provide and monitor training as required by **Chapter 8** of this AFI.

1.3.5. Unit Commanders or Equivalents. These commanders or equivalents will:

1.3.5. (SMC) For the purpose of this supplement, the term "unit commander" encompasses System Program Directors, Directors, Chiefs of staff agencies, or equivalents.

1.3.5.1. Appoint a primary and at least one alternate security manager to administer the unit's information security program.

1.3.5.1. (SMC) The term Acquisition Systems Protection Managers (ASPMs) will be used for security managers who are in the Security Specialist career field. ASPMs within SMC System Program Offices will perform all duties of a Security Manager for their organization as described in DoD 5200.1-R/AFI 31-401 and this supplement.

1.3.5.2. Ensure security managers receive required training according to **Chapter 8**.

1.3.5.3. Execute their programs to comply with this policy.

1.3.6. Security Managers.

1.3.6.1. Set up the Information Security Program within their unit or staff agency.

1.3.6.1. (SMC) Use the guidance contained in DoD 5200.1-R/AFI 31-401 and this supplement to implement unit Information Security Programs.

1.3.6.2. Develop and update a unit security operating instruction.

1.3.6.2. (SMC) Acquisition Systems Protection Managers (ASPMs)/Unit Security Managers (USMs) must establish a Security Manager's Handbook. The book must contain letters of appointment, copies of last SMC/AXP Integrated Protection Review (IPR), Security Operating Instructions, Semi-Annual Security Inspection Reports, Security Manager's Meeting Minutes, Information Letters, Inspection Checklists and other items pertinent to their organizational security programs. Maintain 2 years of Integrated Protection Reviews (IPR) reports. Include other unit security documentation; i.e., Industrial Security, Personnel Security, Operations Security (OPSEC), and Computer Security (COMPUSEC) applicable to the overall unit security program.

1.3.6.2.1. (Added-SMC) Prepare a unit Security Operating Instruction (OI) using the SMC/AXP Security OI template.

1.3.6.3. Advise the unit commander or staff agency chief on security issues pertaining to the unit or staff agency.

1.3.6.4. Attend ISPM hosted security manager meetings.

1.3.6.4.1. (Added-SMC) ASPMs/USMs are required to attend SMC/AXP conducted annual Security All Calls/Security Manager Meetings.

1.3.6.5. Update and remind personnel of security policies and procedures.

1.3.6.6. Oversee the unit or staff agency self-inspection program.

1.3.6.7. Report security incidents immediately to the ISPM through their unit commander or staff agency chief.

1.3.6.8. Assist the unit commander or staff agency chief and ISPM in monitoring security incident investigations.

1.3.6.9. Participating in security education training as defined in **Chapter 8**.

1.3.7. Supervisors:

1.3.7.1. Establish criteria, evaluate, and rate Air Force employees on their performance of security responsibilities. *[Reference DoD 5200.1-R, Paragraph 1-202g]*

1.3.7.1.1. Officer. See AFI 36-2402, *Officer Evaluation System,* paragraph 1.2.7.

1.3.7.1.2. Enlisted. See AFI 36-2403, *The Enlisted Evaluation System (EES)*, paragraphs 1.1.9.2.

1.3.7.1.3. Civilian. See AFI 36-1001, *Managing the Civilian Performance Program,* paragraph 1.4.

1.3.7.2. Provide and ensure training as directed in **Chapter 8** of this AFI.

1.3.8. Sensitive Compartmented Information (SCI). The Director of Intelligence Surveillance and Reconnaissance (HQ USAF/XOI) is responsible for SCI policy.

1.3.9. Foreign Disclosure. The Deputy Under Secretary of the Air Force, International Affairs, (SAF/IA), 1080 Air Force Pentagon, Washington DC 20330-1080, oversees the release of Air Force classified information to foreign governments, persons, and international organizations.

1.3.10. Historian. The Air Force Historian (HQ USAF/HO), 500 Duncan Avenue, Box 94, Bolling AFB DC 20332-1111, approves or disapproves historical researchers access to classified information. *[Reference DoD 5200.1-R, Paragraph 6-201d]*

1.4. Oversight. In addition to using metrics for evaluating the effectiveness of the Information Security Program (see paragraph **1.7.**), these oversight practices will be implemented *[Reference DoD 5200.1-R, Chapter 1, Section 7]*:

1.4.1. MAJCOM, DRU, and FOA ISPMs will incorporate information security issues into Inspector General (IG) inspections/reviews. In addition MAJCOM, DRU, and FOA personnel may conduct security assistance visits upon request from the unit.

1.4.2. Base level ISPMs will conduct program reviews on an annual basis. ***EXCEPTION:*** Conduct program reviews every two years of activities or units that do not store classified information.

1.4.2.1. (Added-SMC) SMC/AXP will conduct annual IPRs of each organization that handles, stores, processes or has access to classified information. IPRs serve two primary purposes: (1) identify and benchmark security processes/products within a program for crossfeed to all SMC organizations, and (2) identify security short falls within a program and recommend corrective action. The IPR team uses a random sampling method; but the review will be sufficiently thorough to determine the overall effectiveness of the unit's protection program.

1.4.2.2. (Added-SMC) Upon completion of the IPR, the commander/director/staff agency chief will be provided a formalized briefing (as applicable) and a written report indicating the status of their security program. Corrective actions will be implemented as soon as possible. When serious program deficiencies are identified, a letter of response to SMC/AXP is required from the commander/director/staff agency chief indicating the applicable corrective measures taken. A copy of the report must be maintained in the Security Manager's Handbook for two years.

1.4.2.3. (Added-SMC) The interval between IPR may be extended to two years when an organization has relatively small classified holdings and results of other visits reflects the organization has a strong Information Security Program.

1.4.3. Unit commanders and equivalents involved with processing or holding classified information ensure personnel conduct semiannual security self-inspections to evaluate information security program effectiveness. ***EXCEPTION:*** Activities with a small volume of classified material may work with the ISPM to develop an oversight schedule consistent with risk management principles.

1.4.3.1. Security managers should not conduct self-inspections themselves but have others in the unit perform them.

1.4.3.2. (Added-SMC) Ensure that contractors performing work at LAAFB on Visitor Group Agreements or classified contracts for your organization are covered under the organization's self-inspection program.

1.4.4. HQ USAF/XOFI will visit MAJCOMs, DRUs, and FOAs to review their information security programs. HQ USAF/XOFI will work with MAJCOM, DRU, and FOA ISPMs to determine frequency and visit dates.

1.5. Special Types of Information. *[Reference DoD 5200.1-R, Chapter 1, Section 3]*

1.5.1. Restricted Data. *[Reference DoDD 5210.2 and DoD 5200.1-R, Paragraph 1-300]*

1.5.1.1. General. This type of Restricted Data is described and governed by DoDD 5210.2, *Access to and Dissemination of Restricted Data,* 12 Jan 78. Air Force personnel will mark and safeguard Restricted Data according to DoDD 5210.2. Air Force certifying officials are listed in **Attachment 2**. These officials are responsible for certifying access to Restricted Data using DoE Form 5631.20, **Request for Visit or Access Approval** (see paragraph **5.7.1.2.**). They may delegate this authority to the level they deem necessary for operational efficiency. Officials delegated the authority will sign "For" the access granting official as identified in **Attachment 2**. Air Force personnel may obtain DoE Forms 5631.20 from the DoE activity they are visiting.

1.5.1.1.1. Activities must notify HQ USAF/XOFI through command ISPM channels of changes to the list of certifying officials (**Attachment 2**) as they occur. When doing so, they must also provide the position title, activity and office symbol of the affected party. ***NOTE:*** When the change involves an activity name change, access granting officials will sign forms authorizing access using the current activity name and a note that identifies the activity it superseded until the list of officials is updated.

1.5.1.1.2. MAJCOM, DRU, and FOA ISPMs maintain a list of certifying officials and their designees who can sign these requests. ISPMs must notify HQ USAF/XOFI of any changes to the list. HQ USAF/XOFI will periodically update a master list (**Attachment 2**) and distribute it to DoE and MAJCOM, DRU, and FOA ISPMs for their information.

1.5.1.2. Critical Nuclear Weapon Design Information (CNWDI). This type of Restricted Data is particularly sensitive and access is limited to the minimum number of people who need it to do their job.

1.5.1.2.1. CNWDI Approving Officials. These officials are responsible for granting CNWDI access. This authority is assigned to division chiefs and above at all levels of command.

1.5.1.3. Granting Access. Approving officials will ensure access and briefings are documented on AF Form 2583, **Request for Personnel Security Action** (available on the Air Force Electronics Publications Library (AFEPL)).

1.5.1.4. Protection. Air Force personnel will protect CNWDI in the same manner prescribed for collateral classified information. This includes limiting access to containers storing CNWDI to only those personnel who have been granted CNWDI access. *[Reference DoD 5200.1-R, Chapter 1, Section 3]*

1.5.2. North Atlantic Treaty Organization (NATO). *[Reference DoD 5200.1-R, Paragraph 1-303]*

1.5.2.1. HQ USAF/XOFI is responsible for overall development, approval, and implementation of NATO security policy within the Air Force.

1.5.2.2. HQ USAFE/SF is responsible for developing and recommending NATO security policy for implementation within the Air Force.

1.6. Exceptional Situations.

1.6.1. Request for Waivers. Commanders send requests to waive provisions of AFPD 31-4, DoD 5200.1-R, or this AFI through command ISPM channels to HQ USAF/XOFI. FOAs also coordinate their requests with their respective functional head of secretariat or air staff office. *[Reference DoD 5200.1-R, Chapter 1, Section 4]*

1.7. Reporting Requirements. *[Reference DoD 5200.1-R, Paragraph 1-600]*

1.7.1. MAJCOM, FOA, and DRU ISPMs will submit the SF Form 311, ***Agency Information Security Program Data*** (available at **http://www.gsa.gov/forms**), report to HQ USAF/XOFI by 1 September of each year. MAJCOM/DRU/FOAs sample data for Item 6 (Number of Classification Decisions) during a consecutive 2 week period each fiscal year quarter (Nov-Jan, Feb-Apr, May-Jul, and Aug). In the last quarter the 2 week period must be set during August since the reports are required by 1 September. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

1.7.1. (SMC) Security Managers will submit SF Form 311, Agency Information Security Program Data (available at **http://www.gsa.gov/forms**), to SMC/AXP by 15 August of each year.

1.7.2. Management Information System (MIS) Reporting. AFPD 31-4 requires all activities to send their measurement data, through command ISPM channels, to HQ USAF/XOFI via Report Control Symbol (RCS): HAF-SFI(SA)9222, *The Information Security Measurement Report*. *[Reference AFPD 31-4]*

1.8. Administrative Sanctions.

1.8.1. Send reports through command ISPM channels to HQ USAF/XOFI when someone knowingly, willfully, or negligently discloses classified information to unauthorized individuals as specified in EO 12958. *[Reference DoD 5200.1-R, Chapter 1, Section 5]*

1.8.2. Air Force commanders and staff agency chiefs report unauthorized disclosures of classified information that violate criminal statutes to their servicing ISPM and Air Force Office of Special Investigations (AFOSI) offices. *[Reference DoD 5200.1-R, Chapter 1, Section 5]*

1.8.3. Commanders and/or staff agency chiefs take and process administrative sanctions/actions for civilian employees in accordance with AFI 36-704, *Discipline and Adverse Actions* and in accordance with AFI 36-2907, *Unfavorable Information File (UIF) Program*, for military personnel. Contact the servicing civilian or military personnel flight office if assistance is needed.

1.9. Self-Inspection. See paragraph **1.4.** of this AFI *[Reference DoD 5200.1-R, Chapter 1, Section 7]*.

1.10. Forms Prescribed. These forms are prescribed throughout this AFI and are available through the Air Force Publications Distribution system: AF Form 54, **Classified Computer Deck Cover Sheet**; AF Form 143, **Top Secret Register Page**; AF Form 144, **Top Secret Access Record and Cover Sheet**; AF Form 310, **Document Receipt and Destruction Certificate**; AF Form 1565, **Entry, Receipt, and Destruction Certificate**; AF Form 2587, **Security Termination Statement**; and, AF Form 2595, **Classified Protection Insertion Sheet.**

Chapter 2

ORIGINAL CLASSIFICATION

2.1. Original Classification Authority: *[Reference DoD 5200.1-R, Chapter 2, Section 2]*

2.1.1. The Secretary of the Air Force serves as the original classification authority (OCA) and may further delegate this authority.

2.1.2. The process for delegating OCA authority is as follows:

2.1.2.1. Secretary of the Air Force delegates Top Secret, Secret, and Confidential authority.

2.1.2.2. The Administrative Assistant to the Secretary of the Air Force delegates Secret and Confidential authority.

2.1.2.3. All requests for the delegation of original classification authority will be forwarded through command ISPM channels to the Chief, Information Security Division, HQ USAF/XOFI, 1340 Air Force Pentagon, Washington, DC 20330-1340, for processing.

2.1.2.3.1. Address requests for original Top Secret authority to the Secretary of the Air Force.

2.1.2.3.2. Address requests for original Secret and Confidential authority to the Administrative Assistant to the Secretary of the Air Force.

2.1.2.3.3. (Added-SMC) Only the individual occupying the position of SMC/CC, as well as AFPEO Space, has been delegated by SAF as an Original Classification Authority (OCA) for Top Secret and further delegation is not authorized. Any SMC organization requesting delegation as an OCA must submit a request with full justification to SMC/AXP for processing through ISPM channels in accordance with para 2.1.2.4.

2.1.2.4. All requests will contain the full position title, functional office symbol, and a detailed explanation of why the position requires original classification authority.

2.1.3. HQ USAF/XOFI will maintain the master list of Air Force OCAs (see **Attachment 10**). Periodically, HQ USAF/XOFI will request OCA validation from the MAJCOMs, FOAs, and DRU ISPMs.

2.1.3.1. Personnel will submit requests for changes or new requests through ISPM command channels as they occur.

2.1.3.2. See paragraph **8.6.** and **8.11.1.2.** for OCA training requirements.

2.2. Classification Prohibitions and Limitations

2.2.1. The OCA having jurisdiction over the subject matter determines if information requested under the Freedom of Information Act (FOIA) or the mandatory declassification review provisions of E.O. 12958 should be declassified. *[Reference DoD 5200.1-R, Paragraph 2-402e]*

2.3. Classification Challenges. *[Reference DoD 5200.1-R, Chapter 4, Section 9]*

2.3.1. Send challenges to classification of Air Force information, in writing, to the OCA with jurisdiction over the information in question.

2.3.1.1. The OCA will monitor, record, and resolve all challenges to classification decisions.

2.3.1.2. Challenges to classification decisions will be processed separate from all Freedom of Information (FOIA) and Privacy Act (PA) requests unless the challenger specifically cites these authorities for obtaining the information.

2.3.1.3. (Added-SMC) Keep a suspense copy of the classification challenge letter with the classified information/material in question until final determination is provided by the OPR.

2.3.2. Send challenges to classification of non-Air Force originated information, in writing, to the OCA with jurisdiction over the information in question with an information copy to HQ USAF/XOFI. This office will assist in the coordination process.

2.3.3. Challenges to reclassification decisions are sent through command ISPM channels to HQ USAF/XOFI.

2.3.4. All classified information undergoing a challenge or a subsequent appeal will remain classified until a final resolution is reached.

2.4. Classification Guides. OCAs are to publish classification guides to facilitate the proper and uniform derivative classification of their information. *NOTE:* In some cases, OCAs may determine that publishing classification guidance in other forms is more effective, i.e., program protection plans, system protect guides, Air Force instructions. In these cases, the applicable publication will be considered the guide and the reporting requirements in paragraph **2.4.2.** still apply. *[Reference DoD 5200.1-R, Chapter 2, Section 5]*

2.4. (SMC) SMC's Program Protection Plans (PPPs) and existing System Protect Guides must contain required collateral security classification determinations for the program in accordance with SMC/CC's approved Space Program Protection Planning Guide (SP^3G). Formal coordination with SMC/AXP, as the designated ISPM for SMC, is required and will be documented in the PPP.

2.4.1. The responsible OCA will ensure the guide is current and reflects accurate classification instructions at all times. All guides will be reviewed at least once every two years.

2.4.1. (SMC) SMC/AXP maintains copies of PPPs, SPGs and associated security classification guides (SCGs) for all SMC programs. SMC Program Directors/Program Managers will conduct biennial reviews of their PPPs to ensure security classification, threat, and vulnerability currency and provide SMC/AXP with a record.

2.4.2. The OCA will report publication of or changes to security classification guides to the Administrator, Defense Technical Information Center (DTIC) using Department of Defense (DD) Form 2024, **DoD Security Classification Guide Data Elements** (available at **http://web1.whs.osd.mil/icdhome/DDEFORMS.HTM**) and to HQ USAF/XOFI. OCAs must also forward a copy of the applicable publication or change to *[Reference DoD 5200.1-R, Paragraph 2-502e]*:

2.4.2.1. HQ USAF/XOFI, 1340 Air Force Pentagon, Washington DC 20330-1340.

2.4.2.2. HQ AFDO/CC, 1720 Air Force Pentagon, Washington, DC 20330-1720.

2.4.2.3. HQ AFHRA/RSA, 600 Chennault Circle, Maxwell AFB AL 36112.

2.4.2.4. SAF/PAS, 1690 Air Force Pentagon, Washington, DC 20330-1690.

2.4.2.5. DTIC, Attention: DTIC-OCP, 8725 John J. Kingman Road, Suite 944, Ft. Belvoir, VA 22060-6218.

2.4.3. Within 180 days of the publication of this AFI, each OCA will provide an electronic version of their classification guidance (i.e., Security Classification Guides (SCGs), AFIs, Correspondence) to the addressees listed in paragraph **2.4.2.** This will facilitate the development of an interactive, key word searchable database. Electronic copies must be done in Microsoft Word 97 and saved to a 3.5" diskette as a .pdf file. If this capability is not yet available, annotate "//SIGNED//" above the signature element and add the date the original was signed.

2.4.4. HQ USAF/XOFI will maintain the master list of all Air Force classification guides.

2.4.5. Each OCA will revise their security classification guides to include an advisory statement in the Release of Information section:

2.4.5.1. Release of Program Data on the World Wide Web. Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. Information intended for publication on publicly accessible or unprotected web sites must be cleared for public release prior to publication according to AFI 35-101. If there are any doubts, do not release the information.

2.5. Nuclear Weapons Classification Policy. The DOD and the Department of Energy (DOE) issue joint security classification guidance for information relating to nuclear weapons. The Air Force issues security classification policy (AFI 31-407) for nuclear weapons surety information. Most of these products are classified and users will require the appropriate security clearance before accessing them. Users may obtain copies of Joint DOD/DOE classification guides through DTIC at a cost. Users forward requests for copies of the Air Force security classification policy to HQ USAF/XOFI (1340 Air Force Pentagon, Washington DC 20330-1340) through command ISPM channels. Requests must include the name, address, and phone number of the activity point of contact, and the point of contact's level of access. ISPMs will validate this information before submitting the requests to HQ USAF/XOFI. For all other Air Force or other agency guides, go direct to the originator. Users refer to DOD 5200.1-I, *DOD Index of Security Classification Guides*, to determine what other guides relating to nuclear weapons classification guidance are needed. DOD 5200.1-I can be obtained from DTIC.

Chapter 3

DECLASSIFYING AND DOWNGRADING INFORMATION

3.1. Declassification and Downgrading Officials. Within the Air Force the following positions have been delegated the authority to declassify or downgrade classified information. This authority extends to information for which the specific declassification official has classification, program, or functional responsibility. *[Reference DoD 5200.1-R, Chapter 4, Section 1]*

3.1.1. All Air Force Original Classification Authorities.

3.1.2. SAF/PAS. Chief, Office for Security Review, Office of Public Affairs, Office of the Secretary of the Air Force, 1690 Air Force Pentagon, Washington, DC, 20330-1690. See AFI 31-205, *Air Force Security and Policy Review Program*, for guidance on use of this authority.

3.1.3. HQ USAF/XOFI. Chief, Information Security Division, Directorate of Security Forces, 1340 Air Force Pentagon, Washington, DC 20330-1340.

3.1.4. AFDO, Chief, Reserve Declassification Team, 2221 South Clark Street, Suite 600, Arlington VA 22202. This authority is delegated to AFDO on a case-by-case basis by SAF/AA.

3.1.5. AFHSO/CC. Commander, Air Force History Support Office, 500 Duncan Avenue, Box 94, Bolling AFB DC 20332-1111. This authority only applies to historical documents under the jurisdiction of HQ USAF/HO and after obtaining classification recommendations from the functional owners of the information.

3.1.6. AFHRA/CC. Commander, Air Force Historical Research Agency, 600 Chennault Circle, Maxwell AFB, AL, 36112-6424. This authority only applies to historical documents under the jurisdiction of HQ USAF/HO and after obtaining classification recommendations from the functional owners of the information.

3.2. Automatic Declassification. According to Executive Order 12958, *Classified National Security Information*, Section 3.4, all Air Force activities that possess classified information that are of permanent historical value and are 25 years old or older should have completed a declassification review of these documents by 17 April 2000.

3.2.1. The 17 April 2000 suspense date has been extended for two groups of records (multiagency and non-multiagency) according to Executive Order 13152, Amendment to Executive Order 12958.

3.2.1.1. The new suspense date for documents still requiring a review that do not contain multiagency equities is 17 October 2001. This applies to all Air Force activities that did not meet the original suspense for reviewing these records (see paragraph **3.2.**).

3.2.1.2. The new suspense date for documents still requiring a review that contain multiagency or intelligence equities is 17 April 2003. MAJCOMs/FOAs/DRUs found to be eligible for the new referral suspense are: AFDO, ACC, AFMC, AFOTEC, AFOSI, AIA, NAIC, AFHSO, and AFTAC.

3.2.2. The Air Force Twenty Five-Year Automatic Declassification Plan (**Attachment 4**) provides specific policy and guidance on performing automatic declassification reviews within the Air Force. This plan is still valid even though some of the suspense dates have changed as indicated in **3.2.1.** above.

3.2.3. The process of automatic declassification evolved into systematic declassification after April 2000.

3.3. Mandatory Declassification.

3.3.1. Send all requests for mandatory declassification review (MDR) to 11 CS/SCSR (MDR), 1000 Air Force Pentagon, Washington DC 20330-1000

3.3.2. Send appeals to MDR decisions through 11 CS/SCSR (MDR) to SAF/AA, the Air Force Appellate Authority for MDRs.

3.4. Systematic Review for Declassification. Activities will set up an annual schedule for conducting systematic declassification reviews for the following records:

3.4.1. Records of permanent historical value prior to their twenty-fifth birthday. These records will be reviewed and appropriate action taken by 31 Dec of the same year of their twenty-fifth birthday (25 years from the origination date).

3.4.2. Records of permanent historical value that have been exempted from automatic declassification prior to their tenth birthday. These records will be reviewed and appropriate action taken by 31 Dec of the tenth year of their exemption (ten years from the exemption date).

3.4.3. Other records. Activities will set up a reasonable schedule for conducting declassification reviews for all other classified records once a review of records described in paragraphs **3.4.1.** and **3.4.2.** have been completed.

3.4.4. It is the intent of the Air Force not to transfer permanently valuable records to the National Archives Records Administration until they can be declassified without bringing harm to the national security. *[Reference DoD 5200.1-R, Section 5]*

3.5. Policy. When information is declassified, it is not releasable to the public until it has been approved for release through the security review process according to AFI 35-205. The same holds true for declassified or unclassified information that will be placed on an Internet site that can be accessed by the public.

Chapter 4

MARKING

Section 4A—General Provisions

4.1. General. Air Force personnel who originally and derivatively classify information will mark those products according to DoD 5200.1-R. They may also use DoD 5200.1-PH, *Marking Classified Documents*, to guide them through the process. *[Reference DoD 5200.1-R, Chapter 5, Section 1]*

Section 4B—Specific Markings on Documents [Reference DoD 5200.1-R, Chapter 5, Section 2]

4.2. Reason for Classification. In the case of exempted information, the reason(s) for classification must be consistent with the exemption category(ies). *[Reference DoD 5200.1-R, Paragraph 5-203]*

4.3. Declassification Instructions. The exemption category(ies) must be consistent with the reason(s) used for classifying the information. *[Reference DoD 5200.1-R, Paragraph 5-204]*

4.4. Marking Waivers. Requesters send requests for marking waivers through command ISPM channels to HQ USAF/XOFI. For Special Access Program (SAP) marking requirements, send requests through command SAP channels to SAF/AAZ. *[Reference DoD 5200.1-R, Paragraph 5-206d]*

4.5. Special Control and Similar Notices. *[Reference DoD 5200.1-R, Paragraph 5-208]*

4.5.1. Communications Security (COMSEC). See AFI 33-211, *Communications Security (COMSEC) User Requirements,* for additional guidance on marking COMSEC media. *[Reference DoD 5200.1-R, Paragraph 5-208d]*

4.5.2. Technical Documents. See AFI 61-204, *Disseminating Scientific and Technical Information,* for guidance on disseminating technical documents. *[Reference DoD 5200.1-R, Paragraph 5-208e]*

4.5.3. SAPs. See AFI 16-701, *Special Access Programs,* for additional guidance on SAP documents. *[Reference DoD 5200.1-R, Paragraph 5-208f]*

4.5.4. Other Special Notices. See **Attachment 2** for references. *[Reference DoD 5200.1-R, Paragraph 5-208h]*

4.6. Audio and Video Tapes. Personnel responsible for marking and maintaining original classified audio and video tapes that document raw test data do not need to include footers/headers showing the applicable classification markings. However, the required classification markings must be placed on the outside of the container and reel. All copies made from the original tapes must include headers/footers that show the applicable classification markings. This will help ensure that valuable historical test data is not inadvertently erased during the classification marking process. *[Reference DoD 5200.1-R, Paragraphs 5-407 and 5-409a-b]*

4.7. Removable AIS Storage Media. Personnel use SF Form 706, Top Secret ADP Media Classification Label; SF 707, Secret ADP Media Classification Label; SF Form 708, Confidential ADP Media Classification Label; SF Form 711, ADP Data Descriptor Label, on removable AIS storage media. These are

available through the Air Force Publications Distribution System. [Reference DOD 5200.1-R, Paragraphs 5-407 and 5-409a-b]

4.7.1. (Added-SMC) Classified diskettes/CDs must be marked externally with the Office of Primary Responsibility, overall classification level, and date. Internal files must be marked with the date of creation, classification & declassification instructions, additional warning notices, as applicable, and page and paragraph markings.

4.7.2. (Added-SMC) Unclassified diskettes must be marked externally with the Office of Primary Responsibility and dated.

4.7.3. (Added-SMC) Apply overall classification marking to the front, back, and spine of all classified media, to include the container of the media (CD, VCR and cassette tape jackets). Apply all applicable associated markings to the media as prescribed in DoD 5200.1-R/AFI 31-401.

4.7.4. (Added-SMC) Mark and control digital cameras used for classified filming with the highest classification of the information contained within, and other applicable associated markings as appropriate.

4.8. Intelligence. *[Reference DoD 5200.1-R, Paragraph 5-410]*

4.8.1. See AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information*, for Air Force policy on intelligence. *[Reference DoD 5200.1-R, Paragraphs 5-410a-b]*

4.8.2. The Special Security Office (SSO) is the focal point for release and dissemination of SCI. The Director of Central Intelligence Directive 5/6, *Intelligence Disclosure Policy*, provides criteria for release of intelligence to foreign officials. *[Reference DoD 5200.1-R, Paragraph 5-410c]*

4.8.2. (SMC) SMC/IN performs SSO functions for all SMC organizations.

4.9. (Added-SMC) Amendment to E.O. 12958 extended the deadline to 17 April 2003 for non-exempt records and 17 Oct 2001 (see para **3.2.1.1.**) for permanent records to ensure that all classification markings required by the Executive Order 12958, Classified National Security Information, are applied to original and derivative classified information.

4.10. (Added-SMC) All classified material must reflect a date of creation either on the classified material itself or within an applicable Technical Order/Security Classification Guide/System Protection Guide/ Program Protection Plan.

4.11. (Added-SMC) Mark file dividers on the top, bottom and tab with the highest classification.

4.12. (Added-SMC) The absence of "NOFORN", or equivalent markings on documentation of any kind is not authority for release to a foreign government, representative, or international organization. This applies to classified national security information and unclassified controlled information requested by a foreign citizen. Contact your ASPM/USM, or SMC/AXP Foreign Disclosure Office for guidance on obtaining authorization for disclosure of information, unless it has already been cleared for public release by SMC/PA.

4.13. (Added-SMC) The last page of a document will be considered its back cover unless there is a clearly discernible separate page serving as the cover. Mark the back cover as required in the DoD 5200.1R.

4.14. (Added-SMC) For Official Use Only (FOUO) markings refer to DoD 5400.7R, Freedom of Information Act program, Chapter 4, as supplemented by AF and AFSPC.

Chapter 5

SAFEGUARDING

Section 5A—Control Measures

5.1. General. The Air Force will control and account for classified information as described in paragraph **5.11.** of this instruction. *[Reference DoD 5200.1-R, Paragraph 6-100a]*

5.2. Reserve Component Participation In Security Planning. Reserve components should be included early on in the security planning phase for weapon systems that will be directly released to and operated by reserve forces.

5.3. Working Papers. Originators must also show their name, organization, and office symbol on classified working papers in indelible ink. *[Reference DoD 5200.1-R, Paragraph 6-101]*

Section 5B—Access

5.4. Granting Access to Classified Information. Personnel who have authorized possession, knowledge, or control of classified information grant individuals access to classified information when required for mission essential needs and when the individual has the appropriate access level according to AFI 31-501; has signed an SF 312, **Classified Information Nondisclosure Agreement** (available on the AFEPL); and, has a need to know the information. Those granting access to classified information must gain the originator's approval before releasing the information outside the Air Force or as specified by the originator of the material. Also see paragraph **5.6.1.1.** of this AFI. *[References DoD 5200.1-R, Paragraph 6-200, and EO 12958, Section 4.2(b)]*

5.4.1. Confirm an Individual's Access Level. Those granting access to classified information will confirm a person's access level by:

5.4.1.1. Checking the person's access level on the Automated Security Clearance Approval System (ASCAS) roster or Sentinel Key (ASCAS successor) clearance record. This only applies to Air Force employees (See AFI 31-501);

5.4.1.2. Confirming it through the employee's security manager, supervisor, or commander;

5.4.1.3. Checking the access level on a person's temporary duty (TDY) or permanent change of station (PCS) orders; or,

5.4.1.4. Receiving a visit request from the visitor's security manager or supervisor. See paragraph **5.7.2.** for further guidance.

5.4.1.5. (Added-SMC) As a additional option, SMC personnel may verify security clearance eligibility and completion of the SF 312, Nondisclosure Agreement, with SMC/AXP. Need-to-know must be determined by the possessor of the classified material/information. SMC organizations will not require formal visit request documents of other SMC organizations.

5.5. Nondisclosure Agreement (NdA). Signing the NdA is a pre-requisite for obtaining access (see paragraph **5.4.**). Unit commanders, staff agency chiefs, or designated personnel are responsible for ensur-

ing their employees have signed one by checking the Automated Security Clearance Approval System (ASCAS) or the employee's personnel records. If they have not signed one, those responsible use DoD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Pamphlet*, to brief people on the purpose. Also see DoD 5200.1-R, paragraph 9-200b for training requirements. ***NOTE:*** When the employee's access level is passed to another office or activity, that office or activity can assume the employee has signed one.

5.5. (SMC) NOTE: Submit signed/resigned SF Forms 312, Nondisclosure Agreements, to SMC/AXP for entry into Sentinel Key. AXP will send the SF 312s to either Civilian Personnel or Military Personnel as applicable.

5.5.1. Retention. The following organizations will retain NdAs for 50 years.

5.5.1.1. For active military members, security managers send NdAs to HQ AFPC/DPSRI1, 550 C St., W, Suite 21, Randolph AFB, TX 78150-4723.

5.5.1.2. For reservists, security managers send NdAs to HQ ARPC/DSMPM, 6760 E. Irvington Place, #4450, Denver, CO 80280-4450.

5.5.1.3. For retired general officers receiving access under the provisions of AFI 31-501 and who do not already have a signed NdA in their retired file, ISPMs send NdAs to HQ AFPC/DPSRS, 550 C St., W, Suite 21, Randolph AFB TX 78150-4723.

5.5.1.4. For Air Force civilians, the servicing civilian personnel office files the NdA in the person's official personnel file.

5.5.1.5. For persons outside the Executive Branch who receive access according to paragraph **5.6.**, the servicing ISPM to the activity granting access will file the NdA. They must retain them for 50 years.

5.5.2. When To Sign.

5.5.2.1. Unit commanders and staff agency chiefs may allow their people 30 days to sign a NdA.

5.5.2.2. Air Reserve and the Guard may allow their people eight training days to sign.

5.5.3. Refusal To Sign. When a person refuses to sign a NdA, the commander:

5.5.3.1. Records the fact the person refused to sign it.

5.5.3.2. Denies the individual access to classified information.

5.5.3.3. Takes steps to deny or revoke the person's security clearance eligibility by setting up a Security Information File according to AFI 31-501.

5.5.3.4. (Added-SMC) Immediately notify SMC/AXP when an individual refuses to sign a SF 312, Nondisclosure Agreement.

5.6. Access by Persons Outside the Executive Branch.

5.6.1. Policy. MAJCOM, DRU, and FOA commanders and heads of Secretariat or Air Staff offices or their designees authorize individuals outside the executive branch to access Air Force classified material as follows unless otherwise provided in DoD 5200.1-R, paragraph 6-201. *[Reference DoD 5200.1-R, Paragraph 6-201]*

5.6.1.1. Authorizing Officials (those cited in paragraph **5.6.1.** above) may grant access once they have:

5.6.1.1.1. Gained release approval from the originator or owner of the information.

5.6.1.1.2. Determined the individual has a current favorable personnel security investigation as defined by AFI 31-501 and a check of the Defense Clearance and Investigations Index (DCII) and a local files check (LFC) shows there is no unfavorable information since the previous clearance. A LFC must be processed according to AFI 31-501. ***EXCEPTION:*** In cases where there is no current personnel security investigation as defined in AFI 31-501, MAJCOM, DRU, and FOA commanders and heads of Secretariat or Air Staff offices may request a National Agency Check (NAC) and grant access up to the Secret level before the NAC is complete when there is a favorable LFC and the 497 IG/INS confirms there is no unfavorable information on the individual in the DCII.

5.6.1.1.3. Determined granting access will benefit the government.

5.6.1.2. Requests for access must include:

5.6.1.2.1. The person's name, date and place of birth, and citizenship.

5.6.1.2.2. Place of employment.

5.6.1.2.3. Name and location of installation or activity where the person needs access.

5.6.1.2.4. Level of access required.

5.6.1.2.5. Subject of information the person will access.

5.6.1.2.6. Full justification for disclosing classified information to the person.

5.6.1.2.7. Comments regarding benefits the U.S. Government may expect by approving the request.

5.6.1.3. The authorizing official will coordinate the processing of the NAC request with the nearest Air Force authorized requester of investigations.

5.6.1.4. Individuals with approval must sign a NdA before accessing information. Upon completion of access, individuals must sign an AF Form 2587, **Security Termination Statement**.

5.6.2. Congress. See AFI 90-401, *Air Force Relations with Congress*, for guidance when granting classified access to members of Congress, its committees, members, and staff representatives. *[Reference DoD 5200.1-R, Paragraph 6-201a]*

5.6.3. Government Printing Office (GPO). The GPO processes and confirms their personnel's access. *[Reference DoD 5200.1-R, Paragraph 6-201b]*

5.6.4. Representatives of the General Accounting Office (GAO). See AFI 65-401, *Relations with the General Accounting Office*, for access requirements. *[Reference DoD 5200.1-R, Paragraph 6-201c]*

5.6.5. Historical Researchers. AFHSO is the authority for granting access to historical researchers on behalf of the Air Force Historian (HQ USAF/HO). *[Reference DoD 5200.1-R, Paragraph 6-201d]*

5.6.5.1. General. Requests for classified access by historical researchers will be processed only in exceptional cases wherein extraordinary justification exists. Access will be granted to the researcher only if the records cannot be obtained through available declassification processes (i.e.,

the FOIA and MDR processes) and when the access clearly supports the interests of national security.

5.6.5.2. Providing Access.

5.6.5.2.1. The researcher must apply to AFHSO in writing for the access. The application will fully describe the project including the sources of documentation that the researcher wants to access.

5.6.5.2.2. If AFHSO accepts the request for access, they will provide the researcher with written authorization to go to the nearest Air Force installation security office to fill out the necessary paperwork for a national agency check (NAC) according to AFI 31-501.

5.6.5.2.3. If the results of the NAC are favorable and AFHSO approves access, the researcher must sign a SF 312 and an agreement to submit any notes and manuscript(s) for security and policy review (AFI 35-205, *Air Force Security and Policy Review Program*). This process is to ensure the documents do not contain any classified information and, if so, determine if they can be declassified. Send the SF 312 to AFHSO for retention.

5.6.5.2.4. Other Terms.

5.6.5.2.4.1. The access agreement is valid for two years. One two-year renewal is possible. A renewal will not be considered if the project appears to be inactive in the months before the end of the original agreement.

5.6.5.2.4.2. Access will be limited to those records 25 or more years of age.

5.6.5.2.4.3. Access based on a NAC is good for Secret and Confidential information but does not meet the requirement for access to Restricted Data (RD) or SAP information. Access to Top Secret information is not authorized.

5.6.5.2.4.4. Access will be allowed only to Air Force records at AFHSO, AFHRA, and the National Archives and Records Administration (NARA).

5.6.5.2.4.5. Access to Air Force records still in the custody of the originating offices in the Washington National Capital Region must be approved in writing by the originating offices or their successors. It is the responsibility of the researcher to secure this approval.

5.6.6. Former Presidential Appointees. Persons who previously occupied policy making positions to which they were appointed by the President may not remove classified information upon departure from office. All such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information they originated, received, reviewed, signed, or that was addressed to them while serving in their official capacity, provided the applicable Air Force original classification authority: *[Reference DoD 5200.1-R, Paragraph 6-201e]*

5.6.6.1. Makes a written determination that such access is clearly consistent with the interests of national security;

5.6.6.2. Uses the same access determination procedures outlined in paragraph **5.6.1.1.** of this AFI;

5.6.6.3. Limits the access to specific categories of information over which the Air Force original classification authority has classification jurisdiction;

5.6.6.4. Maintains custody of the information or authorizes access to documents in the custody of the NARA; and,

5.6.6.5. Obtains the individual's agreement to safeguard the information and to submit any notes and manuscript for a security review (AFI 35-205) to ensure that the documents do not contain classified information or to determine if any classified information should be declassified.

5.6.7. Judicial Proceedings. See AFI 51-301, *Civil Litigation,* for more information regarding the release of classified information in litigation.

5.6.8. Other Situations. Follow the guidance in paragraph **5.6.1.1.** above. *[Reference DoD 5200.1-R, Paragraph 6-201g]*

5.6.9. Foreign Nationals, Foreign Governments, and International Organizations. Owners of classified information disclose it to foreign nationals, foreign governments, and international organizations only when they receive authorization from SAF/IAD, 1080 Air Force Pentagon, Washington DC 20330-1080. (See AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*, for more specific guidance.)

5.6.9. (SMC) SMC/AXP is the AFSPC designated Foreign Disclosure Office for all foreign visits and disclosure for all SMC organizations and The Aerospace Corporation. SMC/AXP must be notified immediately when a foreign visit to any SMC organization is to occur or any SMC personnel are going to visit a foreign national/country.

5.6.10. Retired Flag or General Officers or Civilian Equivalent. See AFI 31-501. These individuals need not sign a NdA if the original one is already filed in their retired file (see paragraph **5.5.1.3.**).

5.7. Access by Visitors. *[Reference DoD 5200.1-R, Paragraph 6-202]*

5.7. (SMC) SMC organizations will send a visit request letter with the following information to the visit location.

Name, Grade, and Position Title

Nationality, Date, and Place of Birth

Duty Address

Level of Security Clearance

Date/Duration of Visit

POC to be Visited

Purpose

Signature (Security Managers), Grade, Title, Phone #, & Date

5.7.1. Outgoing Visit Requests for Air Force Employees. When an Air Force employee requires access to classified information at:

5.7.1.1. A contractor activity, the supervisor or security manager forwards a visit request to the contractor's visitor control center or facility security office. The visit request will include the same information required by DoD 5220.22-M, *National Industrial Security Program Operating Manual*, Jan 95.

5.7.1.2. A Department of Energy (DoE) activity, the supervisor or security manager prepares and processes DoE Form 5631.20, **Request for Visit or Access Approval**, according to DoDD 5210.2, *Access to and Dissemination of Restricted Data*. Also see paragraph **1.5.1.1.** of this AFI.

5.7.1.3. Another Air Force activity, see paragraph **5.4.1.**

5.7.1.4. Another agency, the supervisor or security manager forwards a visit request to the agency security office unless instructed otherwise.

5.7.2. Incoming Visit Requests. Air Force activity visit hosts serve as the approval authority for visits to their activities. Installation or activity commanders receiving a visit request:

5.7.2.1. From Air Force employees, see paragraph **5.4.1.**

5.7.2.2. From contractors, see DoD 5220.22-M, Chapter 6.

5.7.2.3. From foreign nationals or U.S. citizens representing a foreign government, commanders or their designees process the visit request according to AFI 16-201.

5.7.3. Duration of Visit Request. Visit requests are valid for up to a year—renew them annually as necessary to accomplish the mission.

5.8. Preventing Publication of Classified Information in the Public. See AFI 35-205 for guidance on security reviews to keep people from publishing classified information in personal or commercial articles, presentations, theses, books or other products written for general publication or distribution.

5.9. Access to Information Originating in a Non-DoD Department or Agency. Holders allow access under the rules of the originating agency.

5.10. Administrative Controls.

5.10.1. Top Secret. The Air Force accounts for Top Secret material and disposes of such administrative records according to AFMAN 37-139. These procedures ensure stringent need to know rules and security safeguards are applied to our most critical and sensitive information.

5.10.1. (SMC) SMC/AXP must be consulted before any SMC organization establishes a Top Secret account.

5.10.1.1. Establishing a Top Secret Control Account (TSCA). Unit commanders and staff agency chiefs who routinely originate, store, receive, or dispatch Top Secret material establish a Top Secret account and designate a Top Secret Control Officer (TSCO), with one or more alternates, to maintain it. The TSCO uses AF Form 143, **Top Secret Register Page**, to account for each document (to include page changes and inserts) and each piece of material or equipment to include Automated Information System (AIS) media. ***NOTE:*** For AIS or microfiche media, TSCOs must either describe each Top Secret document stored on the media on the AF Form 143 or attach a list of the documents to it. This will facilitate a damage assessment if the media is lost or stolen. ***EXCEPTIONS:***

5.10.1.1.1. Top Secret Messages. TSCOs don't use AF Form 143 for Top Secret messages kept in telecommunications facilities on a transitory basis for less than 30 days. Instead, use message delivery registers or other similar records of accountability.

5.10.1.1.2. Defense Courier Service (DCS) Receipts. TSCOs don't use AF Forms 143 as a receipt for information received from or delivered to the DCS. DCS receipts suffice for accountability purposes in these cases.

NOTE: TSCOs may automate their accounts as long as all of the required information is included in the AIS.

5.10.1.2. Top Secret Disclosure Records.

5.10.1.2.1. The TSCO uses AF Form 144, **Top Secret Access Record and Cover Sheet**, as the disclosure record and keeps it attached to the applicable Top Secret material.

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

5.10.1.3. Top Secret Inventories. Unit commanders and staff agency chiefs:

5.10.1.3.1. Designate officials to conduct annual inventories for all Top Secret material in the account and to conduct inventories whenever there is a change in TSCOs. These officials must be someone other than the TSCO or alternate TSCOs of the TSCA being inventoried. The purpose of the inventory is to ensure all of the Top Secret material is present and its status is correctly annotated on the AF Form 143.

5.10.1.3.2. Ensure necessary actions are taken to correct deficiencies identified in the inventory report.

5.10.1.3.3. Ensure the inventory report and a record of corrective actions taken are maintained with the account.

5.10.1.4. Top Secret Receipts. TSCOs use AF Form 143 as a receipt when transferring Top Secret material from one TSCO to another on the same installation.

5.10.1.5. Top Secret Facsimiles. Top Secret facsimiles will be processed as another copy of the main Top Secret document in the TSCA. All the same rules apply except the register page and disclosure record will be faxed along with the document to the addressee. The addressee will sign and return them immediately to the sender for inclusion in the TSCA.

5.10.2. Secret. Unit commanders and staff agency chiefs set up procedures for internal control of Secret material. ***NOTE:*** Personnel may use AF Form 310, **Document Receipt and Destruction Certificate**, as a receipt when transmitting Secret material. Personnel possessing Secret material must use a receipt when:

5.10.2.1. Entering Secret material into a mail distribution system.

5.10.2.2. Handcarrying Secret material off an installation (i.e., Air Force base, separately located missile field) or to non-Air Force activities.

5.10.2.3. Handcarrying Secret material to a recipient not shown on the material's distribution and who is with another DoD agency or Service or another Air Force activity residing on the same installation (i.e., the Pentagon, Air Force Base). ***EXCEPTION:*** Within the National Capital Region (NCR), a receipt is not required when transferring Secret material to an Air Force activity shown on the distribution list.

5.10.3. Confidential. Individuals need not use a receipt for Confidential material unless asked to do so by the sending activity.

5.10.4. Foreign Government Information. See DoD 5200.1-R, Chapter 6, Section 6, for receipting requirements.

5.10.4.1. (Added-SMC) Record NATO briefing completed for access to NATO classified information on the AF Form 2583, Request for Personnel Security Action. Maintain the forms in the Security Manager Handbook

5.10.5. Retention of Receipts. Retain receipt and other accountability records in accordance with AFMAN 37-139, *Records Disposition Schedule.*

Section 5C—Safeguarding

5.11. Care During Working Hours. Personnel removing classified material from storage must,

5.11.1. For Top Secret material, use AF Form 144 or AF Form 54, **Classified Computer Deck Cover Sheet**, instead of SF Form 703, **Top Secret Cover Sheet** (see paragraph **5.10.1.3.1.**). *[Reference DoD 5200.1-R, Paragraph 6-301]*

5.11.2. For Secret or Confidential material, use SF Form 704, **Secret Cover Sheet**, or SF Form 705, **Confidential Cover Sheet**, as appropriate. These forms are available through the Air Force Publications Distribution system.

5.11.3. (Added-SMC) Annotate the SF 702, Security Container Check Sheet, each time the container is opened and closed and again at the end of each duty day. If the container was not opened, annotate the SF 702 with "NOT OPENED" or line through the applicable row. Ensure that the "check by" block is initialed and the time is recorded. Include weekends and holidays when personnel are working.

5.11.4. (Added-SMC) Safeguard Federal Express packages and United States Postal Service First Class Mail bearing the notice "Postmaster: Do Not Forward" as classified information at the Secret level until you confirm the contents. If the above material has not been verified at the close of business (COB), secure the material in a GSA security container or an approved vault/secure storage room. For organizations that do not have secure storage capability, contact 61 ABG/DO (Command Post) to store overnight.

5.12. End-of-Day Security Checks. Each unit and staff agency that processes classified information will conduct an end-of-day security check to ensure classified material is stored appropriately. Personnel conducting these checks will do so at the close of each working day and record them on the SF Form 701, **Activity Security Checklist**, and the SF Form 702**, Security Container Check Sheet**, when security containers are present. The SF Form 701 is available on the AFEPL and the SF Form 702 is available through the Air Force Publications Distribution system.

5.12.1. (Added-SMC) Each SMC organization that possesses classified, FOUO, unclassified controlled information (UCI) information, or Automated Information System (AIS) equipment will conduct an end-of-day security check to ensure the material is stored/secured appropriately. Individuals must be designated in writing to conduct end-of-day security checks and post SF 701, Activity Security Checklist.

5.13. Residential Storage Arrangements.

5.13.1. SAF/OS and SAF/AA authorize the removal of Top Secret information from designated working areas in off-duty hours for work at home. Requesters send requests through command ISPM channels to HQ USAF/XOFI. ***[Reference DoD 5200.1-R, Paragraph 6-306a]***

5.13.2. MAJCOM, FOA, and DRU commanders, or their ISPMs approve requests for removing Secret and Confidential material from designated work areas during non-duty hours. *[Reference DoD 5200.1-R, Paragraph 6-306b]*

5.13.3. Contingency Plans. The written procedures will include arrangements for notifying the responsible activity to pick up the classified container and material in the event something happens to the user. *[Reference DoD 5200.1-R, Paragraph 6-306c]*

5.14. In-Transit Storage. Installation commanders

5.14.1. Provide an overnight repository for classified material and ensure operations dispatch, passenger services, base entry controllers, and billeting people know about it.

5.14.2. Authorize the storage of Secret material on the flightline during in-processing for deployment when the material is stored in a standard GSA approved security container setting on a pallet and the in-transit area is controlled and located on an Air Force installation.

5.15. Classified Meetings and Conferences. *[Reference DoD 5200.1-R, Paragraph 6-307]*

5.15. (SMC) A DepSecDef Memo, dated 26 Oct 01, rescinds subparagraph 6-307b of DoD Regulation 5200.1-R, dated January 1997. Portions or sessions of classified meetings, conferences, etc., shall be limited to appropriately cleared U.S. government or U.S. government contractor locations".

5.15.1. General. Activities hosting the meetings described will ensure appropriate security measures are taken to protect classified information discussed and provided to the attendees. These activities will develop a security plan addressing how the issues discussed in DoD 5200.1-R, paragraph 6-307, will be accomplished. For science and technology related meetings, see AFI 61-205, *Sponsoring or Cosponsoring, Conducting, and Presenting DoD Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings.*

5.15.2. Approval Authority. Installation commanders or their designees assess the need to set up and approve secure conference facilities under their security control. Normally, secure conference facilities are only set up at locations where frequent classified meetings or forums occur. Since these facilities are located on Air Force installations and are not used to store classified information, secure construction requirements are not mandated. However, if installation commanders or their designees determine the local threat and security environment dictates more stringent construction requirements, they can use DoD 5200.1-R, Appendix G as a guide for constructing the facility. For guidance on classified meetings scheduled at DoD contractor facilities, see DoD 5220.22-M, and AFI 31-601, *Industrial Security Program Management.*

5.15.2. (SMC) SMC/AXP performs this approval authority on behalf of SMC/CC. Organizations requiring recurring secure conference facilities under their control must contact SMC/AXP prior to use for an information and physical security assessment.

5.15.3. Foreign Participation. Hosting officials refer to both AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations,* and AFI 61-205, *Sponsoring or Cosponsoring, Conducting, and Presenting DoD Related*

Scientific Technical Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings for specific guidance.

5.15.3. (SMC) SMC/AXP is the designated Foreign Disclosure Office and must be coordinated with prior to any SMC organization hosting a conference, symposium, or other security meeting involving foreign nations.

5.15.4. Other Types. Meetings, conferences, seminars, and activities other than those described in DoD 5200.1-R, paragraph 6-307a, pertain to those that are going to be held at a non-government-owned and uncleared facility. In these cases, SAF/AA must approve the event. Hosting officials send requests through command ISPM channels to HQ USAF/XOFI. The request must include a security plan that describes how the issues discussed in DoD 5200.1-R, paragraph 6-307 will be accomplished. *[DoD 5200.1-R, Paragraph 6-307b]*

5.15.5. Technical Surveillance Countermeasures (TSCM) Surveys. Commanders or their designees determine to do TSCM surveys based on mission sensitivity and threat. See AFI 71-101, Volume I, *Criminal Investigations, Counterintelligence, and Protective Service Matters*, for additional guidance.

5.16. Protecting Classified Material on Aircraft. Classified material and components are routinely carried on USAF aircraft. The purpose of this paragraph is to provide minimum standards for the protection of classified material and components while minimizing the impact on aircrew operations. The following minimum standards are established to provide cost effective security of classified material and components and to ensure detection of unauthorized access.

5.16.1. Aircraft commanders (owners/users) are responsible for the protection of classified material and components aboard their aircraft whether on a DOD facility, at a civilian airfield, or then stopping in foreign countries in accordance with DOD 5200.1-R, paragraph 6-300. Aircraft commanders should consult with the local ISPM or senior security forces representative for assistance in complying with these requirements.

5.16.2. To provide security-in-depth for classified components and material on aircraft, park the aircraft in an established restricted area or equivalent if the aircraft is designated Protection Level (PL) 1, 2, or 3. Refer to AFI 31-101, Air Force Installation Security Program, for details about protection levels.

5.16.2.1. Lock the aircraft, when possible, using a GSA-approved changeable combination padlock (Federal Specification FF-P-110 series) to secure the crew entry door, and/or

5.16.2.2. Place all removable classified material (e.g., paper document, floppy disks, videotapes) in a storage container secured with a GSA-approved lock. The storage container must be a seamless metal (or similar construction) box or one with welded seams and a lockable hinged top secured to the aircraft. Hinges must be either internally mounted or welded. Containers installed for storage of weapons may also be used to store classified material even if weapons/ammunition are present, provided the criteria listed above have been met.

5.16.2.2.1. Have the aircraft and container checked for tampering every 12 hours. If unable to comply with the 12 hours due to crew rest, perform these checks no later than 1 hour after official end of crew rest.

5.16.2.2.2. Zeroize keyed communications security (COMSEC) equipment as required by AFKAG-1, Air Force Communications Security (COMSEC) Operations.

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

5.16.3. To provide security-in-depth for classified components and material on PL 4 or non-PL aircraft, park the aircraft in a controlled area. PL 4 and non-PL aircraft should not be parked in a restricted area due to use of force limitations.

5.16.3.1. Lock the aircraft using a GSA-approved changeable combination padlock (Federal Specification FF-P-110 series) to secure the crew entry door, and

5.16.3.2. Secure removable classified material IAW paragraph **5.16.2.2.** or **5.16.2.3.**

5.16.4. At non-U.S. controlled locations, host nation restricted/controlled areas may be used only if all material and components aboard the aircraft have been approved for release to the host nation by a cognizant foreign disclosure authority. Material should be secured IAW paragraph **5.16.2.** for restricted areas and paragraph **5.16.3.** for controlled areas.

5.16.5. If the aircraft cannot be parked in a restricted/controlled area:

5.16.5.1. Place removable classified material in a storage container and secure the container as described in paragraph **5.16.2.2.** Lock all aircraft egress points or secure them from the inside. Seal the aircraft with tamper proof seals such as evidence tape, numerically accountable metal, or plastic seals.

5.16.5.2. If the aircraft can be locked and sealed but there is no storage container, remove all removable classified material and store it in an approved security container in an authorized U.S. facility. Classified components (e.g., AAR 47, ALE 47, etc.) may be stored in a locked and sealed aircraft.

5.16.5.3. If the aircraft cannot be locked and sealed and no storage container is available, off-load all classified material and components to an approved security container in an authorized U.S. facility.

5.16.5.4. If none of the above criteria can be met, U.S. cleared personnel must provide continuous surveillance. Foreign national personnel cleared by their government may be used if all material and components aboard the aircraft have been approved for release to the host nation by a cognizant foreign disclosure authority.

5.16.6. MAJCOM/FOA/DRUs determine specific risk management security standards for weather diverts and in-flight emergencies.

5.16.7. If evidence exists of unauthorized entry, initiate a security investigation IAW **Chapter 9** of this AFI.

5.17. Information Processing Equipment.

5.17.1. Machines with Copying Capability. For copiers and facsimile machines or any machines with copying capability (i.e., microfiche machines), personnel consult their servicing information manager to determine if the machines are authorized for copying classified, and if so, determine if they retain any latent images when copying classified, and how to clear them when they do. When they need to be cleared, destroy the waste as classified material latent images are visible. Machine custodians must post a notice on machines approved for copying classified to inform users of the authority and clear-

ance procedures. Also see paragraph **5.27.** for reproduction authority. *[Reference DoD 5200.1-R, Paragraph 6-309]*

5.17.1.1. (Added-SMC) Reproduction equipment, to include microfiche readers/printers, must be approved prior to classified use by 61 CS. SMC/AXP can conduct an on-site survey of the proposed location and review the unit operating instruction outlining procedures for protecting classified information during the reproduction process. If possible, locate reproduction equipment in areas under constant surveillance of personnel responsible for enforcing rules against unauthorized use or in lockable areas/rooms. Once approval is obtained, post Classified Reproduction Rules near the reprographic equipment.

5.17.2. AIS Removable Equipment/Media.

5.17.2.1. For AIS machines and media (i.e., diskettes, compact discs) approved for processing classified information, personnel protect the AIS equipment or the removable hard disk drive and the AIS media at the protection level required by DoD 5200.1-R, Chapter 6 for the highest security classification processed by the AIS.

5.17.2.2. In the case of AIS media (i.e., diskettes, compact discs) used for storing classified information, personnel protect the media at the protection level required by DoD 5200.1-R, Chapter 6, for the highest security classification stored on the media.

5.17.3. Printer Ribbons and Toner Cartridges. For any type of printer with a ribbon that has been used to print classified information, personnel remove the ribbon and store it as classified. This also applies to printers with toner cartridges that retain latent images of the classified. See DoD 5200.1-R, Chapter 6 for storage requirements.

5.18. General Safeguarding Policy. *[Reference DoD 5200.1-R, Paragraph 6-400]*

5.18.1. See DoD 5200.1-R, paragraphs 1-400 and 6-800, when considering use of alternative safeguarding measures.

5.18.2. Use of Force for the Protection of Classified Material. See AFI 31-207, *Arming and Use of Force by Air Force Personnel.*

5.18.3. Sensitive Compartmented Information (SCI) Safeguarding Policy. See Air Force Manual (AFMAN) 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (supersedes USAFINTEL 201-1).*

5.18.4. Retention of Classified Records. Personnel follow the disposition guidance in AFMAN 37-139, *Records Disposition Schedule.*

5.19. Standards for Storage Equipment. Holders of classified material may not use containers without a General Services Administration (GSA) label. If a label is not present on the outside or in the locking drawer of the container, a locksmith should be able to confirm the safe is a GSA approved container. If there is doubt, personnel may contact the DoD Lock Hotline

(DSN 551-1212) or GSA through supply channels for assistance. Personnel must note their findings and the source of confirmation on an Air Force Technical Order (AFTO) Form 36**, Maintenance Record for Security Type Equipment** (available on the AFEPL), and retain that record in the container. *[Reference DoD 5200.1-R, Paragraph 6-401]*

5.20. Storage of Classified Information. ***[Reference DoD 5200.1-R, Paragraph 6-402]***

5.20.1. Storage of Secret Information. In addition to the methods used for protecting Secret information described in DoD 5200.1-R, paragraph 6-402b, Secret information may be stored in an open storage area provided security-in-depth exists (see paragraph **5.20.2.**), and one of the following supplemental controls is used:

5.20.1.1. The open storage area shall be subject to continuous protection by cleared guard or duty personnel;

5.20.1.2. Cleared guard or duty personnel shall inspect the open storage area once every four hours; or

5.20.1.3. An intrusion detection system (IDS) meeting the requirements of DoD 5200.1-R, Appendix G with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

5.20.1.4. (Added-SMC) SMC/AXP is the approval authority for construction/modification of unattended collateral classified storage areas, secure storage rooms and vault-type rooms. All such plans will be coordinated with SMC/AXP prior to use. Initial requests for certification will be accomplished via a letter from the requesting organization. Unattended classified storage areas will meet, as a minimum, the physical security standards identified in DoD 5200.1-R, Appendix G. Upon approval, a Secure Storage Room Certificate will be issued to the requesting organization, to be posted within the certified area. Certification will be re-accomplished at a minimum, every three years.

5.20.2. Security-In-Depth. Security-in-depth can be one or more of the following security measures as long as they are adequate to prevent against unauthorized access: installation perimeter fence lines, entry control points, controlled and restricted area designations, base patrol coverage, and locked building. *[Reference DoD 5200.1-R, Paragraph 6-402 and Appendix B]*

5.20.3. Authority for Delineating the Appropriate Security Measures. If these requirements cannot be met because of local conditions, ISPMs determine alternative methods under the provisions of DoD 5200.1-R, paragraph 6-800. Military commanders do so when it occurs during a military operation as described in DoD 5200.1-R, paragraph 1-400. *[Reference DoD 5200.1-R, Paragraph 6-402d(1)]*

5.20.4. Replacement of Combination Locks. Commanders must ensure all combination locks on GSA approved security containers and doors are replaced with those meeting Federal Specification FF-L-2740 starting with those storing the most sensitive information according to the priority matrix in DoD 5200.1-R, Appendix G. There is no deadline for completing this effort, as it was initially an unfunded requirement. However, commanders must pursue funding and implement the retrofits as soon as possible. *NOTE:* Commanders will designate security containers at locations identified for closure as a low priority for replacing locks when there is a strong possibility that the security containers will not be used at another location. *[Reference DoD 5200.1-R, Paragraph 6-402e]*

5.20.4.1. (Added-SMC) Security containers with a built in Sergeant & Green leaf or Mosler locking devices may continue to be used to store SECRET and CONFIDENTIAL information until the locking device becomes inoperative; i.e., due to wear & tear or a lockout. Organizations must install the MAS-Hamilton X-08 or other certified mechanical locking mechanism IAW Federal Specification FF-L-2740 in order to store classified information. Classified security containers storing TOP SECRET and/or Special Access Program (SAP) information must install the

MAS-Hamilton X-08 locking mechanism or equivalent locking device IAW Federal Specification FF-L-2740.

5.21. Use of Key Operated Locks. *[Reference DoD 5200.1-R, Paragraph 6-402f(1)]*

5.21.1. The authority to determine the appropriateness of using key operated locks for storage areas containing bulky Secret and Confidential material is delegated to the chief of the activity having this storage requirement. When key operated locks are used, the authorizing official will designate lock and key custodians.

5.21.2. Lock and key custodians use AF Form 2427, **Lock and Key Control Register** (available on the AFEPL), to identify and keep track of keys.

5.22. Procurement of New Storage Equipment. *[Reference DoD 5200.1-R, Paragraph 6-403]*

5.22.1. Requesters of exceptions send their requests through command ISPM channels to HQ USAF/XOFI. HQ USAF/XOFI will notify OASD(C3I) of the exception. ***[Reference DoD 5200.1-R, Paragraph 6-403a]***

5.22.2. See AFMAN 23-110, Volume II, *Standard Base Supply Customer's Procedures. [Reference DoD 5200.1-R, Paragraph 6-403b]*

5.23. Equipment Designations and Combinations.

5.23.1. See AFMAN 14-304 for guidance on marking security containers used to store SCI. *[Reference DoD 5200.1-R, Paragraph 6-404a]*

5.23.2. Personnel will use SF Form 700, **Security Container Information** (available through the Air Force Publications Distribution system), for each vault or secure room door and security container, to record the location of the door or container, and the names, home addresses, and home telephone numbers of the individuals who are to be contacted if the door or container is found open and unattended. Personnel will affix the form to the vault or secure door or to the inside of the locking drawer of the security container. *[Reference DoD 5200.1-R, Paragraph 6-404b(3)]*

5.23.3. When SF Form 700, Part II, is used to record a safe combination, it must be:

5.23.3.1. Marked with the highest classification level of material stored in the security container; and,

5.23.3.2. Stored in a security container other than the one for which it is being used.

5.24. Repair of Damaged Security Containers. *[Reference DoD 5200.1-R, Paragraph 6-405]*

5.24.1. Locksmiths must either have a favorable National Agency Check or must be continuously escorted while they are repairing security containers. See guidance for unescorted entry to restricted areas in AFI 31-501.

5.24.2. The Naval Facilities Engineering Service Center Technical Data Sheet (TDS) 2000-SHR can be obtained from the Naval Facilities Engineering Services Center (NFESC), 1100 23rd Avenue, Code ESC66, Port Hueneme, California 93043-4370. *[Reference DoD 5200.1-R, Paragraph 6-405b]*

5.24.3. Personnel who have had their GSA approved security containers repaired, must have the locksmith confirm that the container still meets GSA standards. If there is doubt, personnel may contact

the DoD Lock Hotline managed by NFESC (DSN 551-1212) or GSA through supply channels for assistance. Personnel must note their findings and the source of confirmation on an AFTO Form 36 and retain that record in the container.

5.25. Maintenance and Operating Inspections. Personnel will follow maintenance procedures for security containers provided in Air Force Technical Order (AFTO) 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*. *[Reference DoD 5200.1-R, Paragraph 6-406]*

5.25.1. (Added-SMC) Any Civil Service Job Series 0080 security specialist or military AFSC equivalent can perform preventive maintenance inspections on approved GSA security containers as required by AFTO 00-20F-2, Inspection and Preventive Maintenance Procedures for Classified Storage Containers. The inspection is conducted following instructions in paragraph 7 of the AFTO. Record the inspection on AFTO Form 36, Maintenance Record for Security Type Equipment.

5.26. Reproduction of Classified Material.

5.26.1. Unit commanders and staff agency chiefs and Air Staff and Secretariat directors designate equipment for reproducing classified material.

5.26.2. Information managers approve equipment and issue procedures for clearing copier equipment of latent images.

5.26.3. Unit security managers:

5.26.3.1. Post equipment approved for copying classified material;

5.26.3.2. Develop security procedures that ensure control of reproduction of classified material; and,

5.26.3.3. Ensure personnel understand their security responsibilities and follow procedures.

5.27. Control Procedures. Unit commanders and staff agency chiefs designate people/positions to exercise reproduction authority for classified material in their activities. Also see DoD 5200.1-R, paragraph 6-309, and paragraph **5.18.** of this AFI. *[Reference DoD 5200.1-R, Paragraph 6-502]*

Section 5D—Disposition and Destruction of Classified Material

5.28. Retention of Classified Records.

5.28.1. Personnel follow the disposition guidance in AFMAN 37-139. *[Reference DoD 5200.1-R, Paragraph 6-700a]*

5.28.2. Information Security Program Managers will ensure that management of retention of classified material is included in oversight and evaluation of program effectiveness. *[Reference DoD 5200.1-R, Paragraph 6-700b]*

5.28.3. Unit commanders and staff agency chiefs will designate a “clean-out day” once a year to ensure personnel are not retaining classified material longer than necessary. *[Reference DoD 5200.1-R, Paragraph 6-700b]*

5.28.3.1. (Added-SMC) The second Thursday of March is the annual clean-out day for SMC organizations.

5.29. Methods and Standards. *[Reference DoD 5200.1-R, Paragraph 6-701b]*

5.29.1. Personnel may obtain information on GSA specifications for equipment and standards for destruction of other than electronic media and the like from the local supply office.

5.29.1.1. (Added-SMC) Before procuring any destruction equipment, contact SMC/AXP for the NSA Approved Destruction Devices list used for classified information. Mark it with "Unauthorized Shredder for Classified Destruction" or "Authorized Shredder for Classified Destruction" on the destruction equipment.

5.29.1.2. (Added-SMC) SMC/AXP established procedures for use of the Los Angeles Air Force Base destruction equipment located in Building 100. The equipment is capable of destroying paper products, communication tapes, carbon paper, ribbons, film, microfilm, microfiche, floppy disks and magnetic cards. Contact AXP to schedule an appointment to use the base destruction equipment.

5.29.2. Records of Destruction.

5.29.2.1. Top Secret. TSCOs will ensure:

5.29.2.1.1. Two people with Top Secret access are involved in the destruction process;

5.29.2.1.2. Destruction is recorded on one of these forms: AF Form 143; AF Form 310; or, AF Form 1565, **Entry, Receipt, and Destruction Certificate**; and,

5.29.2.1.3. The destruction record is attached to the AF Form 143 (used to account for the document) when the destruction is not recorded on the AF Form 143 itself.

5.29.2.2. Secret and Confidential. A record of destruction is not required but an appropriately cleared person must be involved in the destruction process.

5.29.2.3. Foreign Government Information. See DoD 5200.1-R, Chapter 6, Section 6, for destruction of foreign government information.

5.29.2.4. Destruction of AIS Media. Dispose of AIS media according to AFSSI 5020, *Remanence Security*.

5.29.2.5. Disposition of Destruction Records. Dispose of destruction records according to AFMAN 37-139.

Section 5E—Alternative or Compensatory Control Measures

5.30. General. *[Reference DoD 5200.1-R, Paragraph 6-800]*

5.30.1. The authority to approve alternative or compensatory security controls is delegated to the ISPM. ISPMs will forward a copy of documentation through command ISPM channels to HQ USAF/XOFI. The documentation must describe the thought process that led up to the decision. *[Reference DoD 5200.1-R, Paragraph 6-800a]*

5.30.1.1. ISPMs may use AF Form 116, **Request for Deviation from Security Criteria** (available on the AFEPL), to document the scenario and approval.

5.30.2. The Air Force doesn't authorize use of security controls listed in DoD 5200.1-R, paragraph 6-800c. *[Reference DoD 5200.1-R, Paragraph 6-800c]*

5.30.3. Send requests to use alternative or compensatory security controls for the safeguarding of NATO or foreign government information through command ISPM channels to HQ USAF/XOFI. *[Reference DoD 5200.1-R, Paragraph 6-800f]*

Chapter 6

TRANSMISSION AND TRANSPORTATION

Section 6A—Methods of Transmission or Transportation

6.1. General Policy.

6.1.1. Handcarrying Classified Material During Temporary Duty (TDY) Travel. Handcarrying classified material during TDY poses a risk and should be done as a last resort in critical situations. Whenever possible, personnel will use standard secure methods for relaying the data, e.g., mail through secure channels or through approved secure electronic means. Authorizing officials must assess the risk before authorizing the handcarrying of classified material. Some factors to consider during the risk assessment process are:

6.1.1.1. The environment in which the material will be handcarried. Consider the chances of the material being apprehended by unauthorized personnel. The servicing Air Force Office of Special Investigations office should be able to assist in determining the risks associated with the environment.

6.1.1.2. The sensitivity of the information. Consider the damage it could cause the United States if the information was compromised.

6.1.1.3. The availability of authorized facilities for storing the classified during overnight layovers, at the TDY location, etc. Consider storing the material at a U.S. military installation or other government facility.

6.1.2. Laptop Computers are High Risk. Because of their commercial value, laptop computers are an especially high risk when used to transport classified information. When using laptops to handcarry classified information, couriers must ensure both laptop and disks are prepared according to paragraph **6.6.5.** In addition, as required for all classified material, couriers must take special care to ensure laptops and disks are kept under constant surveillance or in secure facilities/containers at all times.

6.1.3. Air Force Office of Primary Responsibility for Transmission and Transportation Policy. HQ USAF/XOFI establishes Air Force procedures for transmission and transportation of classified information and material. *[Reference DoD 5200.1-R, Paragraph 7-100a]*

6.1.4. Transmitting Classified Material by Pneumatic Tube Systems. Installation commanders approve the use of pneumatic tube systems and ensure that the equipment and procedures provide adequate security. *[Reference DoD 5200.1-R, Paragraph 7-100a]*

6.1.5. Transmitting COMSEC Information. Personnel may get information about transmitting and transporting COMSEC information through their local COMSEC manager. *[Reference DoD 5200.1-R, Paragraph 7-100b]*

6.1.6. Releasing Other Agency Information Outside of the Department of Defense. Personnel go direct to owners of other agency information to request permission to release the information outside the Department of Defense. *[Reference DoD 5200.1-R, Paragraph 7-100d]*

6.1.7. (Added-SMC) Commanders will designate in their unit security operating instruction internal Official Mail Distribution Points within their organizations.

6.2. Transmitting Top Secret Information. *[Reference DoD 5200.1-R, Paragraph 7-101]*

6.2.1. Electronic Means. Personnel will get information about transmitting Top Secret information via electronic means from their Information Assurance Office. *[Reference DoD 5200.1-R, Paragraph 7-101b]*

6.2.2. DoD Component Courier Service. The Air Force does not have its own courier service. *[Reference DoD 5200.1-R, Paragraph 7-101d]*

6.2.3. Department of State Diplomatic Courier Service. Personnel who need to transport classified material use the Department of State courier system when: *[Reference DoD 5200.1-R, Paragraph 7-101e]*

6.2.3.1. Transmitting any classified material through or within countries hostile to the United States or any foreign country that may inspect it.

6.2.3.2. Transmitting Top Secret material to an installation serviced by diplomatic pouch. Personnel can find out if they are serviced by diplomatic pouch through their local military postal office.

6.3. Transmitting Secret Information. *[Reference DoD 5200.1-R, Paragraph 7-102]*

6.3.1. Also see AFI 31-601. *[Reference DoD 5200.1-R, Paragraph 7-102b]*

6.3.2. The Air Force authorizes the use of the current holder of the General Services Administration contract for overnight delivery of Secret information in urgent cases and when the transmission is between DoD Components within the United States and its Territories. This applies to locations in Alaska, Hawaii, and Guam when overnight delivery is possible. OASD(C3I) has already ensured the conditions cited in DoD 5200.1-R, paragraph 7-102c, have been met. *[Reference DoD 5200.1-R, Paragraph 7-102c]*

6.3.3. For more information on protective security service carriers, see DoD 5220.22-R, *Industrial Security*, AFI 31-601, and AFPD 24-2, *Preparation and Movement of Air Force Material. [Reference DoD 5200.1-R, Paragraph 7-102h]*

6.3.4. Also see guidance in DoD 5200.1-R, paragraph 7-104. *[Reference DoD 5200.1-R, Paragraph 7-102j]*

6.4. Transmitting Confidential Information. *[Reference DoD 5200.1-R, Paragraph 7-103]*

6.4.1. Since first class mail bearing the "Postmaster" notice is an option for transmitting Confidential material, recipients must protect it as Confidential material unless they determine the contents are unclassified. ***EXCEPTION:*** First class mail bearing the notice awaiting distribution at the Base Information Transfer Center (BITC). At this point, such mail will be handled the same as all other First Class Mail.

6.4.1.1. The outer envelope or wrapper shall be endorsed with "Return Service Requested" instead of "POSTMASTER: Do Not Forward."

6.4.1.2. (Added-SMC) Use an opaque pouch, brief case or similar outer container when handcarrying classified information on Los Angeles AFB. This procedure includes message pickup and delivery from/to the Communications Center. Protect classified material with an appropriate cover

sheet while in transit on Los Angeles AFB. Do not mark the exterior pouch/container with classified markings.

6.5. Transmission of Classified Material to Foreign Governments. *[Reference DoD 5200.1-R, Paragraph 7-104]*

6.5.1. Also see AFI 31-601 and AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations. [Reference DoD 5200.1-R, Paragraph 7-104a]*

6.5.2. Personnel may not ship US classified material from a US industrial activity to a foreign entity. *[Reference DoD 5200.1-R, Paragraph 7-104a]*

6.5.3. (Added-SMC) Coordinate with SMC/AXP prior to transmitting any classified material or unclassified controlled information to a foreign government.

Section 6B—Preparation of Material for Transmission

6.6. Envelopes or Containers. *[Reference DoD 5200.1-R, Paragraph 7-200]*

6.6.1. Personnel may use AF Form 2595, **Classified Protection Insertion Sheet**, as a countermeasure for the possible threat posed by the chemical composition referred to as "Liquid Window." *[Reference DoD 5200.1-R, Paragraph 7-200a]*

6.6.1.1. (Added-SMC) When transmitting classified material ensure the inner container is marked with any additional warning notices that appear on the document. This avoids the possibility that unauthorized individuals will access the material.

6.6.2. For the purpose of this policy, an activity is a facility. *[Reference DoD 5200.1-R, Paragraph 7-200a(5)]*

6.6.3. Personnel do not use an outer container when entering Secret and below material into the BITC. The pouch is considered the outer container.

6.6.4. Receipts. See receipting requirements at paragraph **5.10.1.1.**

6.6.4.1. Senders trace receipts when they're not acknowledged:

6.6.4.1.1. Within 30 days for material sent within continental United States (CONUS).

6.6.4.1.2. Within 45 days for material sent outside CONUS.

6.6.4.2. The recipient must immediately date, sign, correct, and return the receipt to the sender.

6.6.4.3. If recipients do not return the receipt and confirm they have not received the material, the sending activity must initiate security incident procedures according to **Chapter 9** of this AFI.

6.6.5. Laptop Computer and Disk Preparation Requirements. Couriers must ensure that:

6.6.5.1. Laptops and disks are both password protected.

6.6.5.2. Laptops and disks are marked according to DoD 5200.1-R, Paragraphs 5-407, 5-408, and 5-409a and b.

6.6.5.3. Removable disks are separated from the computer and are double wrapped according to this AFI, **Section 6B**, and DoD 5200.1-R, paragraph 7-200.

6.6.5.4. Laptops have an outer container when the classified data is stored in the internal memory or maintained on fixed storage media.

6.6.5.5. Laptops and disks containing classified information are kept under constant surveillance or stored in secure containers/facilities.

Section 6C—Escort or Handcarrying of Classified Material

6.7. General Provisions. *[Reference DoD 5200.1-R, Paragraph 7-300]*

6.7.1. Authorization. *[Reference DoD 5200.1-R, Paragraph 7-300a(3)]*

6.7.1.1. The unit commander, staff agency chief, or security manager authorizes appropriately cleared couriers to handcarry classified material on commercial flights. See DoD 5200.1-R, paragraph 7-301, for required documentation and this AFI, paragraph **6.1.2.**, for a cautionary statement regarding handcarrying classified material.

6.7.1.2. The unit commander, staff agency chief, or security manager authorizes appropriately cleared couriers to handcarry classified material by means other than on commercial flights.

6.7.2. Security managers or supervisors brief each authorized member handcarrying classified material. *[Reference DoD 5200.1-R, Paragraph 7-300b]*

6.7.3. Each Air Force activity or unit that releases classified material to personnel for handcarrying: *[Reference DoD 5200.1-R, Paragraph 7-300b(8)(c)]*

6.7.3.1. Maintains a list of all classified material released.

6.7.3.2. Keeps the list until they confirm all the material reaches the recipient's activity or unit.

6.8. Documentation. Unit commanders, staff agency chiefs, and security managers issue and control DD Form 2501, **Courier Authorization** (available through the Air Force Publications Distribution system), for handcarrying classified material by means other than on commercial flights. This doesn't preclude the use of a courier authorization letter for infrequent courier situation (see paragraph **6.7.1.2.** of this AFI). ***EXCEPTION:*** Documentation is not necessary when handcarrying classified information to activities within an installation (i.e., Air Force installation, separately located missile field). ***NOTE:*** Account for DD Form 2501 as prescribed in AFI 37-161, *Distribution Management.* *[Reference DoD 5200.1-R, Paragraph 7-301]*

6.8.1. (Added-SMC) Personnel handcarrying classified information within the confines (Areas A, B, & Aerospace complex) of Los Angeles AFB remain subject to exit/entry inspections when passing through controlled area entry points. To expedite an individual's movement during these checks, provide written authorization to personnel who regularly handcarry information/material. Use DD Form 2501, Courier Authorization Card, or a courier letter signed by the program director, chief of staff agency or security manager. The DD Form 2501 will be stored within the organization when not utilized by authorized personnel.

6.8.2. (Added-SMC) An official courier letter to handcarry classified information/material and an exemption notice affixed to the package is required when an individual will be departing the confines of Los Angeles AFB. Courier letters must include the individual's full name, social security number, organization, description of packages (i.e., how many, size, addresses, etc.), the point of contact and phone number for verifying the information and an expiration date. The exemption notice must

include the organizations full address, official business, the notation that this information is exempt from examination, and the program director, chief of staff agency, or security manager's signature. (see **FIGURE 6.1 (Added)** for an example of a courier letter and **FIGURE 6.2 (Added)** for an example of an exemption notice).

6.9. Handcarrying or Escorting Classified Material Aboard Commercial Passenger Aircraft. *[Reference DoD 5200.1-R, Paragraph 7-302a(e)]***.**

6.9.1. The expiration is not to exceed 7 days from the date of issue.

6.10. (Added-SMC) Transmitting NATO Classified Information . (Reference AFI 31-406, Chap 6, 1 April 00)

6.10.1. (Added-SMC) Requests to handcarry NATO classified information outside the continental United States aboard commercial aircraft must be forwarded through SMC/AXP for approval.

6.10.2. (Added-SMC) All incoming and outgoing NATO Classified information must go through NATO Control Point. Space Command will send the NATO documents directly to the action offices as applicable.

6.10.3. (Added-SMC) When NATO classified information is permanently transmitted outside your activity; use an AF From 310, Document Receipt and Destruction Certificate. For documents loaned out on a temporary basis record the location, date signed out, and the name and address of the individual (on loan basis should be no longer than 72 hours). Maintain records of accountability for two (2) years.

FIGURE 6.1 (Added-SMC) SAMPLE COURIER LETTER

MEMORANDUM FOR (ORGANIZATION)

FROM: (ORGANIZATION)

SUBJECT: Designation of Official Courier Letter

1. Mr. Albert Johnson, SSAN: 122-69-9932, 412 TW/FG, Edwards AFB, California 93524-0001, is designated an official courier for the United States Government. Upon request, he will present official identification.

2. Mr. Johnson is handcarrying four sealed packages, size 9" X 8" X 24" addressed from 2420 Vela Way, Suite 1467, Los Angeles AFB, El Segundo, California 90245-4659, and addressed to HQ AFSPC, 18 Mellow Drive, Peterson AFB, CO 45433-0002. Each package is identified on the outside of the package with the marking "OFFICIAL BUSINESS – MATERIAL EXEMPTED FROM EXAMINATION" bearing the signature of the undersigned.

3. Mr. Johnson is departing Los Angeles International Airport with a final destination to Dayton International Airport. He has a transfer point of Dallas-Fort Worth International Airport.

4. This courier designation can be confirmed by contacting the undersigned at 412 TW/FG, area code (805) 277-1111. This letter expires on (date of return to Los Angeles AFB).

(signature of program director, chief of staff
agency, or security manager)

FIGURE 6.2 (Added-SMC) EXEMPTION NOTICE

Department of the Air Force Space Missile Command Los Angeles AFB, California Official Business MATERIAL EXEMPT FROM EXAMINATION (Program Director, Director/Chief of Staff Agency or Security Manager)

Chapter 7

SPECIAL ACCESS PROGRAMS

7.1. Control and Administration. *[Reference DoD 5200.1-R, Paragraph 8-102c]*

7.1.1. The Office of the Director for Security and Investigative Programs (SAF/AAZ) administers special access programs for the Air Force. See AFPD 16-7, *Special Access Programs.* ***EXCEPTION:*** HQ USAF/XOI controls SCI programs.

7.1.1. (SMC) With the exception of SMC/IN, who controls all SCI Programs for Los Angeles AFB, to include tenant organizations, any SMC organization contemplating establishing a Special Access Program must coordinate with SMC/AXP prior to contacting external SMC organizations.

7.2. Code Words and Nicknames. Unit commanders, heads of staff agencies, or acquisition system program directors: *[Reference DoD 5200.1-R, Paragraph 8-103d(2)]*

7.2.1. Obtain code words and nicknames through channels from the servicing control point (normally, the MAJCOM, FOA, DRU Information Management activity).

Chapter 8

SECURITY EDUCATION AND TRAINING

Section 8A— Policy

8.1. General Policy. 8 Effective information security training is a cornerstone of the Air Force (AF) Information Security Program. All Air Force personnel need information security training whether they have access to classified information or not. All AF personnel are personally and individually responsible for protecting the national interests of the United States. All security infractions and/or violations must be immediately reported, circumstances examined and those responsible held accountable and appropriate corrective action taken. Commanders are responsible for ensuring that personnel are knowledgeable and understand their responsibility to protect information and resources deemed vital to national security. **NOTE**: For the purpose of this chapter, the term *commander* encompasses staff agency chief and director, when applicable.

8.2. Methodology. The AF will provide information security training to its personnel and contractors, as appropriate, on a continuous basis using government and commercial training sources. Various training methods will be used to administer training, such as classroom instruction, one-on-one, computer-based, and other distant learning training media. The AF will maintain a cadre of trained professional career security personnel and security managers to administer, implement, and measure the program's effectiveness. When funds and resources permit, professional security personnel and security managers should attend in-residence type training courses.

8.3. Roles and Responsibilities.

8.3.1. These roles and responsibilities are in addition to those listed in paragraph **1.3.**

8.3.2. The Air Force Security Forces Center, Security Forces Training (AFSFC/SFWT), is responsible for developing Air Force specific information security training course materials, curriculums and awareness products.

8.3.3. Commanders are responsible for implementing the information security training program, developing supplemental training tools, and assessing the health of their programs on a continuous basis. In addition, commanders will:

8.3.3.1. Ensure appointed security managers receive training within 90 days of their assignment and that the training is annotated in the individual's official personnel file (OPF) or military training record.

8.3.3.2. Budget for security awareness training products, materials, and the formal training of security managers.

8.3.3.3. Actively support and monitor security education training.

8.3.3.4. Ensure records are maintained on a calendar year basis of personnel attending initial, refresher and specialized information security training. As a minimum, these records must reflect the date(s) training was conducted and the number of personnel in attendance.

8.3.4. Supervisors will conduct and/or ensure personnel receive training as required by this instruction, document it when required, and ensure credit is given for course completion or briefing attendance, if appropriate.

8.3.5. ISPMs at all levels are responsible for:

8.3.5.1. Developing and overseeing implementation of information security training programs.

8.3.5.2. Assessing the effectiveness of training programs annually.

8.3.5.3. Developing and conducting classroom or one-on-one training for newly appointed security managers. Professional security personnel serving in security manager and/or security officer capacities must also receive this training.

8.3.5.4. Developing and distributing generic information security training lesson plans, which cover the basic information security work-center components (information, personnel and industrial security programs) to include installation specific security requirements.

8.3.5.5. Assisting security managers in the development of unit specific lesson plans, motivational materials and training aids.

8.3.5.6. Publicly recognizing the training efforts of effective security managers.

8.3.5.7. Providing civilian employees who complete information security managers training with a certificate, which they can use to enter course completion into their OPF.

8.3.5.8. Providing military supervisors with the names of military personnel appointed security manager duties that complete the security manager training course. This training will be annotated into the individual's on-job-training (OJT) record and other official records, as appropriate.

8.3.6. Unit Security Managers are responsible for:

8.3.6.1. Ensuring security training is conducted as outlined in this AFI.

8.3.6.2. Developing organizational specific security lesson plans.

8.3.6.3. Advising the commander on the status of the unit's security training program.

8.3.6.4. Ensuring training is documented and records are properly maintained, if applicable.

8.3.6.5. (Added-SMC) Use the SMC Security Education & Training Guide, January 2001 to help conduct and satisfy quarterly security education training requirements.

Section 8B—Initial Security Orientation

8.4. Cleared Personnel.

8.4.1. Initial Training. Supervisors and security managers provide initial training to all cleared personnel. Supervisors are responsible for ensuring that their cleared personnel receive an initial security education orientation before they access classified information.

8.4.1.1. Initial training should ensure cleared personnel are knowledgeable of their security responsibilities as related to their jobs and the organization's mission.

8.4.1.2. As a minimum, initial information security training for cleared personnel will address the following:

8.4.1.2.1. Subjects, material and/or areas as indicated in **Attachment 7**, AF Information Security Program Training Standard, under column heading (C) for cleared personnel.

8.4.1.2.2. When prior personnel security investigations and/or determinations are acceptable.

8.4.1.2.3. What derogatory/unfavorable information or suspicious activities by other cleared personnel that must be immediately reported to the commander or staff agency chief.

8.4.1.2.4. What the personnel security clearance verification, access and safeguarding requirements are when on-base cleared DOD contractors require access to classified information in support of classified contracts.

8.4.1.2.5. What the marking and safeguarding requirements are for protecting unclassified controlled information.

8.5. Uncleared Personnel.

8.5.1. Supervisors and security managers provide training to uncleared personnel. Supervisors are responsible for ensuring that all uncleared personnel receive an initial security education orientation within 90 days of assignment to the unit.

8.5.1.1. Initial orientation training must ensure that uncleared personnel are knowledgeable of their responsibilities and roles in the Air Force Information Security Program.

8.5.1.2. As a minimum, initial security education orientation training for uncleared personnel will address/cover the following:

8.5.1.2.1. Subjects, areas and/or materials identified in **Attachment 7**, AF Information Security Program Training Standards, under column heading (U) for uncleared personnel.

8.5.1.2.2. The identity of the installation Information Security Program Manager (ISPM) official and unit security manager and their respective responsibilities.

8.5.1.2.3. The different levels of classified information and why it is important to protect it.

8.5.1.2.4. The procedures to follow should classified information be discovered unprotected or to report other potential security incidents.

8.5.1.2.5. The requirements for the marking and safeguarding of sensitive unclassified, controlled unclassified and "For Official Use Only" information.

Section 8C—Special Requirements

8.6. Original Classification Authorities (OCAs). The ISPMs are responsible for administering specialized training to Original Classification Authorities (OCAs) in accordance with DOD 5200.1-R, *Information Security Program*. Training must be conducted prior to OCA authority being exercised. ISPMs may either develop their own training or administer/use the Defense Security Service (DSS) OCA or equivalent training product. The specialized OCA training is in addition to the requirements of **Attachment 7**, AF Information Security Program Training Standard, under column heading (C) for cleared personnel.

8.7. Declassification Authorities Other Than Original Classification Authorities. The ISPMs are responsible for administering this specialized training in accordance with DOD 5200.1-R. Training must be conducted before the declassification authority makes any declassification decisions.

This specialized training is in addition to the "cleared personnel" requirements of **Attachment 7**, Air Force Information Security Program Training Standards.

8.8. Derivative Classifiers, Security Personnel and Others.

8.8.1. Derivative Classifiers. Commanders are responsible for ensuring that derivative classifiers are adequately trained in accordance with DOD 5200.1-R. ISPMs will assist security managers in acquiring or developing the appropriate lesson plans and training materials.

8.9. Professional Security Personnel and Security Managers.

8.9.1. Professional Security Personnel and Security Managers. Commanders ensure professional security career personnel and security managers receive training as follows:

8.9.1.1. Subjects, material and/or areas as indicated in **Attachment 7**, Air Force Information Security Program Training Standard, under column heading (S) for security personnel.

8.9.2. Professional Security Career Personnel.

8.9.2.1. Civilians. See AFMAN 36-202, Volume 2, *Air Force Civilian Career Planning*, paragraph 3-16, Security Career Program Master Development Plan (MDP). An AF/DPKCS, Security Career Program Administrator, enhanced/modified version of the MDP can be obtained from the MAJCOM, FOA, or DRU civilian security career program coordinator normally located on the ISPM's staff. A copy can also be obtained by accessing the Air Force Personnel Center Web Site at **http//www.afpc.randolph.af.mil.**, Security Career Program.

8.9.2.2. Military. See requirements for award of Special Experience Identifier (SEI) 322 in AFMAN 36-2108, *Airman Classification*. Also use the Civilian Security Career Program Master Development as a guide for determining additional training.

8.9.3. Security Managers.

8.9.3.1. The ISPM provide training too newly appointed security managers within 90 days of their assignment. Although not mandatory, unit commanders may fund and send their appointed security managers to the DSS in-resident Information Security Management Course or an equivalent AF approved course. Other commercial training sources may be used to provide this training when approved by the MAJCOM.

8.9.3.2. As a minimum, appointed security managers will be administered initial classroom or one-on-one training in accordance with **Attachment 7**. This training must equip the appointees with a workable knowledge and understanding of information security, personnel security and industrial security program mandates, including security access requirement (SAR) unit manpower document (UMD) position coding.

8.9.3.3. Commanders ensure civilians performing these duties receive the appropriate skill coding in their personnel records according to AFMAN 36-505, *Skill Coding*.

8.9.4. Training Costs. Commanders must budget annually for their information security program training needs (training course attendance, educational materials, awareness media, etc.).

8.10. Other Program Related Training Requirements.

8.10.1. ISPMs will identify training requirements for those security disciplines and/or areas for which they are responsible.

8.10.2. Commanders must ensure that training is properly documented in the individual's official personnel records and ensure personnel receive credit for attending and completing courses, if applicable.

8.10.3. Document training as outlined in AFPD 36-22, *Military Training,* AFI 36-2201, *Developing, Managing, and Conducting Training,* and AFPAM 36-2211, *Guide for Management of Air Force Training Systems.*

8.10.4. The following programs have security related training requirements:

8.10.4.1. Sensitive Compartmented Information (SCI).

8.10.4.1.1. The Special Security Officer (SSO) or designee conducts SCI security awareness training quarterly for personnel accessed to SCI. *[Reference DOD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual, Chapter 2, paragraph 12, and AFMAN 14-304, The Security, Use, and Dissemination of Sensitive Compartmented Information, Chapter 12]*

8.10.4.1.2. In addition, personnel granted SCI access will receive an annual briefing on their continuing responsibilities. *[Reference DOD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual, Chapter 2 and AFMAN 14-304, paragraph 12.3]*

8.10.4.2. Operations Security (OPSEC). A designated official conducts OPSEC training within 90 days of an individual's arrival and/or assignment. *[Reference AFI 10-1101, Operations Security, paragraph 4.4.1.]*

8.10.4.3. Information Protection Security Awareness Training and Education (SATE).

8.10.4.3.1. The SATE program is a single, integrated information assurance awareness, training, and education effort. All Air Force military and civilian and contractors who use Air Force information systems must complete IA training annually, and be so certified. This training and certification is accomplished by an IA Intranet-Based (ITB) Training and certification system. *[Reference AFI 33-204, Information Protection Security Awareness, Training and Education (SATE) Program.]*

8.10.4.3.2. A designated official conducts initial SATE training within 60 days of an individual's assignment and training on a recurring basis annually thereafter. Initial and recurring training must be at least one hour in duration. *[Reference AFI 33-204, paragraph 6.1.1.]*

8.10.4.3.3. Personnel that do not require access to or use information systems in the performance of duties are exempt from the initial and recurring one-hour awareness-training requirement. *[Reference AFI 33-204, paragraph 6.1.2.]*

8.10.4.4. Counterintelligence Awareness and Briefing Program. The servicing Air Force Office of Special Investigations (AFOSI) Detachment provides counterintelligence awareness briefings to AF personnel. *[Reference AFCAT 36-2223]*

8.10.4.4.1. After initial training, refresher training is provided every three years thereafter.

8.10.4.4.2. Document initial and refresher in accordance with AFCAT 36-2223.

8.10.4.5. Protection from Terrorism. The designated official provides military personnel training within 180 days of deployment (PCS/TDY to overseas location) and provides civilians training

shortly after their initial hiring. Frequency of refresher training is at the discretion of the MAJCOM. *[Reference AFI 31-210, The Air Force Antiterrorist (AT) Program]*

8.10.4.6. (Added-SMC) Foreign Travel. Security Managers must provide a foreign travel briefing to individuals who perform personal foreign travel. The Foreign Travel Program should consist of reporting procedures, applicable threat information and briefing/debriefing requirements. The Det 110, AF Office of Special Investigations can assist organizations by furnishing applicable threat information.

Section 8D—Continuing Security Education/Refresher Training

8.11. Continuing and Refresher Training.

8.11.1. Commanders ensure that each person receives continuing training throughout their duty assignment.

8.11.1. (SMC) Because of the volume of information to be covered, recurring and refresher training should, as a minimum, be presented in semiannual sessions. Quarterly sessions are recommended for maximum motivational and retentive effect.

8.11.1.1. Cleared and uncleared personnel will receive refresher Classified National Security Information related training annually in accordance with **Attachment 7**.

8.11.1.2. Personnel performing specialized Classified National Security Information program related functions, such as, classification, declassification and derivative classification actions and security personnel, etc., will receive refresher training commensurate with their knowledge and proficiency in performing required tasks and the dissemination of new policy guidance.

8.11.2. Tailor training to mission needs and design it to address an individual's security responsibilities.

8.11.3. Continuing training must include ensuring individuals have the most current security guidance applicable to their responsibilities.

8.11.4. Other related material to be considered include a general overview of the unclassified controlled information, foreign disclosure, security and policy review processes and protection requirements.

Section 8E—Access Briefings and Termination Debriefings

8.12. Access Briefings.

8.12.1. Supervisors, security managers or designated officials conduct and document the following access briefings, as appropriate:

8.12.1.1. Brief and execute the SF-312, **Classified Information Nondisclosure Agreement**, prior to granting an individual access to classified information. The SF-312 may also be used to document attestations. *[Reference AFI 31-401, paragraph **5.4.**]*

8.12.1.2. Brief and execute the DD Form 2501, **Courier Authorization**, when an individual is authorized to escort or handcarry classified information. *[Reference AFI 31-401, paragraph **6.7.**]*

8.12.1.3. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to NATO classified information. *[Reference AFI 31-406, paragraph 4.9.]*

8.12.1.4. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to Critical Nuclear Weapons Design Information (CNWDI). *[Reference AFI 31-401, paragraph **1.5.1.3.**]*

8.12.1.5. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to SIOP-ESI. *[Reference AFI 10-1102, paragraph 6.1.]*

8.12.1.6. The special security officer conducts the SCI indoctrination (inbrief) prior to granting personnel access to SCI. The indoctrination is recorded in the DD Form 1847, **Sensitive Compartment Information Indoctrination Memorandum**. The DD Form 1847-1, **Sensitive Compartment Information Nondisclosure Statement**, is also executed at this time. *[Reference DOD 5105.21-M-1, Chapter 2]*

8.13. Termination Debriefings.

8.13.1. Supervisors, security managers or designated officials conduct and document the following termination debriefings, as appropriate:

8.13.1.1. Debrief individuals having access to classified information or security clearance eligibility when they terminate civilian employment, separate from the military service, have their access suspended, terminated, or have their clearance revoked or denied.

8.13.1.2. Use AF Form 2587, **Security Termination Statement**, to document the debriefing.

8.13.1.3. The debriefing must emphasize to individuals their continued responsibility to:

8.13.1.3.1. Protect classified and unclassified controlled information to which they have had access.

8.13.1.3.2. Report any unauthorized attempts to gain access to such information.

8.13.1.3.3. Adhere to the prohibition against retaining material upon departure.

8.13.1.3.4. And the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

8.13.2. For NATO access termination debriefing, see AFI 31-406, *Applying NATO Protection Standards*, paragraph 4.10.

8.13.3. Commanders ensure personnel accessed to SCI receive a termination debriefing when access is no longer required, is suspended, or is revoked.

8.13.3.1. The Special Security Office (SSO) conducts the SCI termination debriefing.

8.13.3.2. SCI termination debriefing is documented on the DD Form 1848**, Sensitive Compartment Information Debriefing Memorandum**.

8.13.4. For SIOP-ESI termination briefing, see AFI 10-1102, **Safeguarding the Single Integrated Operational Plan (SIOP).**

8.13.5. Dispose of AF Form 2587 according to AFMAN 37-139.

8.14. Refusal to Sign a Termination Statement. When an individual willfully refuses to execute AF Form 2587, the supervisor, in the presence of a witness:

8.14.1. Debriefs the individual orally.

8.14.2. Records the fact that the individual refused to execute the termination statement and was orally debriefed.

8.14.3. Ensures the individual no longer has access to classified information.

8.14.4. Forwards the AF Form 2587 to the servicing ISPM for Security Information File (SIF) processing according to AFI 31-501.

8.14.4. (Added-SMC) Provide AF Form 2587 to SMC/AXP with signature of individuals.

Section 8F—Program Oversight

8.15. General.

8.15.1. Commanders are responsible for ensuring systems are set up to determine training requirements, develop training, and evaluate effectiveness of the training.Commanders are responsible for ensuring systems are set up to determine training requirements, develop training, and evaluate effectiveness of the training.

8.15.2. ISPMs will make security education and training a *special interest item* during annual program reviews.

8.15.3. Commanders will ensure that their security education and training program is given close scrutiny during inspections, self-inspections and staff assistance visits (SAVs).

8.15.4. Personnel that have program oversight responsibilities should use a combination of approaches to assess the effectiveness of the security education program, such as, observations, quizzes, surveys, face-to-face interviews, practical demonstrations, etc.

Section 8G—Coordinating Requests for Formal Training

8.16. Coordinating Requests for Training.

8.16.1. Commanders will ensure that requests for formal training are coordinated through unit, installation and MAJCOM training channels.

8.16.2. Requests for in-residence Defense Security Service (DSS) training courses will be processed in accordance with AFCAT 37-2223, **USAF Formal Schools**, regardless of funding method (AF or unit funded), except as stipulated in paragraph **8.16.3.**, below.

8.16.3. When a unit is willing to fund TDY expenses (travel, per-diem, etc.), out-of-cycle attendance at DSS in-residence training courses may be requested. If seating is available, requests will be filled on a first-come, first-serve basis. Submit requests through the MAJCOM to HQ USAF/XOFI (memo and DSS Registration Request) at least 30 days prior to the class start date. The commander's written approval is required. Once coordination has been completed and request approved, the unit will be notified. AF activities that host/sponsor formal on-site training courses or seminars will make them available to as many personnel as possible.

8.16.3. (SMC) SMC/AXP is the focal point for all host/sponsored on site security training for SMC organizations and will be coordinated with prior to conducting such training.

Chapter 9

ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

9.1. Policy. *[Reference DOD 5200.1-R, Chapter 10]*

9.1.1. It is Air Force policy that security incidents will be thoroughly investigated to minimize any possible damage to national security. The investigation will identify appropriate corrective actions that will be immediately implemented to prevent future security incidents. Further, if the security incident leads to the actual or probable compromise of classified information, a damage assessment will be conducted to judge the effect that the compromise has on national security.

9.2. Definitions.

9.2.1. Security incidents as used in this AFI pertain to any security violation or infraction as defined in EO 12958. Security incidents may be categorized as:

9.2.1.1. Security Violation. Any knowing, willful or negligent action:

9.2.1.1.1. That could reasonably be expected to result in an unauthorized disclosure of classified information.

9.2.1.1.2. To classify or continue the classification of information contrary to the requirements of this order or it's implementing directives.

9.2.1.1.3. To create or continue a special access program contrary to the requirements of EO 12958.

9.2.1.2. Security Infraction. Any knowing, willful or negligent action contrary to the requirements of EO 12958 that is not a security violation.

9.2.2. A compromise of classified information occurs when unauthorized individuals have had access to the classified information.

9.2.3. A probable compromise of classified information is when an investigating official concludes that a compromise of classified information has more than likely occurred as a result of a security incident.

9.3. Automated Information System (AIS) Deviations. Coordinate all security deviations involving AIS with the local ISPM and computer security personnel to begin an evaluation on the impact of the incident to national security and the organization's operations. If communication security (COMSEC) material is involved, refer to AFI 33-212, *Reporting COMSEC Deviations*.

9.4. Sensitive Compartmented Information (SCI) Incidents. To report SCI incidents refer to AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* (FOUO).

9.4. (SMC) Immediately report security incidents/violations involving Sensitive Compartmented Information (SCI) to SMC/INS.

9.5. Classification.

9.5.1. Classify security incident notices, appointment of inquiry official memorandums, and security incident reports at the same level of classification as the information compromised if they contain classified information or if they provide sufficient information that would enable unauthorized individuals to access the classified information in an unsecure environment. In the latter case, the documentation must remain classified until the information has been retrieved and appropriately safeguarded. Do not classify memorandums and reports pertaining to security incidents that have occurred in the AIS environment when the system has been appropriately purged and the correspondence does not contain other classified information.

9.5.1.1. Classify security incident notices, memorandums, and reports according to the classified source from which they are derived. Refer to DOD 5200.1-R, Chapter 3.

9.5.1.2. Mark security incident notices, memorandums, and reports using derivative classification procedures. Refer to DOD 5200.1-R, Chapter 5.

9.5.2. All security incident reports will, as a minimum, be marked "For Official Use Only." Refer to AFI 37-131, *Freedom of Information Act Program*.

9.6. Public Release. Security incident reports cannot be released into the public domain until they have undergone a security review. *[Reference AFI 35-101, Public Affairs Policies and Procedures, Chapter 15]*

9.7. Reporting and Notifications.

9.7.1. Personnel who learn of a security incident must promptly report it to their commander, supervisor, or security manager who will in-turn report the incident to the servicing ISPM by the end of the first duty day.

9.7.2. After assigning a case number beginning with calendar year, base, and sequential number for tracking purposes, the ISPM will:

9.7.2.1. Coordinate with the organization security manager to ensure the commander has been briefed on the incident. The ISPM will brief the commander if the security manager is unable to do so or when the incident is reported directly to the ISPM.

9.7.2.2. Report compromises/probable compromises for the following incidents through command ISPM channels to HQ USAF/XOFI:

9.7.2.2. (SMC) SMC/AXP will accomplish these notifications for all SMC organizations.

9.7.2.2.1. Classified in the public media.

9.7.2.2.2. Foreign intelligence agencies.

9.7.2.2.3. Criminal activity.

9.7.2.2.4. NATO classified information.

9.7.2.2.5. Foreign government information.

9.7.2.2.6. Restricted Data (RD) or Formerly Restricted Data (FRD).

9.7.2.2.7. Disclosure to foreign nationals.

9.7.2.3. Notify the local AFOSI when the circumstances involve criminal activity or foreign intelligence agencies.

9.7.2.4. Notify SAF/AAZ when the compromise involves special access information through the appropriate special access program channels.

9.7.3. The appointing authority will notify the OCA, or the originator when the OCA is not known, when it is determined there is a compromise, probable compromise, or loss of classified information. Refer to paragraph **9.5.1.** of this AFI for security classification marking requirements.

9.8. Preliminary Inquiry. An informal inquiry to determine if classified information has been lost or compromised so that a damage assessment can be completed and the appropriate corrective action can be taken.

9.8.1. The commander or staff agency chief of the activity responsible for the security incident will appoint an inquiry official to conduct a preliminary inquiry. Use the requirements of AFI 90-301, *Inspector General Complaints*, Chapter 2.25, when determining whom to appoint. See **Attachment 8** for a sample appointment memorandum. Refer to paragraph **9.5.1.** of this AFI for appointment memorandum classification requirements.

9.8.1.1. When security incidents occur because of unauthorized transmission of classified material, the sending activity appoints the inquiry official and conducts the inquiry.

9.8.1.2. Inquiry officials will coordinate their actions with the servicing ISPM and the staff judge advocate's office.

9.8.1.2. (SMC) Security incidents involving collateral issues of high visibility or involving multiple organizations will be conducted by personnel assigned to the Director, Acquisition Systems Protection, SMC/AXP. This allows for a complete look at the incident and avoids potential conflicts of interest. If in doubt, contact SMC/AXP.

9.8.1.3. (Added-SMC) Preliminary inquiry officials should have no other assigned duties while conducting required inquiries.

9.8.1.4. (Added-SMC) At Los Angeles AFB, take the following actions.

9.8.1.4.1. (Added-SMC) Security Managers must contact SMC/AXP and briefly describe/discuss preliminary facts surrounding the violation, obtain a control number and guidance/assistance. The appointing authority will forward a copy of the appointment letter to SMC/AXPI. Inquiry officials will contact the organization's Security Manager to obtain an initial briefing on the security incident and administrative inquiry/ investigation guidance.

9.8.2. The preliminary inquiry will determine if classified material was compromised, the extent of the compromise, and the circumstances surrounding the compromise.

9.8.3. A preliminary report will be completed using the sample report format at **Attachment 9** and submitted to the appointing official through the ISPM. The ISPM will provide their concurrence/non-concurrence with the report and forward it to the appointing official for action. Refer to paragraph **9.5.** of this AFI for report classification requirements.

9.8.3.1. (Added-SMC) The appointing official will review the report for adequacy and initiate appropriate corrective action/disciplinary action. Based on the findings in the preliminary report, the appointing official decides whether to open a formal investigation or close the inquiry. The report will indicate administrative corrective action(s) and/or disciplinary action(s) and coordinate

with staff judge advocate, civilian and military personnel offices, as appropriate. Forward completed reports to SMC/AXP.

9.8.4. The report from the preliminary inquiry will be sufficient to resolve the security incident if:

9.8.4.1. The inquiry determines that loss or compromise of classified information has not occurred.

9.8.4.2. The inquiry determines that loss or compromise of classified information has occurred, but there is no indication of significant security weakness.

9.8.4.3. The appointing official determines that no additional information will be obtained by conducting a formal investigation.

9.8.5. If the report from the preliminary inquiry is not sufficient to resolve the security incident, the appointing authority initiates a formal investigation. The preliminary inquiry report will become part of any formal investigation. If the inquiry is closed out as a compromise or probable compromise the appointing authority notifies the OCA to perform a damage assessment.

9.9. Damage Assessment.

9.9.1. A damage assessment is an analysis to determine the effect of a compromise of classified information on the national security. It will be initiated upon notification of a probable or actual compromise to verify and reevaluate the information involved. Damage assessment reports will be classified and marked according to the classification guidance provided on the information being addressed in the reports.

9.9.2. The OCA must:

9.9.2.1. Set up damage assessment controls and procedures.

9.9.2.2. Notify HQ USAF/XOFI through command ISPM channels that a damage assessment is being done.

9.9.2.3. Provide HQ USAF/XOFI through ISPM channels a copy of the completed damage assessment report.

9.10. Formal Investigation. A detailed examination of evidence to determine the extent and seriousness of the compromise of classified information. The formal investigation will fix responsibility for any disregard (deliberate or inadvertent) of governing directives which led to the security incident.

9.10.1. The commander or staff agency chief of the activity responsible for the security incident will appoint an investigative official to conduct an investigation.

9.10.2. The formal investigation may be initiated without a preliminary inquiry if it is deemed prudent due to the seriousness of the security incident.

9.10.3. The formal investigation will include the preliminary inquiry if one has been conducted.

9.11. Management and Oversight.

9.11.1. The inquiry/investigative official will route the completed report through the servicing ISPM and staff judge advocate's office for review before forwarding it to the appointing authority.

9.11.2. The appointing authority will:

9.11.2.1. Close the inquiry/investigation unless MAJCOM, DRU, or FOA directives indicate otherwise.

9.11.2.2. Determine if administrative or disciplinary action is appropriate. See AFI 31-501, *Personnel Security Program Management*, Chapter 8 and applicable military and civilian personnel publications.

9.11.2.3. Debrief anyone who has had unauthorized access using AF Form 2587.

9.11.2.4. Forward a copy of the completed report to the ISPM identifying corrective actions taken.

9.11.2.5. Dispose of the report according to the instructions in AFMAN 37-139, *Records Disposition Schedule.*.

9.11.3. The ISPM will:

9.11.3.1. Provide technical guidance.

9.11.3.2. Monitor the status of security incidents.

9.11.3.2. (SMC) SMC/AXP is the reviewing authority for all preliminary inquiries. Upon review of the final preliminary inquiry report, facts may indicate further investigation. SMC/AXP will notify the appointing official to initiate a formal investigation, as appropriate.

9.11.4. Inquiry/investigative officials must complete inquiry/investigations within 30 duty days from appointment.

9.12. Unauthorized Absences. Report unauthorized absences to the ISPM and appropriate AFOSI detachment. *[Reference DOD 5200.1-R, Paragraph 10-108]*

MARVIN R. ESMOND, Lt Gen, USAF
DCS/Air & Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 12958, *Classified National Security Information,* 20 Apr 95

Federal Register Part VI, OMB, 32 CFR Part 2001, ISOO, *Classified National Security Information, Final Rule,* 13 Oct 96

OMB ISOO Directive Number 1, *Classified National Security Information,* 13 Oct 95

DoD 4000.25-8-M, *Military Assistance Program Address Directory System,* Jul 95

DoDD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs,* 21 Apr 82

DoD 5200.1-R, *Information Security Program,* 17 Jan 97

DoD 5200.1-PH, *DoD Guide to Marking Classified Documents,* Apr 97

DoD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312),* Mar 89

DoDD 5210.2, *Access to and Dissemination of Restricted Data,* Jan 78

DoDD 5210.83, *Unclassified Controlled Nuclear Information (UCNI),* 15 Nov 91

DoD 5220.22-M, *National Industrial Security Program Operating Manual,* Jan 95

DoD 5220.22-R, *Industrial Security Regulation,* Dec 85

DoDI 5240.11, *Damage Assessments,* 23 Dec 91

Naval Facilities Engineering Service Center Technical Data Sheet, TDS-2000-SHR, *Neutralizing "Locked-Out" Security Containers,* Nov 93

RCS Report HAF-SFI(Q)9222, *The Information Security Measurement Report and The Air Force Automatic Declassification Review Summary*

AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* (FOUO)

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to foreign Governments and International Organizations* (C)

AFPD 16-7, *Special Access Programs*

AFI 16-701, *Special Access Programs*

AFMAN 23-110, Volume II, *Standard Base Supply Customer's Procedures*

AFPD 24-2, *Preparation and Movement of Air Force Material*

AFI 31-101, Air Force Installation Security Program

AFI 31-207, *Arming and Use of Force by Air Force Personnel*

AFI 31-700 Series, *Acquisition*

AFPD 31-4, *Information Security*

AFI 31-205, *Air Force Security and Policy Review Program,*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFPD 33-2, *Information Protection*

AFI 33-202, *Computer Security*

AFI 33-204, *The C4 Systems Awareness, Training, and Education (SATE) Program*

AFI 33-208, *Information Assurance Operations*

AFI 33-211, *Communications Security (COMSEC) User Requirements*

AFI 33-212, *Reporting COMSEC Incidents*

AFI 35-101, *Public Affairs Policies and Procedures*

AFI 36-1001, *Managing the Civilian Performance Program*

AFPD 36-22, *Military Training*

AFMAN 36-2108, *Airman Classification*

AFI 36-2201, *Developing, Managing, and Conducting Training*

AFPAM 36-2211, *Guide for Management of Air Force Training System*

AFI 36-2402, *Officer Evaluation System*

AFI 36-2403, *The Enlisted Evaluation System (EES)*

AFI 36-2907, *Unfavorable Information File (UIF) Program*

AFMAN 36-505, *Skill Coding*

AFI 36-704, *Discipline and Adverse Actions*

AFI 37-131, *Air Force Freedom of Information Act Program*

AFMAN 37-139, *Records Disposition Schedule*

AFI 37-161, *Distribution Management*

AFI 51-301, *Civil Litigation*

AFI 61-204, *Disseminating Scientific and Technical Information*

AFI 61-205, *Sponsoring or Cosponsoring, Conducting, and Presenting DoD Related Scientific Technical Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*

AFI 65-401, *Relations with the General Accounting Office*

AFI 71-101, Volume I, *Criminal Investigations, Counterintelligence, and Protective Service Matters*

AFI 90-301, *Inspector General Complaints*

AFI 90-401, *Air Force Relations with Congress*

AFKAG-1, Air Force Communications Security (COMSEC) Operations

AFTO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*

AFSSI 5020, *Remanence Security*

Abbreviations and Acronyms

ADP—Automatic Data Processing

AF—Air Force

AFDO—Air Force Declassification Office

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFPDL—Air Force Publishing Distribution Library

AFSSI—Air Force Special Security Instruction

AFTO—Air Force Technical Order

AIS—Automated Information System

ASCAS—Automated Security Clearance Approval System

BITC—Base Information Transfer Center

CNWDI—Critical Nuclear Weapon Design Information

COMSEC—Communications Security

CONUS—Continental United States

DCII—Defense Clearance and Investigations Index

DCS—Defense Courier Service

DD—Department of Defense (Used for DoD Forms)

DEA—Drug Enforcement Agency

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDSI—Department of Defense Security Institute

DoE—Department of Energy

DRU—Direct Reporting Unit

DSS—Defense Security Service (Formerly DIS and DoDSI)

DTIC—Defense Technical Information Center

EES—Enlisted Evaluation System

EO—Executive Order

FMS—Foreign Military Sales

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FRD—Formerly Restricted Data

GAO—General Accounting Office

GILS—Government Information Locator System

GPO—Government Printing Office

GSA—General Services Administration

IDS—Intrusion Detection System

IG—Inspector General

IO—Investigating Officer

ISPM—Information Security Program Manager

ISOO—Information Security Oversight Office

LFC—Local Files Check

MAJCOM—Major Command

MDR—Mandatory Declassification Review

MIS—Management Information System

NAC—National Agency Check

NARA—National Archives and Records Administration

NATO—North Atlantic Treaty Organization

NCR—National Capital Region

NdA—Nondisclosure Agreement

OCA—Original Classification Authority

OMB—Office of Management and Budget

PA—Privacy Act

PCS—Permanent Change of Station

RCS—Report Control Symbol

RD—Restricted Data

SAP—Special Access Program

SATE—Security Awareness, Training, and Education

SCI—Sensitive Compartmented Information

SCG—Security Classification Guide

SEI—Special Experience Identifier

SF—Standard Form

SIF—Security Information File

SSO—Special Security Office

TDS—Technical Data Sheet

TDY—Temporary Duty

TSCA—Top Secret Control Account

TSCM—Technical Surveillance Countermeasures

TSCO—Top Secret Control Officer

UCNI—Unclassified Controlled Nuclear Information

Attachment 2

LIST OF AIR FORCE OFFICIALS AUTHORIZED TO CERTIFY ACCESS TO RESTRICTED DATA

Secretariat

Secretary of the Air Force (SAF/OS)
Under Secretary of the Air Force (SAF/US)
Assistant Secretary of the Air Force (Space) (SAF/SN)
Assistant Secretary of the Air Force (Financial Management and Comptroller) (SAF/FM)
Assistant Secretary of the Air Force (Manpower, Reserve Affairs, Installations, and Environment) (SAF/MI)
Assistant Secretary of the Air Force (Acquisition) (SAF/AQ)
General Counsel (SAF/GC)
Inspector General (SAF/IG)
Administrative Assistant to the Secretary of the Air Force (SAF/AA)

Air Staff

Chief of Staff (HQ USAF/CC)
Vice Chief of Staff (HQ USAF/CV)
Assistant Vice Chief of Staff (HQ USAF/CVA)
Deputy Chief of Staff/Air and Space Operations (HQ USAF/XO)
Director, Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI)
Deputy Chief of Staff/Installations and Logistics (HQ USAF/IL)
Deputy Chief of Staff/Personnel (HQ USAF/DP)
Deputy Chief of Staff/Plans and Programs (HQ USAF/XP)
Surgeon General (HQ USAF/SG)
Director of Security Forces (HQ USAF/XOF)
Chief, Information Security Division (HQ USAF/XOFI)
Chief of Safety (HQ USAF/SE)

Commands

Commander, Air Education and Training Command (HQ AETC/CC)
Commander, Air Force Institute of Technology (HQ AFIT/CC)
Commander, Air University (HQ AU/CC)
Commander, Air Force Space Command (HQ AFSPC/CC)
Commander, 45th Space Wing (HQ 45 SW/CC)
Commander, Air Force Materiel Command (HQ AFMC/CC)
Commander, Ogden Air Logistics Center (OO-ALC/CC)
Commander, Oklahoma City Logistics Center (OC-ALC/CC)
Commander, Sacramento Air Logistics Center (SM-ALC/CC)
Commander, San Antonio Air Logistics Center (SA-ALC/CC)
Commander, Warner Robins Air Logistics Center (WR-ALC/CC)
Commander, Aeronautical Systems Center (HQ ASC/CC)
Commander, Human Systems Center (HQ HSC/CC)
Commander, Air Force Flight Test Center (HQ AFFTC/CC)
Commander, Air Force Development Test Center (HQ AFDTC/CC)
Commander, Arnold Engineering Development Center (HQ AEDC/CC)
Commander, Air Force Research Laboratory (HQ AFRL/CC)
Commander, Electronic Systems Center (HQ ESC/CC)
Commander, Space and Missile Systems Center (HQ SMC/CC)
Commander, Air Force Reserve Command (HQ AFRC/CC)
Commander, Air Mobility Command (HQ AMC/CC)
Commander, Pacific Air Forces (HQ PACAF/CC)
Commander, United States Air Forces in Europe (HQ USAFE/CC)
Commander, Air Combat Command (HQ ACC/CC)

Direct Reporting Units

Commander, 11 Wing (HQ 11 WG/CC)
Commander, United States Air Force Academy (HQ USAFA/CC)
Commander, Air Force Operational Test and Evaluation Center (HQ AFOTEC/CC)
Commander, Air Force Communications Agency (HQ AFCA/CC)

Field Operating Agencies

Commander, Air Intelligence Agency (HQ AIA/CC)
Commander, National Air Intelligence Center (HQ NAIC/CC)

Miscellaneous

Commander, Air Force Technical Applications Center (HQ AFTAC/CC)

Attachment 3

CONTROLLED UNCLASSIFIED INFORMATION

A3.1. For Official Use Only (FOUO). See AFI 37-131, for additional Air Force policy on FOUO information. *[Reference DoD 5200.1-R, Paragraph 2-204]*

A3.1. (SMC) For protection of For Official Use Only (FOUO) information, see DoD Regulation 5400.7/AF and AFSPC Supplement, Freedom of Information Act Program, 22 Jul 99, which superseded AFI 37-131.

A3.2. Sensitive But Unclassified and Limited Official Use Information. Users apply the same marking, accessing, and protecting policy as required for FOUO information, AFI 37-131. *[Reference DoD 5200.1-R, Paragraph 3-300]*

A3.3. Protection of Drug Enforcement Agency (DEA) Sensitive Information. *[Reference DoD 5200.1-R, Paragraph 4-403a]*

A3.3.1. Users follow DEA policy for safeguarding DEA sensitive information.

A3.3.2. See AFI 33-202, *Computer Security,* for policy on secure communications circuits.

A3.4. Unclassified Controlled Nuclear Information (UCNI)

A3.4.1. Responsibility. The Director of Security Forces (HQ USAF/XOF) has primary responsibility within the Air Force for the implementation of DoDD 5210.83. *[Reference DoD 5200.1-R, Appendix C, Section 5]*

A3.4.2. UCNI Officials.

A3.4.2.1. The following positions have been designated UCNI Officials within the Air Force:

A3.4.2.1.1. Air Staff and Secretariat staff agency chiefs.

A3.4.2.1.2. Major command, field operating agency, and direct reporting unit commanders.

A3.4.2.1.3. Installation commanders and equivalent commander positions.

A3.4.2.1.4. Chiefs of Security Forces at all levels.

A3.4.3. UCNI Officials' Responsibilities.

A3.4.3.1. Identify information meeting definition of UCNI.

A3.4.3.2. Determine criteria for access to UCNI and approve special access requests.

A3.4.3.3. Approve or deny the release of UCNI information.

A3.4.3.4. Ensure all UCNI information is properly marked, safeguarded, transmitted, and destroyed properly.

A3.4.3.5. Document decisions and report them through their command ISPM channels to HQ USAF/XOFI. RCS Number DD-C3I(AR)1810 applies to this data collection.

A3.5. Sensitive Information (Computer Security Act of 1987). See AFI 33-202 for Air Force policy on protecting information in Federal Government AIS. *[Reference DoD 5200.1-R, Paragraph 6-600]*

A3.6. Technical Documents. See AFI 61-204 for Air Force policy on technical documents. *[Reference DoD 5200.1-R, Paragraph 7-700]*

Attachment 4

DEPARTMENT OF THE AIR FORCE EXECUTIVE ORDER (EO) 12958 25-YEAR AUTOMATIC DECLASSIFICATION PLAN

Section A4A—Plan

A4.1. Purpose. This plan provides the framework for Air Force compliance with Section 3.4 of the EO 12958.

A4.2. Scope. This plan pertains to all classified Air Force records determined under Federal law to have permanent historical value wherever they may be stored. Examples of record locations or storage are: National Archives (including regional archive branches), Federal Records Centers, Presidential Libraries, unit file rooms or repositories, other approved repositories, including contractor facilities, libraries, and within other agencies.

A4.3. Senior Official. Air Force Senior Security Official: Mr. William A. DAVIDSON, Administrative Assistant to the Secretary of the Air Force. Address - SAF/AA 1720 Air Force, Pentagon, Washington, DC 20330-1720. Telephone - (703) 695-9492.

A4.4. Estimated Amount Of Records And Locations

A4.4.1. The total estimated amount of Air Force records which meet the criteria of Section 3.4 is: 70,598 Cubic Feet (176,495,000 Pages). Of the total figure, 70,288 Cubic Feet (175,720,000 Pages) contain potentially exemptible information. Specific record reviews over the next five (5) years will determine more precisely what records must remain classified and what records can be automatically declassified. The remaining 310 Cubic Feet (775,000 Pages) can be automatically declassified without further review.

A4.4.2. Record locations and the estimated amount for these locations are as follows:

A4.4.2.1. 52,864 Cubic Feet (132,160,000 Pages)—Air Force Command/Activity Files, Repositories, Libraries, and Historical Centers.

A4.4.2.2. 9,644 Cubic Feet (24,110,000 Pages)—Federal Records Centers.

A4.4.2.3. 6,196 Cubic Feet (15,490,000 Pages)—National Archives.

A4.4.2.4. 1,584 Cubic Feet (3,960,000 Pages)—Presidential Libraries.

A4.4.2.5. 310 Cubic Feet(775,000 Pages)—Air Force Command/Activity Files, Repositories, Libraries, and Historical Centers - pages to be automatically declassified without review.

NOTE: Specific location(s) of Air Force command/activity files is contained in our supporting data and can be provided upon request.

A4.4.3. The survey method used by the Air Force to obtain these figures consisted of tasking each Air Force Secretariat, Air Staff, Major Command, Direct Reporting Unit, and Field Operating Agency activity to search their file holdings to identify records, documents, and information that falls within the purview of EO 12958, Section 3.4. The estimation conversion table provided by ISOO was used.

A4.5. Exempt File Series Description

A4.5.1. Federal Records Center: Record Groups 340, 341, and 342. Reasons for exemption correspond with EO exemption categories 1, 2, 5, 6 and the fact that the files contain some Restricted Data and Formerly Restricted Data.

A4.5.2. National Archives: Category 1 and 3. Reasons for exemption correspond with EO exemption categories 1, 2, 5, and 6.

A4.5.3. Presidential Libraries: Presidential Files. Reasons for exemption correspond with EO exemption categories 1, 2, 5, and 6.

A4.5.4. Air Force Commands/Activities: Various files series are listed as:

A4.5.4.1. Airborne Warning and Control Systems.

A4.5.4.2. Agreements.

A4.5.4.3. Ballistic Missile Systems.

A4.5.4.4. Combat Evaluations.

A4.5.4.5. Command Files.

A4.5.4.6. COMSEC Surveillance Project.

A4.5.4.7. Country Files.

A4.5.4.8. Cryptographic Information.

A4.5.4.9. Cryptologic Information.

A4.5.4.10. Electronic Warfare.

A4.5.4.11. Espionage/Counterespionage Operations.

A4.5.4.12. Flight Technical Reports.

A4.5.4.13. Foreign Civil Litigation Cases.

A4.5.4.14. Foreign Government Agreements.

A4.5.4.15. Foreign Government Technology.

A4.5.4.16. Historical Program and Unit Records.

A4.5.4.17. Intelligence Billet Validation.

A4.5.4.18. Intelligence Material Records.

A4.5.4.19. Intelligence Presentation Aids.

A4.5.4.20. Intelligence Reference Records.

A4.5.4.21. Investigative Files.

A4.5.4.22. Law of Armed Conflict.

A4.5.4.23. Missile/Space Technology.

A4.5.4.24. Munitions Effectiveness/Target Vulnerability.

A4.5.4.25. Negotiating Records.

A4.5.4.26. Nuclear Weapons Information.

A4.5.4.27. Presidential Aircraft System Security Standards.

A4.5.4.28. Security Classification Guides.

A4.5.4.29. Studies, Analysis and Summaries.

A4.5.4.30. Test Plans.

A4.5.4.31. Training Records/Film.

A4.5.4.32. Vietnam.

A4.5.4.33. Weapons Systems.

A4.5.4.34. War Plans.

NOTE: Reasons for exemption correspond with EO exemption categories 1, 2, 3, 4, 5, 6, 7, 8, 9, and Restricted Data and Formerly Restricted Data.

A4.6. Implementation Plan. The following actions will be taken to ensure the Air Force is in compliance with Section 3.4 of the EO.

A4.6.1. All Air Force activities - Secretariat, Air Staff, Major Commands, Direct Reporting Units, and Field Operating Agencies, that classify and/or maintain classified holdings will be responsible for:

A4.6.1.1. Identifying records, files, documents, and information which falls under the purview of Section 3.4.

A4.6.1.2. Providing specific resources, such as manpower and financial support, that will be allocated to identify records and perform declassification reviews.

A4.6.1.3. Implementing self paced classification/declassification management training.

A4.6.1.4. Conducting declassification reviews on all records which fall within the purview of Section 3.4 and reporting results of their reviews quarterly to HQ USAF/XOFI.

A4.6.1.5. Declassifying, where possible, and making available to the public all records not requiring exemption.

A4.6.2. Declassification reviews and actions will be accomplished by:

A4.6.2.1. Using in place and mobile declassification review teams that are composed of local subject matter experts, security personnel, records management personnel, historians, and reserve personnel.

A4.6.2.2. Conducting bulk declassification with concentration directed first to the high risk records, medium risk second, and low risk last. The following risk definitions apply:

A4.6.2.2.1. High - most of the information contained in the records will almost invariably fall into one or more exemption categories and have information which belongs to other agencies. Therefore, these records will require extensive interagency coordination and review.

A4.6.2.2.2. Medium - some of the information contained in the records will fall into one or more exemption categories and have some information which belongs to another agency. These records may require interagency coordination and review.

A4.6.2.2.3. Low - very little, if any, of the information contained in the records will fall into an exemption category or belong to another agency. These records most likely will require no interagency coordination.

A4.6.2.3. Automating applicable Security Classification and Declassification Guides and making them available to other federal agencies.

A4.6.3. Review goal will be:

A4.6.3.1. 20% of records—15 Nov 95 - 15 Oct 96.

A4.6.3.2. 20% of records—16 Oct 96 - 15 Oct 97.

A4.6.3.3. 20% of records—16 Oct 97 - 15 Oct 98.

A4.6.3.4. 20% of records—16 Oct 98 - 15 Oct 99.

A4.6.3.5. 20% of records—16 Oct 99 - 16 Apr 00.

A4.6.4. Results of automatic declassification review will be monitored through the metric - Air Force Automatic Declassification Review Summary. See AFPD 31-4 for a sample of this metric.

A4.6.5. Air Force will alter its review cycle of security classification guides to correspond with the implementation date of the new order.

A4.6.5.1. Review of all Air Force security classification guides will begin 16 October 1995 with a goal of completing the initial review by October 1997.

A4.6.5.2. The purpose of these reviews will be to update the guides as required and to bring them into alignment with the provisions of the new order.

A4.6.5.3. Declassification guidance will be included in each guide as deemed appropriate.

A4.6.5.4. Classification and declassification guides will be placed in the automated Air Force Declassification Toolbook and will be made available through the Air Force Publishing Distribution Library (AFPDL). Ultimately, all classification and declassification instructions will be placed in a key word searchable automated database that will be made available to all Air Force classifiers.

A4.7. Air Force Database. An Air Force locator system will be developed for use within the Government Information Locator System (GILS). As records are declassified, they will be listed in GILS and made available for public information.

Section A4B—Referrals

A4.8. Purpose. This section establishes the process for handling all information which is subject to the provisions of EO 12958, *Classified National Security Information*, Section 3.4, Automatic Declassification, and has been referred to, within, or outside the Air Force for review.

A4.9. Scope. This process applies to all information requiring review as prescribed by Section 3.4 of EO 12958, and:

A4.9.1. Is clearly Air Force information but is held by an organization outside of the Air Force.

A4.9.2. Is Air Force information being held by one Air Force organization but belongs to another Air Force organization.

A4.9.3. Is information being held by the Air Force but belongs to another organization outside of the Air Force.

A4.10. Primary Points Of Contact.

A4.10.1. Referrals to the Air Force: AFDO, Crystal Plaza 6, 2221 South Clark Street, Suite 600, Arlington, VA, 22202; Telephone numbers - (703) 604-4700 (DSN 664); Fax - (703) 604-5533 (DSN 664).

A4.10.2. Referrals from or within the Air Force: Air Force organization initiating the referral.

A4.10.3. Superseded or disestablished Air Force organization: The Air Force organization that has assumed, either directly or indirectly, the responsibility for the functions of the organization no longer in existence.

A4.11. Referral Process.

A4.11.1. Information forwarded to the Air Force by another government organization will be processed as follows:

A4.11.1.1. AFDO is the central point within the Air Force to receive all information referred to the Air Force for review by another government organization.

A4.11.1.2. AFDO, in turn, will be responsible for receiving all referred information; storing and protecting the information; reviewing the information for classification/declassification determination; forwarding to the appropriate Air Force organization(s) to review for classification/declassification determination as necessary; and responding to the government agency that referred the information, if appropriate.

A4.11.2. Air Force organizations will review their information before a decision is made to refer information from or within the Air Force. An Air Force organization will not refer information to another Air Force organization or to another government organization if it intends to exempt, in full, its own information. Nor will an Air Force organization refer information to another Air Force organization if it can first declassify the information from instructions received in an appropriate Air Force classification/declassification guide. For information that will be referred:

A4.11.2.1. Referrals within the Air Force: If information contained in documents held by one Air Force organization but originated by another Air Force organization is referred to the originating Air Force organization for review, the following applies:

A4.11.2.1.1. Unless agreed to on a case by case basis, only information belonging to the originating organization, plus adequate identifying documentation, will be referred.

A4.11.2.1.2. Method of referral, e.g., paper copy, electronic, CD-ROM, will be based on the capability of the receiving organization.

A4.11.2.1.3. Unless agreed to on a case by case basis, no suspense will be levied by the referring organization.

A4.11.2.2. Referrals to another government organization: If information contained in documents held by an Air Force organization but originated by another government organization is referred to the originating government organization for review, the following applies:

A4.11.2.2.1. Unless agreed to on a case by case basis, only information belonging to the originating organization, plus adequate identifying documentation, will be referred.

A4.11.2.2.2. Method of referral, e.g., paper copy, electronic, CD-ROM, will be based on the capability of the receiving organization.

A4.11.2.2.3. Unless agreed to on a case by case basis, no suspense will be levied by the referring organization.

Attachment 5

PHYSICAL SECURITY STANDARDS

A5.1. Intrusion Detection Systems (IDS) Standards. *[Reference DoD 5200.1-R, Appendix G, Paragraph B6]*

A5.1.1. Air Force IDS Standards. See AFI 31-101, Volume 1, **Air Force Physical Security Program**, Chapter 8, for Air Force policy on IDS.

A5.1.2. Trustworthiness Determinations. See AFI 31-501 for Air Force policy on trustworthiness determinations.

Attachment 6

TRANSMISSION TO FOREIGN GOVERNMENTS

A6.1. General. Air Force contracting officials ensure that US industrial activities have a government approved transportation plan or other transmission instructions.

Receipts. Air Force personnel: *[Reference DoD 5200.1-R, Appendix H, Paragraph a]*

A6.1.1. Use AF Form 349, **Receipt for Documents Released to Accredited Representatives of Foreign Nations** (available on the AFEPL);

A6.1.2. Show the complete unclassified title, description of a classified letter, minutes of meeting, and so on and any numerical identification of documents released on the form; and,

A6.1.3. Use the United States Postal System registered mail or Express Mail to transfer Secret or Confidential material to an embassy, official agency, or designated representative of the recipient foreign government in the United States.

A6.2. Whenever possible, shippers should use military airlift for shipping classified to foreign recipients. ***NOTE:*** When Air Mobility Command airlift can't deliver, determine an alternate secure method of direct delivery to a designated representative on a case-by-case basis. *[Reference DoD 5200.1-R, Appendix H, Paragraph c]*

A6.3. Depot and contract administration officials review lists of freight forwarders specified by the recipient foreign government to confirm that DoD 4000.25-8-M, *Military Assistance Program Address Directory System,* Jul 95**,** shows them as authorized to transport classified information.

A6.4. See AFPD 24-2 for instructions on "Report of Shipment."

A6.5. Overseas Shipments. See AFI 31-601 for Air Force policy on overseas shipments. *[Reference DoD 5200.1-R, Appendix H, Paragraph c(5)]*

A6.6. Foreign Military Sales (FMS). Air Force activities having primary management responsibility for processing foreign military sales cases ensure that personnel include transmission instructions. *[Reference DoD 5200.1-R, Appendix H, Paragraph e(1)(a)]*

Foreign military sales processors work with ISPMs and transportation officials on transportation plans submitted by foreign purchasers before giving final approval.

Attachment 7

AIR FORCE INFORMATION SECURITY PROGRAM TRAINING STANDARD

OBJECTIVE: To provide personnel with an understanding and knowledge of the Air Force standards and policies as they related to the DOD information security program, to include basic philosophy, policy, classification process, safeguarding, and security education program. **NOTE**: For training purposes, personnel are categorized and/or identified in the below as security (S) - security professional, specialist and manager); cleared personnel (C) - original classification authorities (OCAs), derivative classifiers, declassifiers, and other personnel that require access to classified information; and/or uncleared personnel (U) - personnel that do not require access. Personnel will receive training (scale value) as indicated during initial, orientation and refresher information security training.

Qualitative Requirements - Proficiency Code Key		
	Scale Value	Definition: The individual
Task Performance Levels	1	Can do simple parts of the task. Needs to be told or shown how to do most of the task. (Extremely limited)
	2	Can do most parts of the task. Needs only help with hardest parts. (Partially Proficient)
	3	Can do all parts of the task. Needs only a spot check of completed work. (Competent)
	4	Can do the complete task quickly and accurately. Can tell or show others how to do the task. (Highly Proficient)
*Task Knowledge Levels	a	Can name parts, tools, and simple facts about the task. (Nomenclature)
	b	Can determine step by step procedures for doing the task. (Procedures)
	c	Can identify why and when the task must be done and why each step is needed. (Operating Principles)
	d	Can predict, isolate, and resolve problems about the task. (Advanced Theory)

Qualitative Requirements - Proficiency Code Key		
**Subject Knowledge Levels	A	Can identify basic facts and terms about the subject. (Facts)
	B	Can identify relationship or basic facts and state general principles about the subject. (Principles)
	C	Can analyze facts and principles and draw conclusions about the subject. (Analysis)
	D	Can evaluate conditions and make proper decisions about the subject. (Evaluation)

Explanations:

* A task knowledge scale value may be used alone or with a task performance scale value to define a level of knowledge for a specific task. (Example: b and 1b)

** A subject knowledge scale value is used alone to define a level of knowledge for subjects not directly
related to any specific task or for a subject common to several tasks.

\- This mark is used alone instead of a scale value to show no proficiency training is provided in the standard.

X This mark is used in course columns to show training required but not given due to limitations in resources.

BASIC INFORMATION SECURITY PROGRAM TRAINING STANDARDS			
SUBJECTS, MATERIALS, AND/OR AREAS	**S**	**C**	**U**
1. POLICY AND PROGRAM MANAGEMENT			
a. Policy			
(1) Purpose and Scope (DOD 5200.1-R, paragraph 1-100)	A	A	A
(2) Policy ((DOD 5200.1-R, paragraph 1-101/AFI 31-401, paragraph **1.1.**)	A	A	A
(3) Philosophy (AFI 31-401, paragraph **1.2.**)	A	A	
b. Program Management			
(1) Program Management (AFI 31-401, paragraph **1.3.**)	A	A	A
(2) Air Force Oversight (AFI 31-401, paragraph **1.4.**)	A	A	
(3) Terms and Definitions (DOD 5200.1-R, Appendix B/AFI 31-501, attachment C)	A	A	
(4) Related Programs (Normally, functional OPR provides training & oversight)			
(a) Personnel Security - Security Forces (XOF)	A	A	A
(b) Industrial Security - Security Forces (XOF)	A	A	A
(c) Operations Security (OPSEC) - Operations (XOO)	A	A	
(d) Emission Security (EMSEC) (SC)	A	A	
(e) Communications Security (COMSEC) (SC)	A		
(f) Intelligence (IN)	A		
(g) Computer Security (COMPUSEC) (SC)	A	A	A
(h) Physical Security - (XOF)	A	A	A
(h) Physical Security - (XOF)	A		
(j) Product Security - Security Forces (XOF)	A		
(k) Freedom of Information Act (FOUO) (SC)	A	A	A
(l) Privacy Act (SC)	A	A	A
(m) Security and Policy Review (PA)	A	A	
(n) Foreign Disclosure (IA)	A	A	
c. Special types of information			
(1) Restricted Data (DOD 5200.1-R, paragraph 1-300/AFI 31-401, paragraph **1.5.**)	A		
(2) Sensitive Compartmented Information (SCI) (DOD 5200.1-R, paragraph 1-301/AFI 31-401, paragraph **1.5.**/AFI 14-302)	A		
(3) Communication Security (COMSEC) Information (DOD 5200.1-R, paragraph 1-301/AFI 31-401, paragraph **1.5.**)	A		

(4) North Atlantic Treaty Organization and Other Foreign Government Information (DOD 5200.1-R, paragraph 1-303)	A		
(5) Controlled Unclassified Information (DOD 5200.1-R, Appendix E/AFI 31-401, **Attachment 3**)	A	A	A
d. Exceptional situations			
(1) Military Operations (DOD 5200.1-R, paragraph 1-400)	A		
(2) Waivers to Requirements (DOD 5200.1-R, paragraph 1-401/AFI 31-401, paragraph **1.6.**)	A		
e. Corrective Actions and Sanctions			
(1) General Policy (DOD 5200.1-R, paragraph 1-500)	A	A	
(2) Sanctions (DOD 5200.1-R, paragraph 1-501/AFI 31-401, paragraph **1.8.**)	B	A	
(3) Reporting of Incidents (DOD 5200.1-R, paragraph 1-502/AFI 31-401, paragraph **1.3.**)	B	A	
f. Reporting Requirements (DOD 5200.1-R, paragraph 1-600/AFI 31-401, paragraph **1.7.**)	A	A	
g. Self-Inspections (DOD 5200.1-R, paragraph 1-700/AFI 31-401, paragraph **1.9.**)	A		
2. ORIGINAL CLASSIFICATION			
a. Original Classification Authority			
(1) Policy (DOD 5200.1-R, paragraph 2-200)	A	A	
(2) Delegation of Authority (DOD 5200.1-R, paragraph 2-301)	A		
(3) Air Force Original Classification Authority Training (DOD 5200.1-R, paragraph 2-202, AFI 31-401, paragraph **2.1.**/32 CFR part 2001)	C		
b. Original Classification Process			
(1) Overview (DOD 5200.1-R, paragraph 2-300)	A	A	
(2) Eligibility for Classification (DOD 5200.1-R, paragraph 2-301)	B		
(3) Possibility of Protection (DOD 5200.1-R, paragraph 2-302)	B		
(4) The Decision to Classify (DOD 5200. 1-R, paragraph 2-303)	B		
(5) Level of Classification (DOD 5200.1-R, paragraph 2-304)	B		
(6) Duration of Classification (DOD 5200,1-R, paragraph 2-305)	B		
(7) Communicating the Decision (DOD 5200.1-R, paragraph 2-306)	B		
b. Special Considerations			
(1) Compilation (DOD 5200.1-R, paragraph 2-400)	A		
(2) The Acquisition Process (DOD 5200.1-R, paragraph 2-401)	A		
(3) Limitations and Prohibitions (DOD 5200.1-R, paragraph 2-402/AFI 31-401, paragraph **2.2.**)	B		
c. Security Classifications and/or Declassification Guides			
(1) Policy (DOD 5200.1-R, paragraph 2-500)	A	A	

(2) Content (DOD 5200.1-R, paragraph 2-501/AFI 31-401, paragraph **2.4.**)	C	B	
(3) Approval, Distribution and Indexing (DOD 5200.1-R, paragraph 2-502/AFI 31-401, paragraph **2.4.**)	A		
(4) Review, revision and Cancellation (DOD 5200.1-R, paragraph 2-503)	A		
d Information for Private Sources			
(1) Policy (DOD 5200.1-R, paragraph 2-600)	A		
(2) Classification Determination (DOD 5200.1-R, paragraph 2-601)	A		
(3) Patent Secrecy Act (DOD 5200.1-R, paragraph 2-602)	A		
3. DERIVATIVE CLASSIFICATION			
a. Policy and General Requirement			
(1) The Nature of the Process (DOD 5200.1-R, paragraph 3-100)	A	A	
(2) Authority and Responsibility (DOD 5200.1-R, paragraph 3-101)	A	A	
(3) Policy (DOD 5200.1-R, paragraph 3-102)	A	A	
b. Procedures			
(1) General (DOD 5200.1-R, paragraph 3-200)	A	A	
(2) Special Cases (DOD 5200.1-R, paragraph 3-201)	A		
4. DECLASSIFICATION AND REGRADING			
a. Policy (DOD 5200.1-R, paragraph 4-100)	A	A	
b. Declassification Systems (DOD 5200.1-R, paragraph 4-101)	B	A	
c. Declassification Authority (DOD 5200.1-R, paragraph 4-102)	A	A	
d. Declassification and Downgrading Officials (AFI 31-401, paragraph **3.1.**)	A	A	
e. Exceptions (DOD 5200.1-R, paragraph 4-103)	A		
f. Declassification Decisions by Original Classifiers			
(1) Requirement (DOD 5200.1-R, paragraph 4-200)	A	A	
(2) The "Ten-Year Rule" (DOD 5200.1-R, paragraph 4-201)	A	A	
(3) Exemption from the "Ten-Year Rule" (DOD 5200.1-R, paragraph 4-202)	A	A	
(4) Extension of Ten-Year Declassification Periods (DOD 5200.1-R, paragraph 4-203)	A	A	
g. Automatic Declassification at 25 Years			
(1) The Automatic Declassification System (DOD 5200.1-R, paragraph 4-300/AFI 31-401, paragraph **3.2.**/**Attachment 4**)	A	A	
(2) Exemption of Specific Information (DOD 5200.1-R, paragraph 4-301)	A	A	
h. Mandatory Review for Declassification			
(1) General (DOD 5200.1-R, paragraph 4-400)	A		
(2) Responsibilities and Procedures (DOD 5200.1-R, paragraph 4-401)	A		
(3) Mandatory Declassification (AFI 31-401, paragraph **3.3.**)	A		

i. Systematic Review for Declassification (DOD 5200.1-R, paragraph 4-500)	A		
j. Downgrading			
(1) Purpose and Authority (DOD 5200.1-R, paragraph 4-600)	A	A	
(2) Downgrading Decisions during Original Classification (DOD 5200.1-R, paragraph 4-601)	A		
(3) Downgrading at a Later Date (DOD 5200.1-R, paragraph 4-602)	A		
k. Upgrading (DOD 5200.1-R, paragraph 4-700)	A		
l. Classification Challenges (DOD 5200.1-R, paragraph 4-900/AFI 31-401, paragraph **2.3.**)	B	A	
5. FOREIGN GOVERNMENT INFORMATION			
a. Policy and Procedures (DOD 5200.1-R, paragraph 4-800)	A	A	
b. Communication with Foreign Government (DOD 5200.1-R, paragraph 4-801)	A	A	
6. MARKING			
a. General Provisions			
(1) Marking and Designations rules (DOD 5200.1-R, paragraph 5-100)	B	A	
(2) Exceptions (DOD 5200.1-R, paragraph 5-101)	A	A	
(3) Marking Classified Documents and Other Material (DOD 5200.1-R, paragraph 5-102/AFI 31-401, **Section 4B**)	B	A	
b. Specific marking on Documents			
(1) Overall Classification Marking (DOD 5200.1-R, paragraph 5-200)	B	A	
(2) Agency, Office of Origin, and Date (DOD 5200.1-R, paragraph 5-201)	B	A	
(3) Source(s) of Classification (DOD 5200.1-R, paragraph 5-202)	B	A	
(4) Reason for Declassification/Classification (DOD 5200.1-R, paragraph 5-203/AFI 31-401, paragraph **4.2.**)	B	A	
(5) Declassification/Downgrading Instructions (DOD 5200.1-R, Paragraph 5-206)	B	A	
c. Identification of Specific Classified Information (DOD 5200.1-R, Paragraph 5-206)	B	A	
(1) Marking waivers (AFI 31-401, paragraph **4.4.**)	B	A	
(2) Page Marking (DOD 5200.1-R, paragraph 5-207)	B	A	
d. Marking Special Types of Documents			
(1) Documents With component Parts (DOD 5200.1-R, paragraph 5-300)	B	A	
(2) Transmittal Documents DOD 5200.1-R, paragraph 5-301)	B	A	
(3) Classification by Compilation DOD 5200.1-R, paragraph 5-302)	B	A	
e. Translations (DOD 5200.1-R, paragraph, 5-304)	B		
f. Information Transmitted Electronically (DOD 5200.1-R, paragraph 5-305)	B	A	
g. Documents and Material Marked for Training Purposes (DOD 5200.1-R, paragraph 5-306)	B		
h. Files, Folders, and Groups of Documents (DOD 5200.1-R, paragraph 5-307)	B	A	

i. Printed Documents Produced by AIS Equipment (DOD 5200.1-R, paragraph 5-308)	B	A	
j. Working Papers (DOD 5200.1-R, paragraph 6-101)	B	A	
k. Marking Special Types of Materials			
(1) Blue prints, Maps (DOD 5200.1-R, paragraph 5-401)	B	A	
(2) Photographs (DOD 5200.1-R, paragraph 5-402)	B	A	
(3) Slides (DOD 5200.1-R, paragraph 5-403)	B	A	
(4) Films (DOD 5200.1-R, paragraph 5-404)	B	A	
(5) Sound Recordings (DOD 5200.1-R, paragraph 5-405)	B	A	
(6) Microfilms (DOD 5200.1-R, paragraph 5-406)	B	A	
(7) AIS Removable (DOD 5200.1-R, paragraph 5-407)	B	A	
(8) AIS Storage (DOD 5200.1-R, paragraph 5-407/AFI 31-401, paragraph **4.6.**)	B	A	
(9) Labels (DOD 5200.1-R, paragraph 4-409)	B	A	
(10) Intelligence Information (DOD 5200.1-R, 5-410/AFI 31-401, paragraph **4.7.**)	B		
l. Changes in Marking			
(1) Downgrading and Declassification (DOD 5200.1-R, paragraph 5-500)	A	A	
(2) Downgrading and Declassification Earlier Than Scheduled (DOD 5200.1-R, paragraph 5-501)	A		
(3) Upgrading (DOD 5200.1-R, paragraph 5-502)	A		
(4) Posted Notice on Bulky Material (DOD 5200.1-R, paragraph 5-503)	A		
(5) Extensions on Duration (DOD 5200.1-R, paragraph 5-504)	A		
m. Remarking and Using Old Classified Material			
(1) Retaining Old Marking (DOD 5200.1-R, paragraph 5-600)	A		
(2) Earlier Declassification and Extension (DOD 5200.1-R, paragraph 5-601)	A		
n. Foreign Government Information/Equivalent U.S.			
(1) Marking NATO Documents (DOD 5200.1-R, paragraph 5-701)	B		
(2) Marking Other Foreign Government Documents (DOD 5200.1-R, paragraph 5-702)	B	A	
(3) Markings for Foreign Government and NATO Information in DOD Documents (DOD 5200.1-R, paragraph 5-703)	B		
(4) Marking for Transfer to Achieves (DOD 5200.1-R, paragraph 5-704)	B		
7. SAFEGUARDING			
a. Control Measures			
(1) General (DOD 5200.1-R, paragraph 6-100/AFI 31-401, paragraph **5.1.**)	B	A	
(2) Working Papers (DOD 5200.1-R, paragraph 6-101/AFI 31-401, paragraph **5.3.**)	B	A	
b. Access			
(1) Policy (DOD 5200.1-R, paragraph 6-300/AFI 31-401, paragraph **5.18.**)	B	A	A

(2) Administrative Controls (AFI 31-401, paragraph **5.10.**)	B	A	
(3) Granting Access to Classified Information (AFI 31-401, paragraph **5.4.**)	B	A	A
(4) Nondisclosure Agreement (NDA) (AFI 31-401, paragraph **5.5.**)	B	A	
(5) Preventing Publication of Classified Information in the Public (AFI 31-401, paragraph **5.8.**)	A		
(6) Access by Persons Outside the Executive Branch (DOD 5200.1-R, paragraph 6-201/AFI 31-401, paragraph **5.6.**)	B	A	
(7) Access to Information Originating in a Non-DOD Department Agency (AFI 31-401, paragraph **5.9.**)	B	A	
(8) Visits (DOD 5200.1-R, paragraph 6-202)	B	A	
(9) Access by Visitors (AFI 31-401, paragraph **5.7.**)	B	A	
(10) Administrative Controls (AFI 31-401, paragraph **5.10.**)	B	A	
c. Safeguarding			
(1) Care During Working Hours (DOD 5200.1-R, paragraph 6-30/AFI 31-401, paragraph **5.11.**)	B	A	
(2) End-of-Day Security Checks (DOD 5200.1-R, paragraph 6-302/AFI 31-401, paragraph **5.12.**)	B	A	A
(3) Emergency Planning (DOD 5200.1-R, paragraph 6-303)	B	A	
(4) Telephone Conversations (DOD 5200.1-R, paragraph 6-304)	B	A	
(5) Removal of Equipment(DOD 5200.1-R, paragraph 6-305)	A		
(6) Residential Storage (DOD 5200.1-R, paragraph 6-306)	B	A	
(7) Meeting and Conferences DOD 5200.1-R, paragraph 6-307/AFI 31-401, paragraph **5.15.**)	B	A	
(8) Information Located in Foreign Countries (DOD 5200.1-R, paragraph 6-308)	B		
(9) Processing Equipment/Reproduction (DOD 5200.1-R, paragraph 6-309/AFI 31-401, paragraphs **5.17./5.26.**)	B	A	
d. Storage			
(1) General Policy (DOD 5200.1-R, paragraph 6-400)	A	A	A
(2) Standards of Equipment (AFI 31-401, paragraph **5.20.**)	A	A	
(3) Storage of Information (DOD 5200.1-R, paragraph 6-402/AFI 31-401, paragraph **5.20.**)	B	A	
(4) Procuring New Equipment (DOD 5200.1-R, paragraph 6-403/AFI 31-401, paragraph **5.22.**)	B		
(5) Designating and Combinations (DOD 5200.1-R, paragraph 6-404/AFI 31-401, paragraph **5.23.**)	B	A	
(6) Repairing Damaged Containers DOD 5200.1-R, paragraph 6-405/AFI 31-401, paragraph **5.24.**)	B		

(7) Maintenance and Operating Inspections (DOD 5200.1-R, paragraph 6-406/AFI 31-401, paragraph **5.25.**)	A		
e. Reproducing Classified Material			
(1) Policy (DOD 5200.-R, paragraph 6-500)	A	A	
(2) Approving Reproduction (DOD 5200.1-R, paragraph 6-501)	A	A	
(3) Control Procedures (DOD 5200.1-R, paragraph 6-502/AFI 31-401, paragraph **5.27.**)	A	A	
f. Foreign Government Information			
(1) General (DOD 5200.1-R, paragraph 6-600)	B	A	
(2) Top Secret, Secret, Confidential (DOD 5200.1-R, paragraph 6-601)	B		
(3) Restricted Information (DOD 5200.1-R, paragraph 6-602)	B		
(4) Third-Country Transfers (DOD 5200.1-R , paragraph 6-603)	B		
(5) Storage (DOD 5200.1-R, paragraph 6-604)	B		
(6) Protecting Classified Material on Aircraft in Foreign Countries (AFI 31-401, paragraph **5.16.**)	B		
g. Disposition and Destroying Classified Material			
(1) Policy (DOD 5200.1-R, paragraph 6-700)	A	A	
(2) Methods and Standards (DOD 5200.1-R, paragraph 6-701/AFI 31-401, paragraph **5.29.**)	A	A	
(3) Retention of Classified Records (AFI 31-401, paragraph **5.28.**)	A	A	
h. Alternative or Compensatory Control Measures (DOD 5200.1-R, paragraph 6-800/AFI 31-401, paragraph **5.30.**)	A		
8. TRANSMISSION AND TRANSPORTATION			
a. Methods of Transmission or Transportation			
(1) Policy (DOD 5200.1-R, paragraph 7-100/Air Force Policy (AFI 31-401, Paragraph **6.1.**)	B	A	
(2) Transmitting Top Secret Information (DOD 5200.1-R, paragraph 7-101/AFI 31-401, paragraph **6.2.**)	B	A	
(3) Transmitting Secret Information (DOD 5200.1-R, paragraph 7-102/AFI 31-401, paragraph **6.3.**)	B	A	
(4) Transmitting Confidential Information (DOD 5200.1-R, paragraph 7-103/AFI 31-401, paragraph **6.4.**)	B	A	
(5) Transmission of Classified Material to Foreign Governments (DOD 5200.1-R, paragraph 7-104/appendix H/AFI 31-401, paragraph **6.5./Attachment 6**)	B		
(6) Shipment of Freight (DOD 5200.1-R, paragraph 7-105)	B		
b. Preparation of Material for Transmission			

(1) Envelopes or Containers (DOD 5200.1-R, paragraph 7-200/AFI 31-401, paragraph **6.6.**) (2) Addressing (DOD 5200.1-R, paragraph 7-201)	B	A	
c. Escort or Hand-Carry of Classified Material			
(1) General Provision (DOD 5200.1-R, paragraph 7-300)	B	A	
(2) Documentation (DOD 5200.1-R, paragraph 7-301)	B	A	
(3) Escort or Hand-Carrying Classified Aboard Commercial Passenger Aircraft (DOD 5200.1-R, paragraph 7-302/AFI 31-501, paragraph **6.9.**)	B		
9. SPECIAL ACCESS PROGRAMS (SAPs)			
a. Policy (DOD 5200.1-R, paragraph 8-100)	A	A	
b. Special Access Controls (DOD 5200.1-R, paragraph 6-801)	A		
c. SAP Procedures (DOD 5200.1-R, paragraph 8-101)	A		
d. Control and Administration (DOD 5200.1-R, paragraph 8-102/AFI 31-501, paragraph **7.1.**)	A		
e. Nicknames and Code Words (DOD 5200.1-R, paragraph 8-103F/AFI 31-501, paragraph **7.2.**)	A		
f. Establishment of DOD SAPs (DOD 5200.1-R, paragraph 8-103/AFI 31-501)	A		
g. Reviews of SAPs (DOD 5200.1-R, paragraph 8-104)	A		
h. Annual Reports and Revalidation (DOD 5200.1-R, paragraph 8-105)	A		
i. Interim Reports (DOD 5200.1-R, paragraph 8-106)	A		
j. Change of Classification (DOD 5200.1-R, paragraph 8-107)	A		
k. Termination and Transitioning of SAPs (DOD 5200.1-R, paragraph 8-108)	A		
10. SECURITY EDUCATION AND TRAINING			
a. Policy			
(1) General Policy (DOD 5200.1-R, paragraph 9-100/AFI 31-401, paragraph **8.1.**)	A	A	A
(2) Methodology (DOD 5200.1-R, paragraph 9-101/AFI 31-401, paragraph **8.2.**)	A	A	A
b. Initial Orientation			
(1) Cleared Personnel (DOD 5200.1-R, paragraph 9-200/AFI 401, paragraph **8.4.**)	B	A	
(2) Uncleared Personnel (DOD 5200.1-R, paragraph 9-201/AFI 31-403 paragraph **8.5.**)	B	A	A
c. Special Requirements			
(1) General (5200.1-R, paragraph 9-300)	A	A	
(2) Original Classifiers (DOD 5200.1-R, paragraph 9-301/AFI 31-401, paragraph **8.6.**)	B	A	
(3) Declassification Authorities Other Than Original Classifiers (DOD 5200.1-R, paragraph 9-302/AFI 31-401, paragraph **8.7.**)	B	A	

d. Derivative Classifiers, Security Personnel and Others (DOD 5200.1-R, paragraph 9-303/AFI 31-401, paragraph **8.8.**)	B	A	
e. Continuing Security Education/Refresher Training			
(1) Continuing Security Education (DOD 5200.1-R, paragraph 9-400)	B	A	A
(2) Refresher Training (DOD 5200.1-R, paragraph 9-401)	B	A	A
f. Termination Briefings			
(1) General Policy (DOD 5200.1-R, paragraph 9-500)	A	A	
(2) Procedures (AFI 31-403, paragraph 1.13)	B		
(3) Refusal to Sign Termination Statement (AFI 31-401, paragraph **8.14.**)	B		
g. Program Oversight (DOD 5200.1-R, paragraph 9-600)	B		
h. Train the trainer	B		
i. Lessons Learned	A	A	
11. ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION			
a. Policy (DOD 5200.1-R, paragraph 10-100/AFI 31-401, paragraph **9.1.**)	A	A	A
b. Reporting (DOD 5200.1-R, paragraph 10-101/AFI 31-401, paragraph **9.2.**)	B	A	A
c. Inquiry/Investigation (DOD 5200.1-R, paragraph 10-102/AFI 31-401, paragraph **9.3.**)	B	A	
d. Results of Inquiry/Investigation (DOD 5200.1-R, paragraph 10-104/AFI 31-401, paragraph **9.4.**)	B		
e. Additional Investigations (DOD 5200.1-R, paragraph 10-107)	B		
f. Verification, Reevaluation, and Damage Assessment (DOD 5200.1-R, 10-104/AFI 31-401, paragraph **9.5.**)	A	A	
g. Debriefing in Cases of Unauthorized Access (DOD 5200.1-R, paragraph 10-105)	A		
h. Management and Oversight (DOD 5200.1-R, paragraph 10-106/AFI 31-401, paragraph **9.6.**)	B	A	A
i. Unauthorized Absences (DOD 5200.1-R, paragraph 10-108/AFI 31-401, paragraph **9.7.**)	A		

Attachment 8

APPOINTMENT OF INQUIRY OFFICIAL MEMORANDUM
DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR

FROM:

SUBJECT:Appointment of Inquiry Official, Incident No.

You are appointed to conduct a preliminary inquiry into security incident (number). The incident involves (provide a short summary). Refer to AFI 31-401, *Information Security Program Management*, paragraph **9.5.**, for security classification requirements.

The purpose of this inquiry is to determine whether a compromise occurred and to categorize this 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 records and files pertinent to this inquiry. Your records indicate that 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 Security Program Manager (ISPM).

Contact (name and phone number of the ISPM), for a briefing on your responsibilities, conduct of, and limitations of this inquiry. Your written report will be forwarded through the ISPM to me within 30 duty days from the date of your appointment. As a minimum, your report must contain the following:

a. A statement that a compromise or probable compromise did or did not occur.

b. Category of the security incident.

c. Cause factors and responsible person(s).

d. Recommended corrective actions needed to preclude a similar incident.

Notify me immediately at (phone number) if you determine that a compromise has occurred. You are required to obtain technical assistance from the ISPM and Staff Judge Advocate during the course of this inquiry whenever necessary.

(Signature Block)

Attachment 9

PRELIMINARY INQUIRY OF SECURITY INCIDENT REPORT
DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR

FROM:

SUBJECT:Preliminary Inquiry of Security Incident No.

Authority: A preliminary inquiry was conducted (date) under the authority of the attached memorandum.

Matters investigated: The basis for this inquiry was that (provide a short summary of the security incident including the date it occurred, the classification of information involved, and the document control number if specific documents were involved). Refer to AFI 31-401, *Information Security Management Program*, paragraph **9.5.**, for security classification requirements.

Personnel Interviewed: (list all personnel interviewed, their position title, office symbol, and security clearance).

Facts: (list specific details answering who, what, why, where, and when questions concerning the security incident).

Conclusions: As a result of the investigation into the circumstances surrounding the security incident, interviews, and personal observations, it is concluded that: (list specific conclusions reached based on the facts and if a compromise or potential compromise did or did not occur). If a damage assessment is or has been done, provide the point of contact along with: the status of the assessment if it hasn't been completed; or, describe the outcome if it has been completed; or, provide a copy of the completed assessment report.

Recommendations: (list corrective actions needed to preclude a similar incident; the category of the incident; damage assessment; if the incident is a compromise, probable compromise or no compromise; and, if this inquiry should be closed without further investigation or with a recommendation for a formal investigation).

(Signature block)

Attachment:
Appointment of Inquiry Official Memo, (date)

Attachment 10

AIR FORCE
ORIGINAL CLASSIFICATION AUTHORITIES

Position Title	Level
Office of the Secretary of the Air Force	
Secretary of the Air Force (SAF/OS)	TS
Military Assistant (SAF/OS)	S
Under Secretary of the Air Force (SAF/US)	TS
Military Assistant (SAF/US)	S
Administrative Assistant (SAF/AA)	TS
Director, Security and Special Program Oversight (SAF/AAZ)	S
Deputy Under Secretary of the Air Force, International Affairs (SAF/IA)	S
Assistant Secretary for Manpower, Reserve Affairs, Installations and Environment (SAF/MI)	TS
Principal Deputy Assistant Secretary (SAF/MI)	S
Assistant Secretary for Financial Management and Comptroller (SAF/FM)	S
Principal Deputy Assistant Secretary, Financial Management and Comptroller (SAF/FM)	S
Deputy Assistant Secretary, Budget (SAF/FMB)	S
Assistant Secretary for Acquisition (SAF/AQ)	TS
Military Assistant (SAF/AQ)	S
Principal Deputy Assistant Secretary for Acquisition (SAF/AQ)	TS
Director, Special Projects (SAF/AQL)	TS
Directorate Global Reach (SAF/AQQ)	S
Directorate Space and Nuclear Deterrence (SAF/AQS)	TS
Assistant Secretary for Space (SAF/SN)	TS
Principal Deputy Assistant Secretary, Space (SAF/SD)	S
Director, Space Systems (SAF/SS)	S
Deputy Director for Security and Policy (SAF/SSS)	S
The General Counsel (SAF/GC)	TS
The Inspector General (SAF/IG)	TS
Director, Intelligence Systems Support Office (SAF/ISSO)	S

Position Title	Level
Director, Legislative Liaison (SAF/LL)	S
Director, Public Affairs (SAF/PA)	S
Air Force Program Executive Officer, Strategic (AFPEO/ST)	S
Air Force Program Executive Officer, Information Systems (AFPEO/IM)	S
Air Force Program Executive Officer, Tactical Airlift (AFPEO/TA)	S
Air Force Program Executive Officer, Command, Control and Communications (AFPEO/C3)	S
Air Force Program Executive Officer, Space (AFPEO/SP)	S
Air Force Program Executive Officer, Tactical Strike (AFPEO/TS)	S

Headquarters USAF

Chief of Staff (AF/CC)	TS
Vice Chief of Staff (AF/CV)	TS
Assistant Vice Chief of Staff (AF/CVA)	TS
Chief of Air Force Safety (AF/SE)	S
Director, Air Force Test and Evaluation (AF/TE)	TS
Air Force Historian (AF/HO)	S
Deputy Chief of Staff, Command, Control, Communications and Computers (AF/SC)	S
The Judge Advocate General (AF/JA)	S
Director of Civil Law and Litigation (AFLSA/JAC)	S
Chairman, USAF Scientific Advisory Board (AF/NB)	S
The Surgeon General (AF/SG)	S
Deputy Chief of Staff, Personnel (AF/DP)	TS
Director, Personnel Programs, Education and Training (AF/DPP)	S
Director, Military Personnel Policy (AF/DPX)	S
Chief, Personnel Readiness Group (AF/DPXC)	S
Deputy Chief of Staff, Plans and Operations (AF/XO)	TS
Director, Operations (AF/XOO)	S
Director, Operational Requirements (AF/XOR)	S
Director, Weather (AF/XOW)	S
Director, Nuclear and Counter Proliferation (AF/XON)	S

Position Title	Level
Director, Intelligence, Surveillance and Reconnaissance (AF/XOI)	TS
Director of Security Forces (AF/XOF)	TS
Deputy Chief of Staff, Plans and Programs (AF/XP)	TS
Deputy Chief of Staff, Installations and Logistics (AF/IL)	TS
Assistant Deputy Chief of Staff, Installations and Logistics (AF/IL)	TS
Director, Maintenance (AF/ILM)	S
Director, Transportation (AF/ILT)	S
Director, Plans and Integration (AF/ILX)	S
Director, Supply (AF/ILS)	S

Major Commands, Field Operating Agencies, and Direct Reporting Units

Air Combat Command

Commander, HQ ACC (ACC/CC)	TS
Comptroller (ACC/FM)	S
Director of Civil Engineering (ACC/CE)	S
Director of Intelligence (ACC/IN)	S
Director of Aerospace Operations (ACC/DO)	S
Director of Personnel (ACC/DP)	S
Command Historian (ACC/HO)	S
Inspector General (ACC/IG)	S
Director of Services (ACC/SV)	S
Director of Maintenance and Logistics (ACC/LG)	S
Staff Judge Advocate (ACC/JA)	S
Director of Public Affairs (ACC/PA)	S
Director of Safety (ACC/SE)	S
Surgeon General (ACC/SG)	S
Director of Plans and Programs (ACC/XP)	S
Director of Communications and Information Systems (ACC/SC)	S
Director of Security Forces (ACC/SF)	S
Advisor to the Commander for Guard Affairs (ACC/CG)	S
Commander, 8th Air Force (8 AF/CC)	TS

Position Title	Level
Commander, 26th Information Operations Group (26 IOG/CC)	S
Commander, 67th Information Operations Wing (67 IOW/CC)	S
Commander, 692nd Information Operations Group (692 IOG/CC)	S
Commander, 12th Air Force (12 AF/CC)	TS
Commander, 1st Fighter Wing (1 FW/CC)	S
Commander, 2nd Bomb Wing (2 BW/CC)	S
Commander, 4th Fighter Wing (4 FW/CC)	S
Commander, 5th Bomb Wing (5 BW/CC)	S
Commander, 6th Air Base Wing (6 ABW/CC)	S
Commander, 7th Bomb Wing (7 BW/CC)	S
Commander, 9th Reconnaissance Wing (9 RW/CC)	S
Commander, 20th Fighter Wing (20 FW/CC)	S
Commander, 27th Fighter Wing (27 FW/CC)	S
Commander, 28th Bomb Wing (28 BW/CC)	S
Commander, 33rd Fighter Wing (33 FW/CC)	S
Commander, 49th Fighter Wing (49 FW/CC)	S
Commander, 55th Wing (55 WG/CC)	S
Commander, 57th Wing (57 WG/CC)	S
Commander, 65th Air Base Wing (65 ABW/CC)	S
Commander, 99th Air Base Wing (99 ABW/CC)	S
Commander, 347th Fighter Wing (347 FW/CC)	S
Commander, 355th Wing (355 WG/CC)	S
Commander, 366th Wing (366 WG/CC)	S
Commander, 509th Bomb Wing (509 BW/CC)	S
Commander, 552nd Air Control Wing (552 ACW/CC)	S
Commander, Air Warfare Center (AWFC/CC)	S
Commander, AIA (AIA/CC)	TS
Vice Commander, AIA (AIA/CV)	TS
Executive Director (AIA/CA)	S
Director of Operations (AIA/DO)	S

Position Title	Level
Director of Plans and Programs (AIA/XP)	S
Commander, National Air Intelligence Center (NAIC/CC)	TS
Director of Technical Assistance (NAIC/TA)	S
Commander, Air Force Information Warfare Center (AFIWC/CC)	S
*Commander, Air Force Technical Applications Center (AFTAC/CC)	TS
*Vice Commander, Air Force Technical Applications Center (AFTAC/CV)	S
Air Education and Training Command (AETC)	
Commander, AETC (AETC/CC)	S
Director of Logistics (AETC/LG)	S
Director of Education (AETC/ED)	S
Air Force Audit Agency (AFAA)	
The Auditor General (AFAA/CC)	S
Air Force Command, Control, Communications and Computer Agency (AFCA)	
Commander, AFCA (AFCA/CC)	TS
Air Force Civil Engineer Support Agency (AFCESA)	
Commander, AFCESA (AFCESA/CC)	S
Air Force Historical Research Agency (AFHRA)	
Commander, AFHRA (AFHRA/CC)	S
Air Force History Support Office (AFHSO)	
Commander, AFHSO (AFHSO/CC)	S
Air Force Materiel Command (AFMC)	

Position Title	Level
Commander, AFMC (AFMC/CC)	TS
Director of Intelligence (AFMC/IN)	S
Commander, Ogden Air Logistics Center (OO-ALC/CC)	TS
Commander, Oklahoma City Air Logistics Center (OC-ALC/CC)	TS
Commander, Sacramento Air Logistics Center (SM-ALC/CC)	TS
Commander, San Antonio Air Logistics Center (SA-ALC/CC)	TS
Commander, Warner Robins Air Logistics Center (WR-ALC/CC)	TS
Commander, Aeronautical Systems Center (ASC/CC)	TS
Director, Weapons Airbase Range Product Support Office (OL-VX/VX)	S
Commander, Air Force Development Test Center (AFDTC/CC)	TS
Commander, Air Force Flight Test Center (AFFTC/CC)	S
Commander, Arnold Engineering Development Center (AEDC/CC)	TS
Commander, Electronic Systems Center (ESC/CC)	TS
Commander, Air Force Cryptological Support Center (AFCSC/CC)	S
Deputy Commander, Program Integration and Planning, Human Systems Center (HSC/XR)	S
Commander, Space and Missile Systems Center (SMC/CC)	TS
Commander, Air Force Research Laboratory (AFRL/CC)	TS
Director, Directed Energy (AFRL/DE)	TS
Director, Information (AFRL/IF)	TS
Director, Materials and Manufacturing (AFRL/ML)	TS
Director, Sensors (AFRL/SN)	TS
Director, Space Vehicles (AFRL/VS)	TS
Director, Munitions (AFRL/MN)	S
Director, Wright Research Site (Det 1, AFRL/WS)	S
Director of Material Management (WR-ALC/LU)	S
Director of Material Management (WR-ALC/LK)	S
Director of Material Management (WR-ALC/LY)	S
Director of Material Management (WR-ALC/LF)	S
Director of Material Management (WR-ALC/LN)	S

Air Force Military Personnel Center (AFMPC)

Position Title	Level
Commander, AFMPC (AFMPC/CC)	S
Director, Personnel Accountability (AFMPC/DPW)	S
Air Force Office of Special Investigations (AFOSI)	
Commander, AFOSI (AFOSI/CC)	S
Air Force Operational Test and Evaluation Center (AFOTEC)	
Commander, AFOTEC (AFOTEC/CC)	TS
Air Force Reserve Command (AFRC)	
Commander, AFRC (AFRC/CC)	TS
Vice Commander, AFRC (AFRC/CV)	S
Assistant Vice Commander, AFRC (AFRC/CS)	S
Commander, 4th AF (4 AF/CC)	S
Commander, 10th AF (10 AF/CC)	S
Commander, 22nd AF (22 AF/CC)	S
Commander, Air Reserve Personnel Center (ARPC/CC)	S
Air Force Safety Agency (AFSA)	
Commander, AFSA (AFSA/CC)	S
Director of Nuclear Surety (AFSA/SN)	S
Air Force Space Command (AFSPC)	
Commander, AFSPC (AFSPC/CC)	TS
Director of Intelligence (AFSPC/IN)	S
Director of Operations (AFSPC/DO)	S
Director of Plans (AFSPC/XP)	S
Director of Requirement (AFSPC/DR)	S

Position Title	Level
Director of Logistics (AFSPC/LG)	S
Director of Communications-Computer Systems (AFSPC/SC)	S
Commander, 14th AF (14 AF/CC)	S
Commander, 20th AF (20 AF/CC)`	S
Commander, 21st Space Wing (21 SW/CC)	S
Commander, 30th Space Wing (30 SW/CC)	S
Commander, 45th Space Wing (45 SW/CC)	S
Commander, 50th Space Wing (50 SW/CC)	S
Commander, 90th Missile Wing (90 MW/CC)	S
Commander, 91st Missile Wing (91 MW/CC)	S
Commander, 321th Missile Wing (321 MW/CC)	S
Commander, 341st Missile Wing (341 MW/CC)	S
Air Force Special Operations Command (AFSOC)	
Commander, AFSOC (AFSOC/CC)	TS
Vice Commander, AFSOC (AFSOC/CV)	S
Director, Command Staff AFSOC (AFSOC/CS)	S
Air Mobility Command (AMC)	
Commander, AMC (AMC/CC)	TS
Vice Commander AMC (AMC/CV)	TS
Director of Special Staff (AMC/DS)	S
Director of Plans and Programs (AMC/XP)	S
Inspector General (AMC/IG)	C
Commander, Defense Courier Service (DCS/CC)	C
Pacific Air Forces (PACAF)	
Commander, PACAF (PACAF/CC)	TS
Director of Operations (PACAF/DO)	S

Position Title	Level
Director of Plans (PACAF/XP)	S
Commander, Fifth Air Force (5 AF/CC)	TS
Commander, Seventh Air Force (7 AF/CC)	TS
Commander, Eleventh Air Force (11 AF/CC)	TS
Commander, Thirteenth Air Force (13 AF/CC)	TS
United States Air Force Academy (USAFA)	
Superintendent, USAFA (USAFA/SUPT)	S
United States Air Forces in Europe (USAFE)	
Commander, USAFE (USAFE/CC)	TS
Vice Commander USAFE (USAFE/CV)	TS
Director of Operations (USAFE/DO)	S
Director, Plans and Programs (USAFE/XP)	S
Political Advisor (USAFE/CCB)	S
Commander, Third Air Force (3 AF/CC)	TS
Commander, Sixteenth Air Force (16 AF/CC)	TS
Joint Services Survival, Evasion, Resistance and Escape Agency (JSSA)	
Commander, JSSA	S

******AIA is responsible for administrative support to AFTAC*

Attachment 11

IC 2000-1 TO AFI 31-401, INFORMATION SECURITY PROGRAM MANAGEMENT

15 MAY 2000

SUMMARY OF REVISIONS

This revision incorporates Interim Change IC 2000-1. This change delegates approval authority for revisions to this AFI (purpose paragraph); updates the office of primary responsibility; updates the table of contents to reflect changes in **Chapter 8**; updates security classification guide distribution addresses (paragraph **2.4.2.**); tells users in what form to submit electronic versions of security classification guides (paragraph **2.4.3.**); adds a requirement for original classification authorities to include a statement in security classification guides regarding release of program data on the World Wide Web (paragraph **2.4.5.**); replaces the security education chapter to implement the new security education requirements (**Chapter 8**); and, adds the Air Force Information Security Program Training Standard (**Attachment 7**). See the last attachment of the publication, IC 00-1, for the complete IC. A "|" indicates revised material since the last edition.

OPR: HQ USAF/XOFI (Deborah Ross (Classification Management & Marking), Steven Harris (Safeguarding), Danny Green (Security Education))

Purpose. It contains Air Force (AF) unique guidance needed to supplement Air Force Policy Directive (AFPD) 31-4, *Information Security*; Executive Order (EO) 12958, *Classified National Security Information*, 20 Apr 95; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information*, 13 Oct 95; and, Department of Defense (DOD) 5200.1-R, *Information Security Program*, 17 Jan 97, for the management of the Air Force Information Security Program. Additional references include DOD Instruction (DODI) 5240.11, *Damage Assessments*, 23 Dec 91; and, DOD Directive (DODD) 5210.83, *Unclassified Controlled Nuclear Information (UCNI),* 15 Nov 91. All these references are listed at the end of each paragraph where applicable. HQ USAF/XOF is delegated approval authority for revisions to this AFI.

Chapter 8—SECURITY EDUCATION

Section 8A Policy

8.1. General Policy

8.2. Methodology

8.3. Roles and Responsibilities

Section 8B Initial Security Orientation

8.4. Cleared Personnel

8.5. Uncleared Personnel

Section 8C Special Requirements

8.6. Original Classification Authorities

8.7. Declassification Authorities Other Than Original Classifiers

8.8. Derivative Classifiers, Security Personnel and Others

8.9. Security Career Personnel and Security Managers

8.10. Other Program Related Training Requirements

Section 8D Continuing and Refresher Training

8.11. Continuing and Refresher Training

Section 8E Access Briefings and Termination Debriefings

8.12. Access Briefings

8.13. Termination Debriefings

8.14. Refusal to Sign a Termination Statement

Section 8F Program Oversight

8.15. General

Section 8G Coordinating Requests for Formal Training

8.16. Coordinating Requests for Training

Attachment 7—AIR FORCE INFORMATION SECURITY PROGRAM TRAINING STANDARD

1.3.5.1. Appoint a primary and at least one alternate security manager to administer the unit's information security program.

1.3.5.2. Ensure security managers receive required training according to **Chapter 8**.

1.3.6.9. Participating in security education training as defined in **Chapter 8**.

2.4.2.2. HQ AFDO/CC, 1720 Air Force Pentagon, Washington, DC 20330-1720.

2.4.2.4. SAF/PAS, 1690 Air Force Pentagon, Washington, DC 20330-1690.

2.4.2.5. DTIC, Attention: DTIC-OCP, 8725 John J. Kingman Road, Suite 944, Ft. Belvoir, VA 22060-6218.

2.4.3. Within 180 days of the publication of this AFI, each OCA will provide an electronic version of their classification guidance (i.e., Security Classification Guides (SCGs), AFIs, Correspondence) to the addressees listed in paragraph **2.4.2.** This will facilitate the development of an interactive, key word searchable database. Electronic copies must be done in Microsoft Word 97 and saved to a 3.5" diskette as a .pdf file. If this capability is not yet available, annotate "//SIGNED//" above the signature element and add the date the original was signed.

2.4.5. Each OCA will revise their security classification guides to include an advisory statement in the Release of Information section:

2.4.5.1. Release of Program Data on the World Wide Web. Extreme care must be taken when considering information for release onto publicly accessible or unprotected World Wide Web sites. In addition to satisfying all of the aforementioned approval provisions, owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. The search and data mining capabilities of Web technology must be assessed from a risk management perspective. Information intended for publication on publicly accessible or unprotected web sites must be cleared for public release prior to publication according to AFI 35-101. If there are any doubts, do not release the information.

Chapter 8

SECURITY EDUCATION AND TRAINING

Section 8A - Policy

8.1. General Policy. Effective information security training is a cornerstone of the Air Force (AF) Information Security Program. All Air Force personnel need information security training whether they have access to classified information or not. All AF personnel are personally and individually responsible for protecting the national interests of the United States. All security infractions and/or violations must be immediately reported, circumstances examined and those responsible held accountable and appropriate corrective action taken. Commanders are responsible for ensuring that personnel are knowledgeable and understand their responsibility to protect information and resources deemed vital to national security. **NOTE**: For the purpose of this chapter, the term *commander* encompasses staff agency chief and director, when applicable.

8.2. Methodology. The AF will provide information security training to its personnel and contractors, as appropriate, on a continuous basis using government and commercial training sources. Various training methods will be used to administer training, such as classroom instruction, one-on-one, computer-based, and other distant learning training media. The AF will maintain a cadre of trained professional career security personnel and security managers to administer, implement, and measure the program's effectiveness. When funds and resources permit, professional security personnel and security managers should attend in-residence type training courses.

8.3. Roles and Responsibilities.

8.3.1. These roles and responsibilities are in addition to those listed in paragraph **1.3.**

8.3.2. The Air Force Security Forces Center, Security Forces Training (AFSFC/SFWT), is responsible for developing Air Force specific information security training course materials, curriculums and awareness products.

8.3.3. Commanders are responsible for implementing the information security training program, developing supplemental training tools, and assessing the health of their programs on a continuous basis. In addition, commanders will:

8.3.4.1. Ensure appointed security managers receive training within 90 days of their assignment and that the training is annotated in the individual's official personnel file (OPF) or military training record.

8.3.4.2. Budget for security awareness training products, materials, and the formal training of security managers.

8.3.4.3. Actively support and monitor security education training.

8.3.4.4. Ensure records are maintained on a calendar year basis of personnel attending initial, refresher and specialized information security training. As a minimum, these records must reflect the date(s) training was conducted and the number of personnel in attendance.

8.3.5. Supervisors will conduct and/or ensure personnel receive training as required by this instruction, document it when required, and ensure credit is given for course completion or briefing attendance, if appropriate.

8.3.6. ISPMs at all levels are responsible for:

8.3.6.1. Developing and overseeing implementation of information security training programs.

8.3.6.2. Assessing the effectiveness of training programs annually.

8.3.6.3. Developing and conducting classroom or one-on-one training for newly appointed security managers. Professional security personnel serving in security manager and/or security officer capacities must also receive this training.

8.3.6.4. Developing and distributing generic information security training lesson plans, which cover the basic information security work-center components (information, personnel and industrial security programs) to include installation specific security requirements.

8.3.6.5. Assisting security managers in the development of unit specific lesson plans, motivational materials and training aids.

8.3.6.6. Publicly recognizing the training efforts of effective security managers.

8.3.6.7. Providing civilian employees who complete information security managers training with a certificate, which they can use to enter course completion into their OPF.

8.3.6.8. Providing military supervisors with the names of military personnel appointed security manager duties that complete the security manager training course. This training will be annotated into the individual's on-job-training (OJT) record and other official records, as appropriate.

8.3.7. Unit Security Managers are responsible for:

8.3.7.1. Ensuring security training is conducted as outlined in this AFI.

8.3.7.2. Developing organizational specific security lesson plans.

8.3.7.3. Advising the commander on the status of the unit's security training program.

8.3.7.4. Ensuring training is documented and records are properly maintained, if applicable.

Section 8B --Initial Security Orientation

8.4. Cleared Personnel.

8.4.1. Initial Training. Supervisors and security managers provide initial training to all cleared personnel. Supervisors are responsible for ensuring that their cleared personnel receive an initial security education orientation before they access classified information.

8.4.1.1. Initial training should ensure cleared personnel are knowledgeable of their security responsibilities as related to their jobs and the organization's mission.

8.4.1.2. As a minimum, initial information security training for cleared personnel will address the following:

8.4.1.2.1. Subjects, material and/or areas as indicated in **Attachment 7**, AF Information Security Program Training Standard, under column heading (C) for cleared personnel.

8.4.1.2.2. When prior personnel security investigations and/or determinations are acceptable.

8.4.1.2.4. What derogatory/unfavorable information or suspicious activities by other cleared personnel that must be immediately reported to the commander or staff agency chief.

8.4.1.2.5. What the personnel security clearance verification, access and safeguarding requirements are when on-base cleared DOD contractors require access to classified information in support of classified contracts.

8.4.1.2.6. What the marking and safeguarding requirements are for protecting unclassified controlled information.

8.5. Uncleared Personnel.

8.5.1. Supervisors and security managers provide training to uncleared personnel. Supervisors are responsible for ensuring that all uncleared personnel receive an initial security education orientation within 90 days of assignment to the unit.

8.5.1.1. Initial orientation training must ensure that uncleared personnel are knowledgeable of their responsibilities and roles in the Air Force Information Security Program.

8.5.1.2. As a minimum, initial security education orientation training for uncleared personnel will address/cover the following:

8.5.1.2.1. Subjects, areas and/or materials identified in **Attachment 7**, AF Information Security Program Training Standards, under column heading (U) for uncleared personnel.

8.5.1.2.2. The identity of the installation Information Security Program Manager (ISPM) official and unit security manager and their respective responsibilities.

8.5.1.2.3. The different levels of classified information and why it is important to protect it.

8.5.1.2.4. The procedures to follow should classified information be discovered unprotected or to report other potential security incidents.

8.5.1.2.5. The requirements for the marking and safeguarding of sensitive unclassified, controlled unclassified and "For Official Use Only" information.

Section 8C--Special Requirements

8.6. Original Classification Authorities (OCAs). The ISPMs are responsible for administering specialized training to Original Classification Authorities (OCAs) in accordance with DOD 5200.1-R, *Information Security Program*. Training must be conducted prior to OCA authority being exercised. ISPMs may either develop their own training or administer/use the Defense Security Service (DSS) OCA or equivalent training product. The specialized OCA training is in addition to the requirements of **Attachment 7**, AF Information Security Program Training Standard, under column heading (C) for cleared personnel.

8.7. Declassification Authorities Other Than Original Classification Authorities. The ISPMs are responsible for administering this specialized training in accordance with DOD 5200.1-R. Training must be conducted before the declassification authority makes any declassification decisions.

This specialized training is in addition to the "cleared personnel" requirements of **Attachment 7**, Air Force Information Security Program Training Standards.

8.8. Derivative Classifiers, Security Personnel and Others.

8.8.1. Derivative Classifiers. Commanders are responsible for ensuring that derivative classifiers are adequately trained in accordance with DOD 5200.1-R. ISPMs will assist security managers in acquiring or developing the appropriate lesson plans and training materials.

8.9. Professional Security Personnel and Security Managers

8.9.1. Professional Security Personnel and Security Managers. Commanders ensure professional security career personnel and security managers receive training as follows:

8.9.1.1. Subjects, material and/or areas as indicated in **Attachment 7**, Air Force Information Security Program Training Standard, under column heading (S) for security personnel.

8.9.2. Professional Security Career Personnel.

8.9.2.1. Civilians. See AFMAN 36-202, Volume 2, *Air Force Civilian Career Planning*, paragraph 3-16, Security Career Program Master Development Plan (MDP). An AF/DPKCS, Security Career Program Administrator, enhanced/modified version of the MDP can be obtained from the MAJCOM, FOA, or

DRU civilian security career program coordinator normally located on the ISPM's staff. A copy can also be obtained by accessing the Air Force Personnel Center Web Site at http//www.afpc.randolph.af.mil., Security Career Program.

8.9.2.2. Military. See requirements for award of Special Experience Identifier (SEI) 322 in AFMAN 36-2108, *Airman Classification*. Also use the Civilian Security Career Program Master Development as a guide for determining additional training.

8.9.3. Security Managers.

8.9.3.1. The ISPM provide training too newly appointed security managers within 90 days of their assignment. Although not mandatory, unit commanders may fund and send their appointed security managers to the DSS in-resident Information Security Management Course or an equivalent AF approved course. Other commercial training sources may be used to provide this training when approved by the MAJCOM.

8.9.3.2. As a minimum, appointed security managers will be administered initial classroom or one-on-one training in accordance with **Attachment 7**. This training must equip the appointees with a workable knowledge and understanding of information security, personnel security and industrial security program mandates, including security access requirement (SAR) unit manpower document (UMD) position coding.

8.9.3.3. Commanders ensure civilians performing these duties receive the appropriate skill coding in their personnel records according to AFMAN 36-505, *Skill Coding.*

8.9.4. Training Costs. Commanders must budget annually for their information security program training needs (training course attendance, educational materials, awareness media, etc.).

8.10. Other Program Related Training Requirements.

8.10.1. ISPMs will identify training requirements for those security disciplines and/or areas for which they are responsible.

8.10.2. Commanders must ensure that training is properly documented in the individual's official personnel records and ensure personnel receive credit for attending and completing courses, if applicable.

8.10.3. Document training as outlined in AFPD 36-22, *Military Training,* AFI 36-2201, *Developing, Managing, and Conducting Training,* and AFPAM 36-2211, *Guide for Management of Air Force Training Systems.*

8.10.4. The following programs have security related training requirements:

8.10.4.1. Sensitive Compartmented Information (SCI).

8.10.4.1.1. The Special Security Officer (SSO) or designee conducts SCI security awareness training quarterly for personnel accessed to SCI. *[Reference DOD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual, Chapter 2, paragraph 12, and AFMAN 14-304, The Security, Use, and Dissemination of Sensitive Compartmented Information, Chapter 12]*

8.10.4.1.2. In addition, personnel granted SCI access will receive an annual briefing on their continuing responsibilities. *[Reference DOD 5105.21-M-1, Sensitive Compartment Information Administrative Security Manual, Chapter 2 and AFMAN 14-304, paragraph 12.3]*

8.10.4.2. Operations Security (OPSEC). A designated official conducts OPSEC training within 90 days of an individual's arrival and/or assignment. *[Reference AFI 10-1101, Operations Security, paragraph 4.4.1.]*

8.10.4.3. Information Protection Security Awareness Training and Education (SATE).

8.10.4.3.1. The SATE program is a single, integrated information assurance awareness, training, and education effort. All Air Force military and civilian and contractors who use Air Force information systems must complete IA training annually, and be so certified. This training and certification is accomplished by an IA Intranet-Based (ITB) Training and certification system. *[Reference AFI 33-204, Information Protection Security Awareness, Training and Education (SATE) Program.]*

8.10.4.3.2. A designated official conducts initial SATE training within 60 days of an individual's assignment and training on a recurring basis annually thereafter. Initial and recurring training must be at least one hour in duration. *[Reference AFI 33-204, paragraph 6.1.1.]*

8.10.4.3.3. Personnel that do not require access to or use information systems in the performance of duties are exempt from the initial and recurring one-hour awareness-training requirement. *[Reference AFI 33-204, paragraph 6.1.2.]*

8.10.4.4. Counterintelligence Awareness and Briefing Program. The servicing Air Force Office of Special Investigations (AFOSI) Detachment provides counterintelligence awareness briefings to AF personnel. *[Reference AFCAT 36-2223]*

8.10.4.4.1. After initial training, refresher training is provided every three years thereafter.

8.10.4.4.2. Document initial and refresher in accordance with AFCAT 36-2223.

8.10.4.5. Protection from Terrorism. The designated official provides military personnel training within 180 days of deployment (PCS/TDY to overseas location) and provides civilians training shortly after their initial hiring. Frequency of refresher training is at the discretion of the MAJCOM. *[Reference AFI 31-210, The Air Force Antiterrorist (AT) Program]*

Section 8D--Continuing Security Education/Refresher Training

8.11. Continuing and Refresher Training.

8.11.1. Commanders ensure that each person receives continuing training throughout their duty assignment.

8.11.1.1. Cleared and uncleared personnel will receive refresher Classified National Security Information related training annually in accordance with **Attachment 7**.

8.11.1.2. Personnel performing specialized Classified National Security Information program related functions, such as, classification, declassification and derivative classification actions and security personnel, etc., will receive refresher training commensurate with their knowledge and proficiency in performing required tasks and the dissemination of new policy guidance.

8.11.2. Tailor training to mission needs and design it to address an individual's security responsibilities.

8.11.3. Continuing training must include ensuring individuals have the most current security guidance applicable to their responsibilities.

8.11.4. Other related material to be considered include a general overview of the unclassified controlled information, foreign disclosure, security and policy review processes and protection requirements.

Section 8E-- Access Briefings and Termination Debriefings

8.12. Access Briefings.

8.12.1. Supervisors, security managers or designated officials conduct and document the following access briefings, as appropriate:

8.12.1.1. Brief and execute the SF-312, **Classified Information Nondisclosure Agreement**, prior to granting an individual access to classified information. The SF-312 may also be used to document attestations. *[Reference AFI 31-401, paragraph **5.4.**]*

8.12.1.2. Brief and execute the DD Form 2501, **Courier Authorization**, when an individual is authorized to escort or handcarry classified information. *[Reference AFI 31-401, paragraph **6.7.**]*

8.12.1.3. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to NATO classified information. *[Reference AFI 31-406, paragraph 4.9.]*

8.12.1.4. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to Critical Nuclear Weapons Design Information (CNWDI). *[Reference AFI 31-401, paragraph **1.5.1.3.**]*

8.12.1.5. Brief and execute the AF Form 2583, **Request for Personnel Security Action**, prior to granting an individual access to SIOP-ESI. *[Reference AFI 10-1102, paragraph 6.1.]*

8.12.1.6. The special security officer conducts the SCI indoctrination (inbrief) prior to granting personnel access to SCI. The indoctrination is recorded in the DD Form 1847, **Sensitive Compartment Information Indoctrination Memorandum**. The DD Form 1847-1, **Sensitive Compartment Information Nondisclosure Statement**, is also executed at this time. *[Reference DOD 5105.21-M-1, Chapter 2]*

8.13. Termination Debriefings.

8.13.1. Supervisors, security managers or designated officials conduct and document the following termination debriefings, as appropriate:

8.13.1.1. Debrief individuals having access to classified information or security clearance eligibility when they terminate civilian employment, separate from the military service, have their access suspended, terminated, or have their clearance revoked or denied.

8.13.1.2. Use AF Form 2587, **Security Termination Statement**, to document the debriefing.

8.13.1.3. The debriefing must emphasize to individuals their continued responsibility to:

8.13.1.3.1. Protect classified and unclassified controlled information to which they have had access.

8.13.1.3.2. Report any unauthorized attempts to gain access to such information.

8.13.1.3.3. Adhere to the prohibition against retaining material upon departure.

8.13.1.3.4. And the potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

8.13.2. For NATO access termination debriefing, see AFI 31-406, *Applying NATO Protection Standards*, paragraph 4.10.

8.13.3. Commanders ensure personnel accessed to SCI receive a termination debriefing when access is no longer required, is suspended, or is revoked.

8.13.3.1. The Special Security Office (SSO) conducts the SCI termination debriefing.

8.13.3.2. SCI termination debriefing is documented on the DD Form 1848**, Sensitive Compartment Information Debriefing Memorandum**.

8.13.4. For SIOP-ESI termination briefing, see AFI 10-1102, **Safeguarding the Single Integrated Operational Plan (SIOP).**

8.13.5. Dispose of AF Form 2587 according to AFMAN 37-139.

8.14. Refusal to Sign a Termination Statement. When an individual willfully refuses to execute AF Form 2587, the supervisor, in the presence of a witness:

8.14.1. Debriefs the individual orally.

8.14.2. Records the fact that the individual refused to execute the termination statement and was orally debriefed.

8.14.3. Ensures the individual no longer has access to classified information.

8.14.4. Forwards the AF Form 2587 to the servicing ISPM for Security Information File (SIF) processing according to AFI 31-501.

Section 8F—Program Oversight

8.15. General.

8.15.1. Commanders are responsible for ensuring systems are set up to determine training requirements, develop training, and evaluate effectiveness of the training.

8.15.2. ISPMs will make security education and training a *special interest item* during annual program reviews.

8.15.3. Commanders will ensure that their security education and training program is given close scrutiny during inspections, self-inspections and staff assistance visits (SAVs).

8.15.4. Personnel that have program oversight responsibilities should use a combination of approaches to assess the effectiveness of the security education program, such as, observations, quizzes, surveys, face-to-face interviews, practical demonstrations, etc.

Section 8G - Coordinating Requests for Formal Training

8.16. Coordinating Requests for Training.

8.16.1. Commanders will ensure that requests for formal training are coordinated through unit, installation and MAJCOM training channels.

8.16.2. Requests for in-residence Defense Security Service (DSS) training courses will be processed in accordance with AFCAT 37-2223, **USAF Formal Schools**, regardless of funding method (AF or unit funded), except as stipulated in paragraph **8.16.3.**, below.

8.16.3. When a unit is willing to fund TDY expenses (travel, per-diem, etc.), out-of-cycle attendance at DSS in-residence training courses may be requested. If seating is available, requests will be filled on a first-come, first-serve basis. Submit requests through the MAJCOM to HQ USAF/XOFI (memo and DSS Registration Request) at least 30 days prior to the class start date. The commander's written approval is required. Once coordination has been completed and request approved, the unit will be notified. AF activities that host/sponsor formal on-site training courses or seminars will make them available to as many personnel as possible.

Attachment 7

AIR FORCE INFORMATION SECURITY PROGRAM TRAINING STANDARD

OBJECTIVE: To provide personnel with an understanding and knowledge of the Air Force standards and policies as they related to the DOD information security program, to include basic philosophy, policy, classification process, safeguarding, and security education program. **NOTE**: For training purposes, personnel are categorized and/or identified in the below as security (S) - security professional, specialist and manager); cleared personnel (C) - original classification authorities (OCAs), derivative classifiers, declassifiers, and other personnel that require access to classified information; and/or uncleared personnel (U) - personnel that do not require access. Personnel will receive training (scale value) as indicated during initial, orientation and refresher information security training.

Qualitative Requirements - Proficiency Code Key		
	Scale Value	Definition: The individual
Task Performance Levels	1	Can do simple parts of the task. Needs to be told or shown how to do most of the task. (Extremely limited)
	2	Can do most parts of the task. Needs only help with hardest parts. (Partially Proficient)
	3	Can do all parts of the task. Needs only a spot check of completed work. (Competent)
	4	Can do the complete task quickly and accurately. Can tell or show others how to do the task. (Highly Proficient)
*Task Knowledge Levels	a	Can name parts, tools, and simple facts about the task. (Nomenclature)
	b	Can determine step by step procedures for doing the task. (Procedures)
	c	Can identify why and when the task must be done and why each step is needed. (Operating Principles)
	d	Can predict, isolate, and resolve problems about the task. (Advanced Theory)

Qualitative Requirements - Proficiency Code Key		
**Subject Knowledge Levels	A	Can identify basic facts and terms about the subject. (Facts)
	B	Can identify relationship or basic facts and state general principles about the subject. (Principles)
	C	Can analyze facts and principles and draw conclusions about the subject. (Analysis)
	D	Can evaluate conditions and make proper decisions about the subject. (Evaluation)

Explanations:

* A task knowledge scale value may be used alone or with a task performance scale value to define a level of knowledge for a specific task. (Example: b and 1b)

** A subject knowledge scale value is used alone to define a level of knowledge for subjects not directly
related to any specific task or for a subject common to several tasks.

\- This mark is used alone instead of a scale value to show no proficiency training is provided in the standard.

X This mark is used in course columns to show training required but not given due to limitations in resources.

BASIC INFORMATION SECURITY PROGRAM TRAINING STANDARDS			
SUBJECTS, MATERIALS, AND/OR AREAS	**S**	**C**	**U**
1. POLICY AND PROGRAM MANAGEMENT			
a. Policy			
(1) Purpose and Scope (DOD 5200.1-R, paragraph 1-100)	A	A	A
(2) Policy ((DOD 5200.1-R, paragraph 1-101/AFI 31-401, paragraph **1.1.**)	A	A	A
(3) Philosophy (AFI 31-401, paragraph **1.2.**)	A	A	
b. Program Management			
(1) Program Management (AFI 31-401, paragraph **1.3.**)	A	A	A
(2) Air Force Oversight (AFI 31-401, paragraph **1.4.**)	A	A	
(3) Terms and Definitions (DOD 5200.1-R, Appendix B/AFI 31-501, attachment C)	A	A	
(4) Related Programs (Normally, functional OPR provides training & oversight)			
(a) Personnel Security - Security Forces (XOF)	A	A	A
(b) Industrial Security - Security Forces (XOF)	A	A	A
(c) Operations Security (OPSEC) - Operations (XOO)	A	A	
(d) Emission Security (EMSEC) (SC)	A	A	
(e) Communications Security (COMSEC) (SC)	A		
(f) Intelligence (IN)	A		
(g) Computer Security (COMPUSEC) (SC)	A	A	A
(h) Physical Security - (XOF)	A	A	A
(h) Physical Security - (XOF)	A		
(j) Product Security - Security Forces (XOF)	A		
(k) Freedom of Information Act (FOUO) (SC)	A	A	A
(l) Privacy Act (SC)	A	A	A
(m) Security and Policy Review (PA)	A	A	
(n) Foreign Disclosure (IA)	A	A	
c. Special types of information			
(1) Restricted Data (DOD 5200.1-R, paragraph 1-300/AFI 31-401, paragraph **1.5.**)	A		
(2) Sensitive Compartmented Information (SCI) (DOD 5200.1-R, paragraph 1-301/AFI 31-401, paragraph **1.5.**/AFI 14-302)	A		
(3) Communication Security (COMSEC) Information (DOD 5200.1-R, paragraph 1-301/AFI 31-401, paragraph **1.5.**)	A		

(4) North Atlantic Treaty Organization and Other Foreign Government Information (DOD 5200.1-R, paragraph 1-303)	A		
(5) Controlled Unclassified Information (DOD 5200.1-R, Appendix E/AFI 31-401, **Attachment 3**)	A	A	A
d. Exceptional situations			
(1) Military Operations (DOD 5200.1-R, paragraph 1-400)	A		
(2) Waivers to Requirements (DOD 5200.1-R, paragraph 1-401/AFI 31-401, paragraph **1.6.**)	A		
e. Corrective Actions and Sanctions			
(1) General Policy (DOD 5200.1-R, paragraph 1-500)	A	A	
(2) Sanctions (DOD 5200.1-R, paragraph 1-501/AFI 31-401, paragraph **1.8.**)	B	A	
(3) Reporting of Incidents (DOD 5200.1-R, paragraph 1-502/AFI 31-401, paragraph **1.3.**)	B	A	
f. Reporting Requirements (DOD 5200.1-R, paragraph 1-600/AFI 31-401, paragraph **1.7.**)	A	A	
g. Self-Inspections (DOD 5200.1-R, paragraph 1-700/AFI 31-401, paragraph **1.9.**)	A		
2. ORIGINAL CLASSIFICATION			
a. Original Classification Authority			
(1) Policy (DOD 5200.1-R, paragraph 2-200)	A	A	
(2) Delegation of Authority (DOD 5200.1-R, paragraph 2-301)	A		
(3) Air Force Original Classification Authority Training (DOD 5200.1-R, paragraph 2-202, AFI 31-401, paragraph **2.1.**/32 CFR part 2001)	C		
b. Original Classification Process			
(1) Overview (DOD 5200.1-R, paragraph 2-300)	A	A	
(2) Eligibility for Classification (DOD 5200.1-R, paragraph 2-301)	B		
(3) Possibility of Protection (DOD 5200.1-R, paragraph 2-302)	B		
(4) The Decision to Classify (DOD 5200. 1-R, paragraph 2-303)	B		
(5) Level of Classification (DOD 5200.1-R, paragraph 2-304)	B		
(6) Duration of Classification (DOD 5200,1-R, paragraph 2-305)	B		
(7) Communicating the Decision (DOD 5200.1-R, paragraph 2-306)	B		
b. Special Considerations			
(1) Compilation (DOD 5200.1-R, paragraph 2-400)	A		
(2) The Acquisition Process (DOD 5200.1-R, paragraph 2-401)	A		
(3) Limitations and Prohibitions (DOD 5200.1-R, paragraph 2-402/AFI 31-401, paragraph **2.2.**)	B		
c. Security Classifications and/or Declassification Guides			
(1) Policy (DOD 5200.1-R, paragraph 2-500)	A	A	

(2) Content (DOD 5200.1-R, paragraph 2-501/AFI 31-401, paragraph 2.4.)	C	B	
(3) Approval, Distribution and Indexing (DOD 5200.1-R, paragraph 2-502/AFI 31-401, paragraph 2.4.)	A		
(4) Review, revision and Cancellation (DOD 5200.1-R, paragraph 2-503)	A		
d Information for Private Sources			
(1) Policy (DOD 5200.1-R, paragraph 2-600)	A		
(2) Classification Determination (DOD 5200.1-R, paragraph 2-601)	A		
(3) Patent Secrecy Act (DOD 5200.1-R, paragraph 2-602)	A		
3. DERIVATIVE CLASSIFICATION			
a. Policy and General Requirement			
(1) The Nature of the Process (DOD 5200.1-R, paragraph 3-100)	A	A	
(2) Authority and Responsibility (DOD 5200.1-R, paragraph 3-101)	A	A	
(3) Policy (DOD 5200.1-R, paragraph 3-102)	A	A	
b. Procedures			
(1) General (DOD 5200.1-R, paragraph 3-200)	A	A	
(2) Special Cases (DOD 5200.1-R, paragraph 3-201)	A		
4. DECLASSIFICATION AND REGRADING			
a. Policy (DOD 5200.1-R, paragraph 4-100)	A	A	
b. Declassification Systems (DOD 5200.1-R, paragraph 4-101)	B	A	
c. Declassification Authority (DOD 5200.1-R, paragraph 4-102)	A	A	
d. Declassification and Downgrading Officials (AFI 31-401, paragraph 3.1.)	A	A	
e. Exceptions (DOD 5200.1-R, paragraph 4-103)	A		
f. Declassification Decisions by Original Classifiers			
(1) Requirement (DOD 5200.1-R, paragraph 4-200)	A	A	
(2) The “Ten-Year Rule” (DOD 5200.1-R, paragraph 4-201)	A	A	
(3) Exemption from the “Ten-Year Rule” (DOD 5200.1-R, paragraph 4-202)	A	A	
(4) Extension of Ten-Year Declassification Periods (DOD 5200.1-R, paragraph 4-203)	A	A	
g. Automatic Declassification at 25 Years			
(1) The Automatic Declassification System (DOD 5200.1-R, paragraph 4-300/AFI 31-401, paragraph 3.2./Attachment 4)	A	A	
(2) Exemption of Specific Information (DOD 5200.1-R, paragraph 4-301)	A	A	
h. Mandatory Review for Declassification			
(1) General (DOD 5200.1-R, paragraph 4-400)	A		
(2) Responsibilities and Procedures (DOD 5200.1-R, paragraph 4-401)	A		
(3) Mandatory Declassification (AFI 31-401, paragraph 3.3.)	A		

i. Systematic Review for Declassification (DOD 5200.1-R, paragraph 4-500)	A		
j. Downgrading			
(1) Purpose and Authority (DOD 5200.1-R, paragraph 4-600)	A	A	
(2) Downgrading Decisions during Original Classification (DOD 5200.1-R, paragraph 4-601)	A		
(3) Downgrading at a Later Date (DOD 5200.1-R, paragraph 4-602)	A		
k. Upgrading (DOD 5200.1-R, paragraph 4-700)	A		
l. Classification Challenges (DOD 5200.1-R, paragraph 4-900/AFI 31-401, paragraph **2.3.**)	B	A	
5. FOREIGN GOVERNMENT INFORMATION			
a. Policy and Procedures (DOD 5200.1-R, paragraph 4-800)	A	A	
b. Communication with Foreign Government (DOD 5200.1-R, paragraph 4-801)	A	A	
6. MARKING			
a. General Provisions			
(1) Marking and Designations rules (DOD 5200.1-R, paragraph 5-100)	B	A	
(2) Exceptions (DOD 5200.1-R, paragraph 5-101)	A	A	
(3) Marking Classified Documents and Other Material (DOD 5200.1-R, paragraph 5-102/AFI 31-401, **Section 4B**)	B	A	
b. Specific marking on Documents			
(1) Overall Classification Marking (DOD 5200.1-R, paragraph 5-200)	B	A	
(2) Agency, Office of Origin, and Date (DOD 5200.1-R, paragraph 5-201)	B	A	
(3) Source(s) of Classification (DOD 5200.1-R, paragraph 5-202)	B	A	
(4) Reason for Declassification/Classification (DOD 5200.1-R, paragraph 5-203/AFI 31-401, paragraph **4.2.**)	B	A	
(5) Declassification/Downgrading Instructions (DOD 5200.1-R, Paragraph 5-206)	B	A	
c. Identification of Specific Classified Information (DOD 5200.1-R, Paragraph 5-206)	B	A	
(1) Marking waivers (AFI 31-401, paragraph **4.4.**)	B	A	
(2) Page Marking (DOD 5200.1-R, paragraph 5-207)	B	A	
d. Marking Special Types of Documents			
(1) Documents With component Parts (DOD 5200.1-R, paragraph 5-300)	B	A	
(2) Transmittal Documents DOD 5200.1-R, paragraph 5-301)	B	A	
(3) Classification by Compilation DOD 5200.1-R, paragraph 5-302)	B	A	
e. Translations (DOD 5200.1-R, paragraph, 5-304)	B		
f. Information Transmitted Electronically (DOD 5200.1-R, paragraph 5-305)	B	A	
g. Documents and Material Marked for Training Purposes (DOD 5200.1-R, paragraph 5-306)	B		
h. Files, Folders, and Groups of Documents (DOD 5200.1-R, paragraph 5-307)	B	A	

i. Printed Documents Produced by AIS Equipment (DOD 5200.1-R, paragraph 5-308)	B	A	
j. Working Papers (DOD 5200.1-R, paragraph 6-101)	B	A	
k. Marking Special Types of Materials			
(1) Blue prints, Maps (DOD 5200.1-R, paragraph 5-401)	B	A	
(2) Photographs (DOD 5200.1-R, paragraph 5-402)	B	A	
(3) Slides (DOD 5200.1-R, paragraph 5-403)	B	A	
(4) Films (DOD 5200.1-R, paragraph 5-404)	B	A	
(5) Sound Recordings (DOD 5200.1-R, paragraph 5-405)	B	A	
(6) Microfilms (DOD 5200.1-R, paragraph 5-406)	B	A	
(7) AIS Removable (DOD 5200.1-R, paragraph 5-407)	B	A	
(8) AIS Storage (DOD 5200.1-R, paragraph 5-407/AFI 31-401, paragraph **4.6.**)	B	A	
(9) Labels (DOD 5200.1-R, paragraph 4-409)	B	A	
(10) Intelligence Information (DOD 5200.1-R, 5-410/AFI 31-401, paragraph **4.7.**)	B		
l. Changes in Marking			
(1) Downgrading and Declassification (DOD 5200.1-R, paragraph 5-500)	A	A	
(2) Downgrading and Declassification Earlier Than Scheduled (DOD 5200.1-R, paragraph 5-501)	A		
(3) Upgrading (DOD 5200.1-R, paragraph 5-502)	A		
(4) Posted Notice on Bulky Material (DOD 5200.1-R, paragraph 5-503)	A		
(5) Extensions on Duration (DOD 5200.1-R, paragraph 5-504)	A		
m. Remarking and Using Old Classified Material			
(1) Retaining Old Marking (DOD 5200.1-R, paragraph 5-600)	A		
(2) Earlier Declassification and Extension (DOD 5200.1-R, paragraph 5-601)	A		
n. Foreign Government Information/Equivalent U.S.			
(1) Marking NATO Documents (DOD 5200.1-R, paragraph 5-701)	B		
(2) Marking Other Foreign Government Documents (DOD 5200.1-R, paragraph 5-702)	B	A	
(3) Markings for Foreign Government and NATO Information in DOD Documents (DOD 5200.1-R, paragraph 5-703)	B		
(4) Marking for Transfer to Achieves (DOD 5200.1-R, paragraph 5-704)	B		
7. SAFEGUARDING			
a. Control Measures			
(1) General (DOD 5200.1-R, paragraph 6-100/AFI 31-401, paragraph **5.1.**)	B	A	
(2) Working Papers (DOD 5200.1-R, paragraph 6-101/AFI 31-401, paragraph **5.3.**)	B	A	
b. Access			
(1) Policy (DOD 5200.1-R, paragraph 6-300/AFI 31-401, paragraph **5.18.**)	B	A	A

(2) Administrative Controls (AFI 31-401, paragraph **5.10.**)	B	A	
(3) Granting Access to Classified Information (AFI 31-401, paragraph **5.4.**)	B	A	A
(4) Nondisclosure Agreement (NDA) (AFI 31-401, paragraph **5.5.**)	B	A	
(5) Preventing Publication of Classified Information in the Public (AFI 31-401, paragraph **5.8.**)	A		
(6) Access by Persons Outside the Executive Branch (DOD 5200.1-R, paragraph 6-201/AFI 31-401, paragraph **5.6.**)	B	A	
(7) Access to Information Originating in a Non-DOD Department Agency (AFI 31-401, paragraph **5.9.**)	B	A	
(8) Visits (DOD 5200.1-R, paragraph 6-202)	B	A	
(9) Access by Visitors (AFI 31-401, paragraph **5.7.**)	B	A	
(10) Administrative Controls (AFI 31-401, paragraph **5.10.**)	B	A	
c. Safeguarding			
(1) Care During Working Hours (DOD 5200.1-R, paragraph 6-30/AFI 31-401, paragraph **5.11.**)	B	A	
(2) End-of-Day Security Checks (DOD 5200.1-R, paragraph 6-302/AFI 31-401, paragraph **5.12.**)	B	A	A
(3) Emergency Planning (DOD 5200.1-R, paragraph 6-303)	B	A	
(4) Telephone Conversations (DOD 5200.1-R, paragraph 6-304)	B	A	
(5) Removal of Equipment(DOD 5200.1-R, paragraph 6-305)	A		
(6) Residential Storage (DOD 5200.1-R, paragraph 6-306)	B	A	
(7) Meeting and Conferences DOD 5200.1-R, paragraph 6-307/AFI 31-401, paragraph **5.15.**)	B	A	
(8) Information Located in Foreign Countries (DOD 5200.1-R, paragraph 6-308)	B		
(9) Processing Equipment/Reproduction (DOD 5200.1-R, paragraph 6-309/AFI 31-401, paragraphs **5.17./5.26.**)	B	A	
d. Storage			
(1) General Policy (DOD 5200.1-R, paragraph 6-400)	A	A	A
(2) Standards of Equipment (AFI 31-401, paragraph **5.20.**)	A	A	
(3) Storage of Information (DOD 5200.1-R, paragraph 6-402/AFI 31-401, paragraph **5.20.**)	B	A	
(4) Procuring New Equipment (DOD 5200.1-R, paragraph 6-403/AFI 31-401, paragraph **5.22.**)	B		
(5) Designating and Combinations (DOD 5200.1-R, paragraph 6-404/AFI 31-401, paragraph **5.23.**)	B	A	
(6) Repairing Damaged Containers DOD 5200.1-R, paragraph 6-405/AFI 31-401, paragraph **5.24.**)	B		

(7) Maintenance and Operating Inspections (DOD 5200.1-R, paragraph 6-406/AFI 31-401, paragraph **5.25.**)	A		
e. Reproducing Classified Material			
(1) Policy (DOD 5200.-R, paragraph 6-500)	A	A	
(2) Approving Reproduction (DOD 5200.1-R, paragraph 6-501)	A	A	
(3) Control Procedures (DOD 5200.1-R, paragraph 6-502/AFI 31-401, paragraph **5.27.**)	A	A	
f. Foreign Government Information			
(1) General (DOD 5200.1-R, paragraph 6-600)	B	A	
(2) Top Secret, Secret, Confidential (DOD 5200.1-R, paragraph 6-601)	B		
(3) Restricted Information (DOD 5200.1-R, paragraph 6-602)	B		
(4) Third-Country Transfers (DOD 5200.1-R , paragraph 6-603)	B		
(5) Storage (DOD 5200.1-R, paragraph 6-604)	B		
(6) Protecting Classified Material on Aircraft in Foreign Countries (AFI 31-401, paragraph **5.16.**)	B		
g. Disposition and Destroying Classified Material			
(1) Policy (DOD 5200.1-R, paragraph 6-700)	A	A	
(2) Methods and Standards (DOD 5200.1-R, paragraph 6-701/AFI 31-401, paragraph **5.29.**)	A	A	
(3) Retention of Classified Records (AFI 31-401, paragraph **5.28.**)	A	A	
h. Alternative or Compensatory Control Measures (DOD 5200.1-R, paragraph 6-800/AFI 31-401, paragraph **5.30.**)	A		
8. TRANSMISSION AND TRANSPORTATION			
a. Methods of Transmission or Transportation			
(1) Policy (DOD 5200.1-R, paragraph 7-100/Air Force Policy (AFI 31-401, Paragraph **6.1.**)	B	A	
(2) Transmitting Top Secret Information (DOD 5200.1-R, paragraph 7-101/AFI 31-401, paragraph **6.2.**)	B	A	
(3) Transmitting Secret Information (DOD 5200.1-R, paragraph 7-102/AFI 31-401, paragraph **6.3.**)	B	A	
(4) Transmitting Confidential Information (DOD 5200.1-R, paragraph 7-103/AFI 31-401, paragraph **6.4.**)	B	A	
(5) Transmission of Classified Material to Foreign Governments (DOD 5200.1-R, paragraph 7-104/appendix H/AFI 31-401, paragraph **6.5./Attachment 6**)	B		
(6) Shipment of Freight (DOD 5200.1-R, paragraph 7-105)	B		
b. Preparation of Material for Transmission			

(1) Envelopes or Containers (DOD 5200.1-R, paragraph 7-200/AFI 31-401, paragraph **6.6.**) (2) Addressing (DOD 5200.1-R, paragraph 7-201)	B	A	
c. Escort or Hand-Carry of Classified Material			
(1) General Provision (DOD 5200.1-R, paragraph 7-300)	B	A	
(2) Documentation (DOD 5200.1-R, paragraph 7-301)	B	A	
(3) Escort or Hand-Carrying Classified Aboard Commercial Passenger Aircraft (DOD 5200.1-R, paragraph 7-302/AFI 31-501, paragraph **6.9.**)	B		
9. SPECIAL ACCESS PROGRAMS (SAPs)			
a. Policy (DOD 5200.1-R, paragraph 8-100)	A	A	
b. Special Access Controls (DOD 5200.1-R, paragraph 6-801)	A		
c. SAP Procedures (DOD 5200.1-R, paragraph 8-101)	A		
d. Control and Administration (DOD 5200.1-R, paragraph 8-102/AFI 31-501, paragraph **7.1.**)	A		
e. Nicknames and Code Words (DOD 5200.1-R, paragraph 8-103F/AFI 31-501, paragraph **7.2.**)	A		
f. Establishment of DOD SAPs (DOD 5200.1-R, paragraph 8-103/AFI 31-501)	A		
g. Reviews of SAPs (DOD 5200.1-R, paragraph 8-104)	A		
h. Annual Reports and Revalidation (DOD 5200.1-R, paragraph 8-105)	A		
i. Interim Reports (DOD 5200.1-R, paragraph 8-106)	A		
j. Change of Classification (DOD 5200.1-R, paragraph 8-107)	A		
k. Termination and Transitioning of SAPs (DOD 5200.1-R, paragraph 8-108)	A		
10. SECURITY EDUCATION AND TRAINING			
a. Policy			
(1) General Policy (DOD 5200.1-R, paragraph 9-100/AFI 31-401, paragraph **8.1.**)	A	A	A
(2) Methodology (DOD 5200.1-R, paragraph 9-101/AFI 31-401, paragraph **8.2.**)	A	A	A
b. Initial Orientation			
(1) Cleared Personnel (DOD 5200.1-R, paragraph 9-200/AFI 401, paragraph **8.4.**)	B	A	
(2) Uncleared Personnel (DOD 5200.1-R, paragraph 9-201/AFI 31-403 paragraph **8.5.**)	B	A	A
c. Special Requirements			
(1) General (5200.1-R, paragraph 9-300)	A	A	
(2) Original Classifiers (DOD 5200.1-R, paragraph 9-301/AFI 31-401, paragraph **8.6.**)	B	A	
(3) Declassification Authorities Other Than Original Classifiers (DOD 5200.1-R, paragraph 9-302/AFI 31-401, paragraph **8.7.**)	B	A	

d. Derivative Classifiers, Security Personnel and Others (DOD 5200.1-R, paragraph 9-303/AFI 31-401, paragraph **8.8.**)	B	A	
e. Continuing Security Education/Refresher Training			
(1) Continuing Security Education (DOD 5200.1-R, paragraph 9-400)	B	A	A
(2) Refresher Training (DOD 5200.1-R, paragraph 9-401)	B	A	A
f. Termination Briefings			
(1) General Policy (DOD 5200.1-R, paragraph 9-500)	A	A	
(2) Procedures (AFI 31-403, paragraph 1.13)	B		
(3) Refusal to Sign Termination Statement (AFI 31-401, paragraph **8.14.**)	B		
g. Program Oversight (DOD 5200.1-R, paragraph 9-600)	B		
h. Train the trainer	B		
i. Lessons Learned	A	A	
11. ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION			
a. Policy (DOD 5200.1-R, paragraph 10-100/AFI 31-401, paragraph **9.1.**)	A	A	A
b. Reporting (DOD 5200.1-R, paragraph 10-101/AFI 31-401, paragraph **9.2.**)	B	A	A
c. Inquiry/Investigation (DOD 5200.1-R, paragraph 10-102/AFI 31-401, paragraph **9.3.**)	B	A	
d. Results of Inquiry/Investigation (DOD 5200.1-R, paragraph 10-104/AFI 31-401, paragraph **9.4.**)	B		
e. Additional Investigations (DOD 5200.1-R, paragraph 10-107)	B		
f. Verification, Reevaluation, and Damage Assessment (DOD 5200.1-R, 10-104/AFI 31-401, paragraph **9.5.**)	A	A	
g. Debriefing in Cases of Unauthorized Access (DOD 5200.1-R, paragraph 10-105)	A		
h. Management and Oversight (DOD 5200.1-R, paragraph 10-106/AFI 31-401, paragraph **9.6.**)	B	A	A
i. Unauthorized Absences (DOD 5200.1-R, paragraph 10-108/AFI 31-401, paragraph **9.7.**)	A		

Attachment 12

IC 2000-2 TO AFI 31-401, INFORMATION SECURITY PROGRAM MANAGEMENT

15 DECEMBER 2000

SUMMARY OF REVISIONS

This change updates the office of primary responsibility; updates the table of contents to reflect these changes; completely revises **Section 4B** to include guidance on marking classified audio and video tapes; and, implements a standard level of security for protecting classified material and components on aircraft (paragraph **5.16.**). See the last attachment of the publication, IC 00-2, for the complete IC. A bar (|) indicates revision from the previous edition.

OPR: HQ USAF/XOFI (Deborah Ross (Classification Management), Linda Patten (Safeguarding), and Danny Green (Security Education)

Chapter 4-Marking

Section 4B Specific Markings on Documents

4.6. Audio and Video Tapes

4.7. Removable AIS Storage Media

4.8. Intelligence

Chapter 5-Safeguarding

Section 5C Safeguarding

5.16. Protecting Classified Material and Components on Aircraft

Chapter 4

MARKING

Section 4B-Specific Markings on Documents [Reference DOD 5200.1-R, Chapter 5, Section 2]

4.2. Reason for Classification. In the case of exempted information, the reason(s) for classification must be consistent with the exemption category(ies). [Reference DOD 5200.1-R, Paragraph 5-203]

4.3. Declassification Instructions. The exemption category(ies) must be consistent with the reason(s) used for classifying the information. [Reference DOD 5200.1-R, Paragraph 5-204]

4.4. Marking Waivers. Requesters send requests for marking waivers through command ISPM channels to HQ USAF/XOFI. For Special Access Program (SAP) marking requirements, send requests through command SAP channels to SAF/AAZ. [Reference DOD 5200.1-R, Paragraph 5-206d]

4.5. Special Control and Similar Notices. [Reference DOD 5200.1-R, Paragraph 5- 208]

4.5.1. Communications Security (COMSEC). See AFI 33-211, Communications Security (COMSEC) User Requirements, for additional guidance on marking COMSEC media. [Reference DOD 5200.1-R, Paragraph 5-208d]

4.5.2. Technical Documents. See AFI 61-204, Disseminating Scientific and Technical Information, for guidance on disseminating technical documents. [Reference DOD 5200.1-R, Paragraph 5-208e]

4.5.3. SAPs. See AFI 16-701, Special Access Programs, for additional guidance on SAP documents. [Reference DOD 5200.1-R, Paragraph 5-208f]

4.5.4. Other Special Notices. See Attachment 2 for references. [Reference DOD 5200.1-R, Paragraph 5-208h]

4.6. Audio and Video Tapes. Personnel responsible for marking and maintaining original classified audio and video tapes that document raw test data do not need to include footers/headers showing the applicable classification markings. However, the required classification markings must be placed on the outside of the container and reel. All copies made from the original tapes must include headers/footers that show the applicable classification markings. This will help ensure that valuable historical test data is not inadvertently erased during the classification marking process. [Reference DOD 5200.1-R, Paragraphs 5-404 and 5-405]

4.7. Removable AIS Storage Media. Personnel use SF Form 706, Top Secret ADP Media Classification Label; SF Form 707, Secret ADP Media Classification Label; SF Form 708, Confidential ADP Media Classification Label; SF Form 711, ADP Data Descriptor Label, on removable AIS storage media. These are available through the Air Force Publications Distribution system. [Reference DOD 5200.1-R, Paragraphs 5-407 and 5-409a-b]

4.8. Intelligence. [Reference DOD 5200.1-R, Paragraph 5-410]

4.8.1. See AFI 14-302, Control, Protection, and Dissemination of Sensitive Compartmented Information, for Air Force policy on intelligence. [Reference DOD 5200.1-R, Paragraph 5-410a-b]

4.8.2. The Special Security Office (SSO) is the focal point for release and dissemination of SCI. The Director of Central Intelligence Directive 5/6, Intelligence Disclosure Policy, provides criteria for release of intelligence to foreign officials. [Reference DOD 5200.1-R, Paragraph 5-410c]

Chapter 5

SAFEGUARDING

5.16. Protecting Classified Material and Components on Aircraft. Classified material and components are routinely carried on USAF aircraft. The purpose of this paragraph is to provide minimum standards for the protection of classified material and components while minimizing the impact on aircrew operations. The following minimum standards are established to provide cost effective security of classified material and components and to ensure detection of unauthorized access.

5.16.1. Aircraft commanders (owners/users) are responsible for the protection of classified material and components aboard their aircraft whether on a DOD facility, at a civilian airfield, or when stopping in foreign countries in accordance with DOD 5200.1R, paragraph 6-300. Aircraft commanders should consult with the local ISPM or senior security forces representative for assistance in complying with these requirements.

5.16.2. To provide security-in-depth for classified components and material on aircraft, park the aircraft in an established restricted area or equivalent if the aircraft is designated Protection Level (PL) 1, 2, or 3. Refer to AFI 31-101, Air Force Installation Security Program, for details about protection levels.

5.16.2.1. Lock the aircraft, when possible, using a GSA-approved changeable combination padlock (Federal Specification FF-P-110 series) to secure the crew entry door, and/or

5.16.2.2. Place all removable classified material (e.g., paper documents, floppy disks, videotapes) in a storage container secured with a GSA-approved lock. The storage container must be a seamless metal (or similar construction) box or one with welded seams and a lockable hinged top secured to the aircraft. Hinges must be either internally mounted or welded. Containers installed for storage of weapons may also be used to store classified material even if weapons/ammunition are present, provided the criteria listed above have been met.

5.16.2.2.1. Have the aircraft and container checked for tampering every 12 hours. If unable to comply with the 12 hours due to crew rest, perform these checks no later than 1 hour after official end of crew rest.

5.16.2.2.2. Zeroize keyed communications security (COMSEC) equipment as required by AFKAG-1, Air Force Communications Security (COMSEC) Operations.

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

5.16.3. To provide security-in-depth for classified components and material on PL 4 or non-PL aircraft, park the aircraft in a controlled area. PL 4 and non-PL aircraft should not be parked in a restricted area due to use of force limitations.

5.16.3.1. Lock the aircraft using a GSA-approved changeable combination padlock (Federal Specification FF-P-110 series) to secure the crew entry door, and

5.16.3.2. Secure removable classified material IAW paragraph **5.16.2.2.** or **5.16.2.3.**

5.16.4. At non-U.S. controlled locations, host nation restricted/controlled areas may be used only if all material and components aboard the aircraft have been approved for release to the host nation by a cognizant foreign disclosure authority. Material should be secured IAW paragraph **5.16.2.** for restricted areas and paragraph **5.16.3.** for controlled areas.

5.16.5. If the aircraft cannot be parked in a restricted/controlled area:

5.16.5.1. Place removable classified material in a storage container and secure the container as described in paragraph **5.16.2.2.** Lock all aircraft egress points or secure them from the inside. Seal the aircraft with tamperproof seals such as evidence tape, numerically accountable metal, or plastic seals.

5.16.5.2. If the aircraft can be locked and sealed but there is no storage container, remove all removable classified material and store it in an approved security container in an authorized U.S. facility. Classified components (e.g., AAR 47, ALE 47, etc.) may be stored in a locked and sealed aircraft.

5.16.5.3. If the aircraft cannot be locked and sealed and no storage container is available, off-load all classified material and components to an approved security container in an authorized U.S. facility.

5.16.5.4. If none of the above criteria can be met, U.S. cleared personnel must provide continuous surveillance. Foreign national personnel cleared by their government may be used if all material and compo-

nents aboard the aircraft have been approved for release to the host nation by a cognizant foreign disclosure authority.

5.16.6. MAJCOM/FOA/DRUs determine specific risk management security standards for weather diverts and in-flight emergencies.

5.16.7. If evidence exists of unauthorized entry, initiate a security investigation IAW **Chapter 9** of this AFI.

Attachment 1

References

AFI 31-101, Air Force Installation Security Program

AFKAG-1, Air Force Communications Security (COMSEC) Operations

AFKAG-1, Air Force Communications Security (COMSEC) Operations

Attachment 13

IC 2001-1 TO AFI 31-401, INFORMATION SECURITY PROGRAM MANAGEMENT

17 AUGUST 2001

SUMMARY OF REVISIONS

This revision incorporates Interim Change IC 2001-1. This change updates the table of contents to reflect new attachments for Original Classification Authorities, an Appointment of Inquiry Official Memorandum, and a Preliminary Inquiry of Security Incident Report; updates the office of primary responsibility for this Air Force Instruction (AFI); clarifies Standard Form (SF) 311, ***Agency Information Security Program Data***, reporting requirements; clarifies authority for nuclear weapon security classification policy and how to obtain the policy; adds guidance for commanders and/or staff agency chiefs to process administrative sanctions; adds the requirement for HQ USAF/XOFI to conduct program reviews; completely replaces **Chapter 9**, Actual or Potential Compromise of Classified Information, to implement additional reporting and investigative procedures concerning security incidents; implements automatic declassification extensions; incorporates guidance on systematic declassification reviews; clarifies safeguarding requirements for secure rooms; and, updates handcarrying classified information policy to include laptops. See the last attachment of the publication, IC 01-3, for the complete IC. A bar (|) indicates revision from the previous edition.

OPR: HQ USAF/XOFI (Deborah Ross)

Chapter 1

POLICY AND PROGRAM MANAGEMENT

1.4.4. HQ USAF/XOFI will visit MAJCOMs, DRUs, and FOAs to review their information security programs. HQ USAF/XOFI will work with MAJCOM, DRU, and FOA ISPMs to determine frequency and visit dates.

1.7. Reporting Requirements. *[Reference DoD 5200.1-R, Paragraph 1-600]*

1.7.1. MAJCOM, FOA, and DRU ISPMs will submit the SF Form 311, ***Agency Information Security Program Data*** (available at **http://www.gsa.gov/forms**), report to HQ USAF/XOFI by 1 September of each year. MAJCOM/DRU/FOAs sample data for Item 6 (Number of Classification Decisions) during a consecutive 2 week period each fiscal year quarter (Nov-Jan, Feb-Apr, May-Jul, and Aug). In the last quarter the 2 week period must be set during August since the reports are required by 1 September. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

1.8.3. Commanders and/or staff agency chiefs take and process administrative sanctions/actions for civilian employees in accordance with AFI 36-704, *Discipline and Adverse Actions* and in accordance with AFI 36-2907, *Unfavorable Information File (UIF) Program*, for military personnel. Contact the servicing civilian or military personnel flight office if assistance is needed.

Chapter 2

ORIGINAL CLASSIFICATION

2.1.3. HQ USAF/XOFI will maintain the master list of Air Force OCAs (see **Attachment 10**). Periodically, HQ USAF/XOFI will request OCA validation from the MAJCOMs, FOAs, and DRU ISPMs.

2.1.3.1. Personnel will submit requests for changes or new requests through ISPM command channels as they occur.

2.1.3.2. See paragraph **8.6.** and **8.11.1.2.** for OCA training requirements.

2.5. Nuclear Weapons Classification Policy. The DOD and the Department of Energy (DOE) issue joint security classification guidance for information relating to nuclear weapons. The Air Force issues security classification policy (AFI 31-407) for nuclear weapons surety information. Most of these products are classified and users will require the appropriate security clearance before accessing them. Users may obtain copies of Joint DOD/DOE classification guides through DTIC at a cost. Users forward requests for copies of the Air Force security classification policy to HQ USAF/XOFI (1340 Air Force Pentagon, Washington DC 20330-1340) through command ISPM channels. Requests must include the name, address, and phone number of the activity point of contact, and the point of contact's level of access. ISPMs will validate this information before submitting the requests to HQ USAF/XOFI. For all other Air Force or other agency guides, go direct to the originator. Users refer to DOD 5200.1-I, *DOD Index of Security Classification Guides*, to determine what other guides relating to nuclear weapons classification guidance are needed. DOD 5200.1-I can be obtained from DTIC.

Chapter 3

DECLASSIFYING AND DOWNGRADING INFORMATION

3.2. Automatic Declassification. According to Executive Order 12958, *Classified National Security Information*, Section 3.4, all Air Force activities that possess classified information that are of permanent historical value and are 25 years old or older should have completed a declassification review of these documents by 17 April 2000.

3.2.1. The 17 April 2000 suspense date has been extended for two groups of records (multiagency and non-multiagency) according to Executive Order 13152, Amendment to Executive Order 12958.

3.2.1.1. The new suspense date for documents still requiring a review that do not contain multiagency equities is 17 October 2001. This applies to all Air Force activities that did not meet the original suspense for reviewing these records (see paragraph **3.2.**).

3.2.1.2. The new suspense date for documents still requiring a review that contain multiagency or intelligence equities is 17 April 2003. MAJCOMs/FOAs/DRUs found to be eligible for the new referral suspense are: AFDO, ACC, AFMC, AFOTEC, AFOSI, AIA, NAIC, AFHSO, and AFTAC.

3.2.2. The Air Force Twenty Five-Year Automatic Declassification Plan (**Attachment 4**) provides specific policy and guidance on performing automatic declassification reviews within the Air Force. This plan is still valid even though some of the suspense dates have changed as indicated in **3.2.1.** above.

3.2.3. The process of automatic declassification evolved into systematic declassification after April 2000.

3.4. Systematic Review for Declassification. Activities will set up an annual schedule for conducting systematic declassification reviews for the following records:

3.4.1. Records of permanent historical value prior to their twenty-fifth birthday. These records will be reviewed and appropriate action taken by 31 Dec of the same year of their twenty-fifth birthday (25 years from the origination date).

3.4.2. Records of permanent historical value that have been exempted from automatic declassification prior to their tenth birthday. These records will be reviewed and appropriate action taken by 31 Dec of the tenth year of their exemption (ten years from the exemption date).

3.4.3. Other records. Activities will set up a reasonable schedule for conducting declassification reviews for all other classified records once a review of records described in paragraphs **3.4.1.** and **3.4.2.** have been completed.

3.4.4. It is the intent of the Air Force not to transfer permanently valuable records to the National Archives Records Administration until they can be declassified without bringing harm to the national security. *[Reference DoD 5200.1-R, Section 5]*

3.5. Policy. When information is declassified, it is not releasable to the public until it has been approved for release through the security review process according to AFI 35-205. The same holds true for declassified or unclassified information that will be placed on an Internet site that can be accessed by the public.

Chapter 5

SAFEGUARDING

5.20. Storage of Classified Information. ***[Reference DoD 5200.1-R, Paragraph 6-402]***

5.20.1. Storage of Secret Information. In addition to the methods used for protecting Secret information described in DoD 5200.1-R, paragraph 6-402b, Secret information may be stored in an open storage area provided security-in-depth exists (see paragraph **5.20.2.**), and one of the following supplemental controls is used:

5.20.1.1. The open storage area shall be subject to continuous protection by cleared guard or duty personnel;

5.20.1.2. Cleared guard or duty personnel shall inspect the open storage area once every four hours; or

5.20.1.3. An intrusion detection system (IDS) meeting the requirements of DoD 5200.1-R, Appendix G with the personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

5.20.2. Security-In-Depth. Security-in-depth can be one or more of the following security measures as long as they are adequate to prevent against unauthorized access: installation perimeter fence lines, entry control points, controlled and restricted area designations, base patrol coverage, and locked building. *[Reference DoD 5200.1-R, Paragraph 6-402 and Appendix B]*

5.20.3. Authority for Delineating the Appropriate Security Measures. If these requirements cannot be met because of local conditions, ISPMs determine alternative methods under the provisions of DoD 5200.1-R, paragraph 6-800. Military commanders do so when it occurs during a military operation as described in DoD 5200.1-R, paragraph 1-400. *[Reference DoD 5200.1-R, Paragraph 6-402d(1)]*

5.20.4. Replacement of Combination Locks. Commanders must ensure all combination locks on GSA approved security containers and doors are replaced with those meeting Federal Specification FF-L-2740 starting with those storing the most sensitive information according to the priority matrix in DoD 5200.1-R, Appendix G. There is no deadline for completing this effort, as it was initially an unfunded requirement. However, commanders must pursue funding and implement the retrofits as soon as possible. *NOTE:* Commanders will designate security containers at locations identified for closure as a low priority for replacing locks when there is a strong possibility that the security containers will not be used at another location. *[Reference DoD 5200.1-R, Paragraph 6-402e]*

Chapter 6

TRANSMISSION AND TRANSPORTATION

6.1. General Policy.

6.1.1. Handcarrying Classified Material During Temporary Duty (TDY) Travel. Handcarrying classified material during TDY poses a risk and should be done as a last resort in critical situations. Whenever possible, personnel will use standard secure methods for relaying the data, e.g., mail through secure channels or through approved secure electronic means. Authorizing officials must assess the risk before authorizing the handcarrying of classified material. Some factors to consider during the risk assessment process are:

6.1.1.1. The environment in which the material will be handcarried. Consider the chances of the material being apprehended by unauthorized personnel. The servicing Air Force Office of Special Investigations office should be able to assist in determining the risks associated with the environment.

6.1.1.2. The sensitivity of the information. Consider the damage it could cause the United States if the information was compromised.

6.1.1.3. The availability of authorized facilities for storing the classified during overnight layovers, at the TDY location, etc. Consider storing the material at a U.S. military installation or other government facility.

6.1.2. Laptop Computers are High Risk. Because of their commercial value, laptop computers are an especially high risk when used to transport classified information. When using laptops to handcarry classified information, couriers must ensure both laptop and disks are prepared according to paragraph **6.6.5.** In addition, as required for all classified material, couriers must take special care to ensure laptops and disks are kept under constant surveillance or in secure facilities/containers at all times.

6.1.3. Air Force Office of Primary Responsibility for Transmission and Transportation Policy. HQ USAF/XOFI establishes Air Force procedures for transmission and transportation of classified information and material. *[Reference DoD 5200.1-R, Paragraph 7-100a]*

6.1.4. Transmitting Classified Material by Pneumatic Tube Systems. Installation commanders approve the use of pneumatic tube systems and ensure that the equipment and procedures provide adequate security. *[Reference DoD 5200.1-R, Paragraph 7-100a]*

6.1.5. Transmitting COMSEC Information. Personnel may get information about transmitting and transporting COMSEC information through their local COMSEC manager. *[Reference DoD 5200.1-R, Paragraph 7-100b]*

6.1.6. Releasing Other Agency Information Outside of the Department of Defense. Personnel go direct to owners of other agency information to request permission to release the information outside the Department of Defense. *[Reference DoD 5200.1-R, Paragraph 7-100d]*

6.6.5. Laptop Computer and Disk Preparation Requirements. Couriers must ensure that:

6.6.5.1. Laptops and disks are both password protected.

6.6.5.2. Laptops and disks are marked according to DoD 5200.1-R, Paragraphs 5-407, 5-408, and 5-409a and b.

6.6.5.3. Removable disks are separated from the computer and are double wrapped according to this AFI, **Section 6B**, and DoD 5200.1-R, paragraph 7-200.

6.6.5.4. Laptops have an outer container when the classified data is stored in the internal memory or maintained on fixed storage media.

6.6.5.5. Laptops and disks containing classified information are kept under constant surveillance or stored in secure containers/facilities.

6.7.1.1. The unit commander, staff agency chief, or security manager authorizes appropriately cleared couriers to handcarry classified material on commercial flights. See DoD 5200.1-R, paragraph 7-301, for required documentation and this AFI, paragraph **6.1.2.**, for a cautionary statement regarding handcarrying classified material.

6.7.1.2. The unit commander, staff agency chief, or security manager authorizes appropriately cleared couriers to handcarry classified material by means other than on commercial flights.

Chapter 9

ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

9.1. Policy. *[Reference DOD 5200.1-R, Chapter 10]*

9.1.1. It is Air Force policy that security incidents will be thoroughly investigated to minimize any possible damage to national security. The investigation will identify appropriate corrective actions that will be immediately implemented to prevent future security incidents. Further, if the security incident leads to the actual or probable compromise of classified information, a damage assessment will be conducted to judge the effect that the compromise has on national security.

9.2. Definitions.

9.2.1. Security incidents as used in this AFI pertain to any security violation or infraction as defined in EO 12958. Security incidents may be categorized as:

9.2.1.1. Security Violation. Any knowing, willful or negligent action:

9.2.1.1.1. That could reasonably be expected to result in an unauthorized disclosure of classified information.

9.2.1.1.2. To classify or continue the classification of information contrary to the requirements of this order or it's implementing directives.

9.2.1.1.3. To create or continue a special access program contrary to the requirements of EO 12958.

9.2.1.2. Security Infraction. Any knowing, willful or negligent action contrary to the requirements of EO 12958 that is not a security violation.

9.2.2. A compromise of classified information occurs when unauthorized individuals have had access to the classified information.

9.2.3. A probable compromise of classified information is when an investigating official concludes that a compromise of classified information has more than likely occurred as a result of a security incident.

9.3. Automated Information System (AIS) Deviations. Coordinate all security deviations involving AIS with the local ISPM and computer security personnel to begin an evaluation on the impact of the incident to national security and the organization's operations. If communication security (COMSEC) material is involved, refer to AFI 33-212, *Reporting COMSEC Deviations*.

9.4. Sensitive Compartmented Information (SCI) Incidents. To report SCI incidents refer to AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* (FOUO).

9.5. Classification.

9.5.1. Classify security incident notices, appointment of inquiry official memorandums, and security incident reports at the same level of classification as the information compromised if they contain classified information or if they provide sufficient information that would enable unauthorized individuals to access the classified information in an unsecure environment. In the latter case, the documentation must remain classified until the information has been retrieved and appropriately safeguarded. Do not classify memorandums and reports pertaining to security incidents that have occurred in the AIS environment when the system has been appropriately purged and the correspondence does not contain other classified information.

9.5.1.1. Classify security incident notices, memorandums, and reports according to the classified source from which they are derived. Refer to DOD 5200.1-R, Chapter 3.

9.5.1.2. Mark security incident notices, memorandums, and reports using derivative classification procedures. Refer to DOD 5200.1-R, Chapter 5.

9.5.2. All security incident reports will, as a minimum, be marked "For Official Use Only." Refer to AFI 37-131, *Freedom of Information Act Program*.

9.6. Public Release. Security incident reports cannot be released into the public domain until they have undergone a security review. *[Reference AFI 35-101, Public Affairs Policies and Procedures, Chapter 15]*

9.7. Reporting and Notifications.

9.7.1. Personnel who learn of a security incident must promptly report it to their commander, supervisor, or security manager who will in-turn report the incident to the servicing ISPM by the end of the first duty day.

9.7.2. After assigning a case number beginning with calendar year, base, and sequential number for tracking purposes, the ISPM will:

9.7.2.1. Coordinate with the organization security manager to ensure the commander has been briefed on the incident. The ISPM will brief the commander if the security manager is unable to do so or when the incident is reported directly to the ISPM.

9.7.2.2. Report compromises/probable compromises for the following incidents through command ISPM channels to HQ USAF/XOFI:

9.7.2.2.1. Classified in the public media.

9.7.2.2.2. Foreign intelligence agencies.

9.7.2.2.3. Criminal activity.

9.7.2.2.4. NATO classified information.

9.7.2.2.5. Foreign government information.

9.7.2.2.6. Restricted Data (RD) or Formerly Restricted Data (FRD).

9.7.2.2.7. Disclosure to foreign nationals.

9.7.2.3. Notify the local AFOSI when the circumstances involve criminal activity or foreign intelligence agencies.

9.7.2.4. Notify SAF/AAZ when the compromise involves special access information through the appropriate special access program channels.

9.7.3. The appointing authority will notify the OCA, or the originator when the OCA is not known, when it is determined there is a compromise, probable compromise, or loss of classified information. Refer to paragraph **9.5.1.** of this AFI for security classification marking requirements.

9.8. Preliminary Inquiry. An informal inquiry to determine if classified information has been lost or compromised so that a damage assessment can be completed and the appropriate corrective action can be taken.

9.8.1. The commander or staff agency chief of the activity responsible for the security incident will appoint an inquiry official to conduct a preliminary inquiry. Use the requirements of AFI 90-301, *Inspector General Complaints*, Chapter 2.25, when determining whom to appoint. See **Attachment 8** for a sample appointment memorandum. Refer to paragraph **9.5.1.** of this AFI for appointment memorandum classification requirements.

9.8.1.1. When security incidents occur because of unauthorized transmission of classified material, the sending activity appoints the inquiry official and conducts the inquiry.

9.8.1.2. Inquiry officials will coordinate their actions with the servicing ISPM and the staff judge advocate's office.

9.8.2. The preliminary inquiry will determine if classified material was compromised, the extent of the compromise, and the circumstances surrounding the compromise.

9.8.3. A preliminary report will be completed using the sample report format at **Attachment 9** and submitted to the appointing official through the ISPM. The ISPM will provide their concurrence/nonconcurrence with the report and forward it to the appointing official for action. Refer to paragraph **9.5.** of this AFI for report classification requirements.

9.8.4. The report from the preliminary inquiry will be sufficient to resolve the security incident if:

9.8.4.1. The inquiry determines that loss or compromise of classified information has not occurred.

9.8.4.2. The inquiry determines that loss or compromise of classified information has occurred, but there is no indication of significant security weakness.

9.8.4.3. The appointing official determines that no additional information will be obtained by conducting a formal investigation.

9.8.5. If the report from the preliminary inquiry is not sufficient to resolve the security incident, the appointing authority initiates a formal investigation. The preliminary inquiry report will become part of any formal investigation. If the inquiry is closed out as a compromise or probable compromise the appointing authority notifies the OCA to perform a damage assessment.

9.9. Damage Assessment.

9.9.1. A damage assessment is an analysis to determine the effect of a compromise of classified information on the national security. It will be initiated upon notification of a probable or actual compromise to verify and reevaluate the information involved. Damage assessment reports will be classified and marked according to the classification guidance provided on the information being addressed in the reports.

9.9.2. The OCA must:

9.9.2.1. Set up damage assessment controls and procedures.

9.9.2.2. Notify HQ USAF/XOFI through command ISPM channels that a damage assessment is being done.

9.9.2.3. Provide HQ USAF/XOFI through ISPM channels a copy of the completed damage assessment report.

9.10. Formal Investigation. A detailed examination of evidence to determine the extent and seriousness of the compromise of classified information. The formal investigation will fix responsibility for any disregard (deliberate or inadvertent) of governing directives which led to the security incident.

9.10.1. The commander or staff agency chief of the activity responsible for the security incident will appoint an investigative official to conduct an investigation.

9.10.2. The formal investigation may be initiated without a preliminary inquiry if it is deemed prudent due to the seriousness of the security incident.

9.10.3. The formal investigation will include the preliminary inquiry if one has been conducted.

9.11. Management and Oversight.

9.11.1. The inquiry/investigative official will route the completed report through the servicing ISPM and staff judge advocate's office for review before forwarding it to the appointing authority.

9.11.2. The appointing authority will:

9.11.2.1. Close the inquiry/investigation unless MAJCOM, DRU, or FOA directives indicate otherwise.

9.11.2.2. Determine if administrative or disciplinary action is appropriate. See AFI 31-501, *Personnel Security Program Management*, Chapter 8 and applicable military and civilian personnel publications.

9.11.2.3. Debrief anyone who has had unauthorized access using AF Form 2587.

9.11.2.4. Forward a copy of the completed report to the ISPM identifying corrective actions taken.

9.11.2.5. Dispose of the report according to the instructions in AFMAN 37-139, *Records Disposition Schedule.*.

9.11.3. The ISPM will:

9.11.3.1. Provide technical guidance.

9.11.3.2. Monitor the status of security incidents.

9.11.4. Inquiry/investigative officials must complete inquiry/investigations within 30 duty days from appointment.

9.12. Unauthorized Absences. Report unauthorized absences to the ISPM and appropriate AFOSI detachment. *[Reference DOD 5200.1-R, Paragraph 10-108]*

Attachment 1

References

AFI 35-101, *Public Affairs Policies and Procedures*

AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* (FOUO)

AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to foreign Governments and International Organizations* (C)

AFI 36-704, *Discipline and Adverse Actions*

AFI 36-2907, *Unfavorable Information File (UIF) Program*

AFI 90-301, *Inspector General Complaints*

AFI 35-205, Air Force Security and Policy Review Program (DELETE)

Attachment 8

APPOINTMENT OF INQUIRY OFFICIAL MEMORANDUM

DEPARTMENT OF THE AIR FORCE

AIR FORCE UNIT HEADING

MEMORANDUM FOR

FROM:

SUBJECT:Appointment of Inquiry Official, Incident No.

You are appointed to conduct a preliminary inquiry into security incident (number). The incident involves (provide a short summary). Refer to AFI 31-401, *Information Security Program Management*, paragraph **9.5.**, for security classification requirements.

The purpose of this inquiry is to determine whether a compromise occurred and to categorize this 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 records and files pertinent to this inquiry. Your records indicate that 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 Security Program Manager (ISPM).

Contact (name and phone number of the ISPM), for a briefing on your responsibilities, conduct of, and limitations of this inquiry. Your written report will be forwarded through the ISPM to me within 30 duty days from the date of your appointment. As a minimum, your report must contain the following:

a. A statement that a compromise or probable compromise did or did not occur.

b. Category of the security incident.

c. Cause factors and responsible person(s).

d. Recommended corrective actions needed to preclude a similar incident.

Notify me immediately at (phone number) if you determine that a compromise has occurred. You are required to obtain technical assistance from the ISPM and Staff Judge Advocate during the course of this inquiry whenever necessary.

(Signature Block)

Attachment 9

PRELIMINARY INQUIRY OF SECURITY INCIDENT REPORT
DEPARTMENT OF THE AIR FORCE
AIR FORCE UNIT HEADING

MEMORANDUM FOR

FROM:

SUBJECT:Preliminary Inquiry of Security Incident No.

Authority: A preliminary inquiry was conducted (date) under the authority of the attached memorandum.

Matters investigated: The basis for this inquiry was that (provide a short summary of the security incident including the date it occurred, the classification of information involved, and the document control number if specific documents were involved). Refer to AFI 31-401, *Information Security Management Program*, paragraph **9.5.**, for security classification requirements.

Personnel Interviewed: (list all personnel interviewed, their position title, office symbol, and security clearance).

Facts: (list specific details answering who, what, why, where, and when questions concerning the security incident).

Conclusions: As a result of the investigation into the circumstances surrounding the security incident, interviews, and personal observations, it is concluded that: (list specific conclusions reached based on the facts and if a compromise or potential compromise did or did not occur). If a damage assessment is or has been done, provide the point of contact along with: the status of the assessment if it hasn't been completed; or, describe the outcome if it has been completed; or, provide a copy of the completed assessment report.

Recommendations: (list corrective actions needed to preclude a similar incident; the category of the incident; damage assessment; if the incident is a compromise, probable compromise or no compromise; and, if this inquiry should be closed without further investigation or with a recommendation for a formal investigation).

(Signature block)

Attachment:
Appointment of Inquiry Official Memo, (date)

Attachment 10

AIR FORCE
ORIGINAL CLASSIFICATION AUTHORITIES

Position Title	**Level**
Office of the Secretary of the Air Force	
Secretary of the Air Force (SAF/OS)	TS
Military Assistant (SAF/OS)	S
Under Secretary of the Air Force (SAF/US)	TS
Military Assistant (SAF/US)	S
Administrative Assistant (SAF/AA)	TS
Director, Security and Special Program Oversight (SAF/AAZ)	S
Deputy Under Secretary of the Air Force, International Affairs (SAF/IA)	S
Assistant Secretary for Manpower, Reserve Affairs, Installations and Environment (SAF/MI)	TS
Principal Deputy Assistant Secretary (SAF/MI)	S
Assistant Secretary for Financial Management and Comptroller (SAF/FM)	S
Principal Deputy Assistant Secretary, Financial Management and Comptroller (SAF/FM)	S
Deputy Assistant Secretary, Budget (SAF/FMB)	S
Assistant Secretary for Acquisition (SAF/AQ)	TS
Military Assistant (SAF/AQ)	S
Principal Deputy Assistant Secretary for Acquisition (SAF/AQ)	TS
Director, Special Projects (SAF/AQL)	TS
Directorate Global Reach (SAF/AQQ)	S
Directorate Space and Nuclear Deterrence (SAF/AQS)	TS
Assistant Secretary for Space (SAF/SN)	TS
Principal Deputy Assistant Secretary, Space (SAF/SD)	S
Director, Space Systems (SAF/SS)	S
Deputy Director for Security and Policy (SAF/SSS)	S

Position Title	Level
The General Counsel (SAF/GC)	TS
The Inspector General (SAF/IG)	TS
Director, Intelligence Systems Support Office (SAF/ISSO)	S
Director, Legislative Liaison (SAF/LL)	S
Director, Public Affairs (SAF/PA)	S
Air Force Program Executive Officer, Strategic (AFPEO/ST)	S
Air Force Program Executive Officer, Information Systems (AFPEO/IM)	S
Air Force Program Executive Officer, Tactical Airlift (AFPEO/TA)	S
Air Force Program Executive Officer, Command, Control and Communications (AFPEO/C3)	S
Air Force Program Executive Officer, Space (AFPEO/SP)	S
Air Force Program Executive Officer, Tactical Strike (AFPEO/TS)	S

Headquarters USAF

Chief of Staff (AF/CC)	TS
Vice Chief of Staff (AF/CV)	TS
Assistant Vice Chief of Staff (AF/CVA)	TS
Chief of Air Force Safety (AF/SE)	S
Director, Air Force Test and Evaluation (AF/TE)	TS
Air Force Historian (AF/HO)	S
Deputy Chief of Staff, Command, Control, Communications and Computers (AF/SC)	S
The Judge Advocate General (AF/JA)	S
Director of Civil Law and Litigation (AFLSA/JAC)	S
Chairman, USAF Scientific Advisory Board (AF/NB)	S
The Surgeon General (AF/SG)	S
Deputy Chief of Staff, Personnel (AF/DP)	TS
Director, Personnel Programs, Education and Training (AF/DPP)	S
Director, Military Personnel Policy (AF/DPX)	S
Chief, Personnel Readiness Group (AF/DPXC)	S
Deputy Chief of Staff, Plans and Operations (AF/XO)	TS
Director, Operations (AF/XOO)	S

Position Title	Level
Director, Operational Requirements (AF/XOR)	S
Director, Weather (AF/XOW)	S
Director, Nuclear and Counter Proliferation (AF/XON)	S
Director, Intelligence, Surveillance and Reconnaissance (AF/XOI)	TS
Director of Security Forces (AF/XOF)	TS
Deputy Chief of Staff, Plans and Programs (AF/XP)	TS
Deputy Chief of Staff, Installations and Logistics (AF/IL)	TS
Assistant Deputy Chief of Staff, Installations and Logistics (AF/IL)	TS
Director, Maintenance (AF/ILM)	S
Director, Transportation (AF/ILT)	S
Director, Plans and Integration (AF/ILX)	S
Director, Supply (AF/ILS)	S

Major Commands, Field Operating Agencies, and Direct Reporting Units

Air Combat Command

Commander, HQ ACC (ACC/CC)	TS
Comptroller (ACC/FM)	S
Director of Civil Engineering (ACC/CE)	S
Director of Intelligence (ACC/IN)	S
Director of Aerospace Operations (ACC/DO)	S
Director of Personnel (ACC/DP)	S
Command Historian (ACC/HO)	S
Inspector General (ACC/IG)	S
Director of Services (ACC/SV)	S
Director of Maintenance and Logistics (ACC/LG)	S
Staff Judge Advocate (ACC/JA)	S
Director of Public Affairs (ACC/PA)	S
Director of Safety (ACC/SE)	S
Surgeon General (ACC/SG)	S
Director of Plans and Programs (ACC/XP)	S
Director of Communications and Information Systems (ACC/SC)	S
Director of Security Forces (ACC/SF)	S

Position Title	Level
Advisor to the Commander for Guard Affairs (ACC/CG)	S
Commander, 8th Air Force (8 AF/CC)	TS
Commander, 26th Information Operations Group (26 IOG/CC)	S
Commander, 67th Information Operations Wing (67 IOW/CC)	S
Commander, 692nd Information Operations Group (692 IOG/CC)	S
Commander, 12th Air Force (12 AF/CC)	TS
Commander, 1st Fighter Wing (1 FW/CC)	S
Commander, 2nd Bomb Wing (2 BW/CC)	S
Commander, 4th Fighter Wing (4 FW/CC)	S
Commander, 5th Bomb Wing (5 BW/CC)	S
Commander, 6th Air Base Wing (6 ABW/CC)	S
Commander, 7th Bomb Wing (7 BW/CC)	S
Commander, 9th Reconnaissance Wing (9 RW/CC)	S
Commander, 20th Fighter Wing (20 FW/CC)	S
Commander, 27th Fighter Wing (27 FW/CC)	S
Commander, 28th Bomb Wing (28 BW/CC)	S
Commander, 33rd Fighter Wing (33 FW/CC)	S
Commander, 49th Fighter Wing (49 FW/CC)	S
Commander, 55th Wing (55 WG/CC)	S
Commander, 57th Wing (57 WG/CC)	S
Commander, 65th Air Base Wing (65 ABW/CC)	S
Commander, 99th Air Base Wing (99 ABW/CC)	S
Commander, 347th Fighter Wing (347 FW/CC)	S
Commander, 355th Wing (355 WG/CC)	S
Commander, 366th Wing (366 WG/CC)	S
Commander, 509th Bomb Wing (509 BW/CC)	S
Commander, 552nd Air Control Wing (552 ACW/CC)	S
Commander, Air Warfare Center (AWFC/CC)	S
Commander, AIA (AIA/CC)	TS
Vice Commander, AIA (AIA/CV)	TS

Position Title	Level
Executive Director (AIA/CA)	S
Director of Operations (AIA/DO)	S
Director of Plans and Programs (AIA/XP)	S
Commander, National Air Intelligence Center (NAIC/CC)	TS
Director of Technical Assistance (NAIC/TA)	S
Commander, Air Force Information Warfare Center (AFIWC/CC)	S
*Commander, Air Force Technical Applications Center (AFTAC/CC)	TS
*Vice Commander, Air Force Technical Applications Center (AFTAC/CV)	S
Air Education and Training Command (AETC)	
Commander, AETC (AETC/CC)	S
Director of Logistics (AETC/LG)	S
Director of Education (AETC/ED)	S
Air Force Audit Agency (AFAA)	
The Auditor General (AFAA/CC)	S
Air Force Command, Control, Communications and Computer Agency (AFCA)	
Commander, AFCA (AFCA/CC)	TS
Air Force Civil Engineer Support Agency (AFCESA)	
Commander, AFCESA (AFCESA/CC)	S
Air Force Historical Research Agency (AFHRA)	
Commander, AFHRA (AFHRA/CC)	S
Air Force History Support Office (AFHSO)	
Commander, AFHSO (AFHSO/CC)	S

Position Title	Level
Air Force Materiel Command (AFMC)	
Commander, AFMC (AFMC/CC)	TS
Director of Intelligence (AFMC/IN)	S
Commander, Ogden Air Logistics Center (OO-ALC/CC)	TS
Commander, Oklahoma City Air Logistics Center (OC-ALC/CC)	TS
Commander, Sacramento Air Logistics Center (SM-ALC/CC)	TS
Commander, San Antonio Air Logistics Center (SA-ALC/CC)	TS
Commander, Warner Robins Air Logistics Center (WR-ALC/CC)	TS
Commander, Aeronautical Systems Center (ASC/CC)	TS
Director, Weapons Airbase Range Product Support Office (OL-VX/VX)	S
Commander, Air Force Development Test Center (AFDTC/CC)	TS
Commander, Air Force Flight Test Center (AFFTC/CC)	S
Commander, Arnold Engineering Development Center (AEDC/CC)	TS
Commander, Electronic Systems Center (ESC/CC)	TS
Commander, Air Force Cryptological Support Center (AFCSC/CC)	S
Deputy Commander, Program Integration and Planning, Human Systems Center (HSC/XR)	S
Commander, Space and Missile Systems Center (SMC/CC)	TS
Commander, Air Force Research Laboratory (AFRL/CC)	TS
Director, Directed Energy (AFRL/DE)	TS
Director, Information (AFRL/IF)	TS
Director, Materials and Manufacturing (AFRL/ML)	TS
Director, Sensors (AFRL/SN)	TS
Director, Space Vehicles (AFRL/VS)	TS
Director, Munitions (AFRL/MN)	S
Director, Wright Research Site (Det 1, AFRL/WS)	S
Director of Material Management (WR-ALC/LU)	S
Director of Material Management (WR-ALC/LK)	S
Director of Material Management (WR-ALC/LY)	S
Director of Material Management (WR-ALC/LF)	S
Director of Material Management (WR-ALC/LN)	S

Position Title	Level
Air Force Military Personnel Center (AFMPC)	
Commander, AFMPC (AFMPC/CC)	S
Director, Personnel Accountability (AFMPC/DPW)	S
Air Force Office of Special Investigations (AFOSI)	
Commander, AFOSI (AFOSI/CC)	S
Air Force Operational Test and Evaluation Center (AFOTEC)	
Commander, AFOTEC (AFOTEC/CC)	TS
Air Force Reserve Command (AFRC)	
Commander, AFRC (AFRC/CC)	TS
Vice Commander, AFRC (AFRC/CV)	S
Assistant Vice Commander, AFRC (AFRC/CS)	S
Commander, 4th AF (4 AF/CC)	S
Commander, 10th AF (10 AF/CC)	S
Commander, 22nd AF (22 AF/CC)	S
Commander, Air Reserve Personnel Center (ARPC/CC)	S
Air Force Safety Agency (AFSA)	
Commander, AFSA (AFSA/CC)	S
Director of Nuclear Surety (AFSA/SN)	S
Air Force Space Command (AFSPC)	
Commander, AFSPC (AFSPC/CC)	TS
Director of Intelligence (AFSPC/IN)	S
Director of Operations (AFSPC/DO)	S

Position Title	Level
Director of Plans (AFSPC/XP)	S
Director of Requirement (AFSPC/DR)	S
Director of Logistics (AFSPC/LG)	S
Director of Communications-Computer Systems (AFSPC/SC)	S
Commander, 14th AF (14 AF/CC)	S
Commander, 20th AF (20 AF/CC)`	S
Commander, 21st Space Wing (21 SW/CC)	S
Commander, 30th Space Wing (30 SW/CC)	S
Commander, 45th Space Wing (45 SW/CC)	S
Commander, 50th Space Wing (50 SW/CC)	S
Commander, 90th Missile Wing (90 MW/CC)	S
Commander, 91st Missile Wing (91 MW/CC)	S
Commander, 321th Missile Wing (321 MW/CC)	S
Commander, 341st Missile Wing (341 MW/CC)	S
Air Force Special Operations Command (AFSOC)	
Commander, AFSOC (AFSOC/CC)	TS
Vice Commander, AFSOC (AFSOC/CV)	S
Director, Command Staff AFSOC (AFSOC/CS)	S
Air Mobility Command (AMC)	
Commander, AMC (AMC/CC)	TS
Vice Commander AMC (AMC/CV)	TS
Director of Special Staff (AMC/DS)	S
Director of Plans and Programs (AMC/XP)	S
Inspector General (AMC/IG)	C
Commander, Defense Courier Service (DCS/CC)	C
Pacific Air Forces (PACAF)	

Position Title	Level
Commander, PACAF (PACAF/CC)	TS
Director of Operations (PACAF/DO)	S
Director of Plans (PACAF/XP)	S
Commander, Fifth Air Force (5 AF/CC)	TS
Commander, Seventh Air Force (7 AF/CC)	TS
Commander, Eleventh Air Force (11 AF/CC)	TS
Commander, Thirteenth Air Force (13 AF/CC)	TS
United States Air Force Academy (USAFA)	
Superintendent, USAFA (USAFA/SUPT)	S
United States Air Forces in Europe (USAFE)	
Commander, USAFE (USAFE/CC)	TS
Vice Commander USAFE (USAFE/CV)	TS
Director of Operations (USAFE/DO)	S
Director, Plans and Programs (USAFE/XP)	S
Political Advisor (USAFE/CCB)	S
Commander, Third Air Force (3 AF/CC)	TS
Commander, Sixteenth Air Force (16 AF/CC)	TS
Joint Services Survival, Evasion, Resistance and Escape Agency (JSSA)	
Commander, JSSA	S

******AIA is responsible for administrative support to AFTAC*