***BY ORDER OF THE SECRETARY OF THE AIR FORCE***

***AIR FORCE INSTRUCTION 31-401***

***1 NOVEMBER 2005***

*Incorporating Change 1, 19 August 2009*

***Security***

***INFORMATION SECURITY PROGRAM MANAGEMENT***

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

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

**RELEASABILITY:** There are no releasability restrictions on this publication.

OPR: HQ USAF/XOS-FI

Certified by: HQ USAF/XO (Lt Gen Carrol H. Chandler)

Supersedes: AFI 31-401, 1 November 2001

Pages: 91

This publication implements Air Force Policy Directive (AFPD) 31-4, Information Security. It prescribes and explains how to manage and protect unclassified controlled information and classified information. Use this instruction with Executive Order (EO) 12958, as amended, *Classified National Security Information*, 25 March 2003; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, *Classified National Security Information*, Executive Order 12829, National Industrial Security Program (NISP), DOD Manual 5220.22, *National Industrial Security Program Operating Manual*, January 1995; and, Department of Defense (DOD) 5200.1-R, *Information Security Program*, 14 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; DOD Directive (DODD) 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*, 15 Nov 91; Air Force Policy Directive (AFPD) 31-4, *Information Security*. This instruction is applicable to contractors as prescribed in AFI 31-601, *Industrial Security Program*. All these references are listed at the end of each paragraph where applicable. This instruction is not to be used as a stand-alone document. HQ USAF/XOS-F is delegated approval authority for revisions to this AFI.

***SUMMARY OF CHANGES***

This interim change reflects new requirements for management of the Information Security Program at all echelons; transfers responsibility for Unclassified Controlled Nuclear Information; reflects the transfer of Information Security Program Manager (ISPM) duties and responsibilities

from the Chief, Security Forces or installation security official to the Chief of Information Protection at MAJCOM and installation levels and codifies staff office changes from that action; updates locations possible for overnight delivery of Secret information in urgent cases; updates references and deletes terms not used in the text; updates glossary of references and supporting information (**Attachment 1**); updates transmission procedures for unclassified controlled nuclear information (**Attachment 2**); deletes use of United States Postal System registered mail or Express Mail to transfer Secret or Confidential material (**Attachment 4**). An asterisk (|) indicates newly revised material.

**Chapter 1—POLICY AND PROGRAM MANAGEMENT** **5**

1.1. Policy ..... 5

1.2. Philosophy. ..... 5

1.3. Program Management. ..... 5

1.4. Oversight. ..... 7

1.5. Special Types of Information. ..... 9

1.6. Waivers. ..... 10

1.7. Reporting Requirements. ..... 11

1.8. Administrative Sanctions. ..... 11

1.9. Self-Inspection. ..... 12

**Chapter 2—ORIGINAL AND DERIVATIVE CLASSIFICATION** **12**

2.1. Original Classification Authority (OCA) ..... 12

2.2. Original Classification. ..... 13

2.3. Derivative Classification. ..... 13

2.4. Classification Prohibitions and Limitations. ..... 14

2.5. Classification Challenges ..... 14

2.6. Security Classification/Declassification Guides. ..... 14

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

3.1. Declassification and Downgrading Officials. ..... 17

3.2. Declassification. ..... 17

3.3. Exceptions. ..... 17

3.4. Automatic Declassification. ..... 17

3.5. Mandatory Review. ..... 18

3.6. Systematic Review for Declassification. ..... 18

3.7. Referrals. ..... 19

3.8. Public Release. ..... 19

3.9. Downgrading. ..... 19

**Chapter 4—MARKINGS** **19**

4.1. General. ..... 19

4.2. Required Markings. ..... 19

4.3. Special Control and Similar Notices. ..... 20

4.4. NATO. ..... 21

4.5. Other Foreign Government Information (FGI). ..... 21

4.6. Marking of Foreign Government and NATO Information in DOD Documents. .. 23

4.7. Audio and Video Tapes. ..... 24

4.8. Removable Information Systems Storage Media. ..... 24

4.9. Sensitive Compartmented Information (SCI). ..... 24

4.10. Authorized for Release To (REL TO) Markings. ..... 25

4.11. Classified Electronic Mail (E-Mail) ..... 26

**Chapter 5—SAFEGUARDING** **26**

Section 5A—Control Measures 26

5.1. General. ..... 26

Section 5B—Access 27

5.2. Granting Access to Classified Information. ..... 27

5.3. Nondisclosure Agreement (NdA). ..... 28

5.4. Access by Persons Outside the Executive Branch. ..... 29

5.5. Access by Visitors. ..... 33

5.6. Preventing Public Release of Classified Information. ..... 33

5.7. Access to Information Originating in a Non-DOD Department or Agency. ..... 33

5.8. Administrative Controls. ..... 34

Section 5C—Safeguarding 36

5.9. Care During Working Hours. ..... 36

5.10. End-of-Day Security Checks. ..... 37

5.11. Residential Storage Arrangements. ..... 37

5.12. In-Transit Storage. ..... 37

5.13. Classified Meetings and Conferences ..... 38

5.14. Protecting Classified Material on Aircraft. ..... 38

5.15. Information Processing Equipment. ..... 41

5.16. General Safeguarding Policy. ..... 41
5.17. Standards for Storage Equipment. ..... 42
5.18. Storage of Classified Information. ..... 42
5.19. Use of Key-Operated Locks ..... 43
5.20. Procurement of New Storage Equipment ..... 43
5.21. Equipment Designations and Combinations. ..... 43
5.22. Repair of Damaged Security Containers ..... 44
5.23. Maintenance and Operating Inspections. ..... 44
5.24. Reproduction of Classified Material. ..... 44
5.25. Control Procedures. ..... 44
5.26. Emergency Authority. ..... 45

Section 5D—Disposition and Destruction of Classified Material 45
5.27. Retention of Classified Records. ..... 45
5.28. Disposition and Destruction of Classified Material ..... 46

**Chapter 6—TRANSMISSION AND TRANSPORTATION 47**

Section 6A—Methods of Transmission or Transportation 47
6.1. General Policy. ..... 47
6.2. Transmission and Transporting Top Secret Information. ..... 48
6.3. Transmitting and Transporting Secret Information. ..... 48
6.4. Transmitting Confidential Information. ..... 49
6.5. Transmission of Classified Material to Foreign Governments. ..... 50

Section 6B—Preparation of Material for Transmission 50
6.6. Envelopes or Containers. ..... 50

Section 6C—Escort or Handcarrying of Classified Material 50
6.7. General Provisions ..... 50
6.8. Documentation. ..... 51

**Chapter 7—SPECIAL ACCESS PROGRAMS (SAPS) 51**

7.1. Control and Administration ..... 51
7.2. Code Words and Nicknames. ..... 51

**Chapter 8—SECURITY EDUCATION AND TRAINING 52**

Section 8A—Policy 52
8.1. General Policy. ..... 52

8.2. Methodology. ..... 52
8.3. Roles and Responsibilities. ..... 52
Section 8B—Initial Security Orientation 54
8.4. Cleared Personnel. ..... 54
8.5. Uncleared Personnel. ..... 55
Section 8C—Special Requirements 56
8.6. Original Classification Authorities (OCAs). ..... 56
8.7. Derivative Classifiers, Security Personnel, and Others. ..... 56
8.8. Restricted Data (RD)/Formerly Restricted Data (FRD). ..... 56
Section 8D—Continuing Security Education/Refresher Training 56
8.9. Continuing and Refresher Training. ..... 56
Section 8E—Access Briefings and Termination Debriefings 57
8.10. Access Briefings. ..... 57
8.11. Termination Debriefings. ..... 58
8.12. Refusal to Sign a Termination Statement. ..... 58
Section 8F—Program Oversight 59
8.13. General. ..... 59
Section 8G—Coordinating Requests for Formal Training 59
8.14. Coordinating Requests for Training. ..... 59
**Chapter 9—ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION 59**
9.1. Policy. ..... 59
9.2. Definitions. ..... 59
9.3. Information System (IS) Deviations. ..... 60
9.4. Sensitive Compartmented Information (SCI) Incidents. ..... 60
9.5. Special Access Program (SAP) Incidents ..... 60
9.6. Classification. ..... 60
9.7. Public Release. ..... 61
9.8. Reporting and Notifications. ..... 61
9.9. Preliminary Inquiry. ..... 62
9.10. Damage Assessment. ..... 63
9.11. Formal Investigation. ..... 64

9.12. Management and Oversight. ..... 65

9.13. Unauthorized Absences. ..... 65

9.14. Prescribed Forms. These forms are prescribed throughout this AFI and are available through the Air Force Publications Distribution system: ..... 65

**Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 66**

**Attachment 2—CONTROLLED UNCLASSIFIED INFORMATION 75**

**Attachment 3—PHYSICAL SECURITY STANDARDS 80**

**Attachment 4—TRANSMISSION TO FOREIGN GOVERNMENTS 81**

**Attachment 5—APPOINTMENT OF INQUIRY OFFICIAL MEMORANDUM 81**

**Attachment 6—PRELIMINARY INQUIRY OF SECURITY INCIDENT REPORT 82**

**Attachment 7—FORMAT FOR CLASSIFICATION/DECLASSIFICATION GUIDE 83**

# 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 and unclassified information and material consistent with national policy. This general policy statement also applies to unclassified controlled information (**Attachment 2**) under the purview of relevant statutes, regulations and directives *[Reference DOD 5200.1-R, C1.1.]*.

**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.

**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, C1.2.]*.

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 Director, Information Protection (SAF/AAP) is responsible for policy, resource advocacy, and oversight of this program.

1.3.3. Commanders of Major Commands (MAJCOM), Field Operating Agencies (FOAs), Direct Reporting Units (DRUs), 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. The installation Chief of the Information Protection (IP) Office (IPO) or MAJCOM Director, Information Protection is designated the ISPM at each Air Force installation or site. Air Force Chiefs of Information Protection:

1.3.4.1. Implement the Information Security Program, for the Information, Personnel, and Industrial Security Programs on behalf of the installation commander. Assist in the program/technology protection planning process as it relates to information, personnel and industrial security, to include direction on physical security requirements

for the protection of assets during the various states, i.e., production, deployment, maintenance, test, or undergoing modifications.

1.3.4.2. Integrate on-base contractor operations into the installation's Information Security Program in accordance with (IAW) AFI 31-601.

1.3.4.2.1. Review pre-award and/or draft solicitations and contract documents associated with classified contract efforts; security classification guides and Department of Defense (DD) Form 254 to ensure appropriate security clauses and/or language is contained therein which address the protection of sensitive government information and resources.

1.3.4.2.2. Serve as technical OPR for the development and preparation of the Visitor Group Security Agreement (VGSA) or other security agreements as determined necessary by the installation commander.

1.3.4.2.3. Conduct security oversight of on-base designated "cleared facilities" as determined by the installation commander.

1.3.4.3. Provide oversight within their jurisdiction.

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

1.3.4.5. For organizations at the Wing level and below, conduct security manager meetings no less than semi-annually.

1.3.5. Unit Commanders or Equivalents, and Staff Agency Chiefs. NOTE: For the purpose of this instruction, staff agency chiefs are those individuals serving in 2-digit positions reporting to the commander or vice commander above the Wing level and 2 and 3 digit positions at Headquarters Air Force. These commanders or equivalents, and staff agency chiefs will:

1.3.5.1. Appoint a security manager to administer the unit's information security program. Alternate security managers may be appointed as necessary. Commanders or equivalents, and staff agency chiefs should consider Air Expeditionary Force rotation cycles, TDY, training requirements, and other assigned duties. Continuity should receive serious consideration in selection of security managers. Military security managers must have a favorable National Agency Check, local agency check, and credit check (NACLC); civilians a National Agency Check with written inquiries and credit check (ANACI), investigation or higher and eligibility for JPAS access before appointment. ***NOTE:*** Smaller organizations and staff agencies are encouraged to appoint primary and alternate security managers to serve multiple activities.

1.3.5.1.1. Contractors will not be appointed as primary or alternate security managers. However, they can be required to provide other security program support, under Air Force direction, such as, assisting the security manager, conducting end-of-day security checks, security training/briefings, etc.

1.3.5.2. Ensure security managers receive training required by **Chapter 8**.

1.3.5.3. Notify the ISPM in writing when either primary or alternate security managers are changed.

1.3.6. Security Managers:

1.3.6.1. Establish and manage the Information Security Program within their unit or staff agency.

1.3.6.2. Develop and update a unit security operating instruction.

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

1.3.6.4. Attend ISPM hosted security manager meetings.

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

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

1.3.6.7. Report security incidents immediately, but no later than by the end of the first duty day.

1.3.6.8. Assist the unit commander or equivalent, staff agency chief and ISPM in monitoring security incident investigations. Normally security managers will not conduct security incident inquiries.

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

1.3.6.10. Manage the JPAS within their organization.

1.3.6.10.1. In-process and out-process all unit personnel.

1.3.6.10.2. Monitor and act on system notifications.

1.3.7. Supervisors:

1.3.7.1. Establish criteria, evaluate, and rate all Air Force employees on their performance of security responsibilities *[Reference DOD 5200.1-R, C1.1.2.1.]*.

1.3.7.1.1. Military. See AFI 36-2406, *Officer and Enlisted Evaluation Systems*, paragraph 1.3.7.

1.3.7.1.2. Civilian. See AFI 36-1001, *Managing the Civilian Performance Program*, paragraph A3.2.8.

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

1.3.8. 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 all Air Force information to foreign governments, persons, and international organizations.

1.3.9. Historian. The Air Force Historian (HQ USAF/HO), 3 Brookley Avenue, Box 94, Bolling AFB DC 20032-5000, approves or disapproves historical researchers' access to classified information. *[Reference DOD 5200.1-R, C6.2.2.4.]*

**1.4. Oversight.** In addition to the reporting requirements of the Information Security Program (see **paragraph 1.7**), the following will be implemented *[Reference DOD 5200.1-R, C1.7.]*.

1.4.1. MAJCOMs will incorporate information protection issues into Inspector General (IG) inspections/reviews. In addition, MAJCOM Information Protection Offices (IPO) will

conduct oversight and assistance visits in the form of either an Information Security Program Review (ISPR) or Staff Assistance Visit (SAV) to subordinate IPOs at least every 36 months. MAJCOM IPO staffs are encouraged to explore oversight options to minimize resource impact.

1.4.1.1. ISPR.

1.4.1.1.1. An ISPR is an assistance-oriented oversight visit for the information security programs performed by an ISPM, or designated representative(s) on a subordinate ISPM or security manager. It is a non-rated review for policy and program effectiveness to benchmark processes/products, identify problem areas and corrective actions. A key component of the ISPR is an assessment of the effectiveness of the information security training program.

1.4.1.1.2. Air Force on-base contractor visitor groups will be integrated into the host installation's Information Security Program unless the mission, operational requirements, autonomous nature or other factors require them to establish and maintain their own security program as a cleared facility under the National Industrial Security Program Operating Manual (NIS- POM).

1.4.1.1.3. The ISPM will provide the commander or equivalent, and staff agency chief the ISPR results in writing.

1.4.2. Base level ISPMs will conduct ISPRs on an annual basis. ***EXCEPTION:*** An extension to 18 months may be granted by the ISPM for units that have demonstrated highly effective, discrepancy free programs during the previous ISPR. ISPRs/SAVs may be conducted every two years for activities or units that do not store classified information.

1.4.3. Security Self-Inspections: Unit commanders or equivalents, and staff agency chiefs 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. Unit commanders or equivalents, and staff agency chiefs will appoint an individual, in writing, other than the unit security manager to conduct a semiannual security inspection.

1.4.3.2. A program review may satisfy the requirement for one of the semiannual self-inspections.

1.4.4. SAF/AAP, Chief of Information Protection will visit MAJCOMs to review their information protection and associated security programs every 36 months.

**1.5. Special Types of Information.** *[Reference DOD 5200.1-R, C1.3.]*

1.5.1. Restricted Data (RD)/Formerly Restricted Data (FRD). *[Reference DODD 5210.2 and DOD 5200.1-R, C1.3.1.]*

1.5.1.1. General. RD is governed by DODD 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78. Air Force personnel will mark and safeguard RD according to DODD 5210.2. A list of Air Force Officials Authorized to Certify Access to RD is

located on the AFSFC web site. These officials are responsible for certifying access to RD using DoE Form 5631.20, *Request for Visit or Access Approval* (see **paragraph 5.5.1.2**). They may delegate this authority to the level they deem necessary for operational efficiency. Officials delegated the authority will sign in the "For" block on behalf of the access granting official. Air Force personnel may obtain DoE Form5631.20 from the DoE activity they are visiting or at the DoE Forms web site.

1.5.1.1.1. Activities must notify SAF/AAP through command IP channels of changes to the list of certifying officials as they occur. When doing so, they must also provide the position title, activity and office symbol of the affected authority. ***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. SAF/AAP will periodically update a master list available at the Information Protection Directorate Community of Practice (CoP).

1.5.1.2. Critical Nuclear Weapon Design Information (CNWDI). RD that is particularly sensitive. 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.

1.5.1.2.2. Granting Access. Approving officials will ensure access and briefings are documented on AF Form 2583, *Request for Personnel Security Action*.

1.5.1.2.3. 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 DODD5210.2, Paragraph 6]*

1.5.2. North Atlantic Treaty Organization (NATO). *[Reference DOD 5200.1-R, C1.3.4.]*

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

1.5.2.2. The HQ USAFE IP Office is responsible for developing and recommending NATO security policy for implementation within the Air Force.

1.5.3. For Official Use Only (FOUO). Unclassified information that is exempt from release under the Freedom of Information Act (FOIA) exemptions 2-9, may be designated "For Official Use Only." No other material shall be considered FOUO. FOUO is not authorized as an anemic form of classification to protect national security interests. *[Reference DOD Regulation 5400.7/AF Supplement, DOD Freedom of Information Act Program, C4.1.1]* The FOIA exemptions are detailed in *DOD Regulation 5400.7/AF Supplement*, Chapter 3.

1.5.4. Sensitive Compartmented Information (SCI). The Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2), 1480 Air Force Pentagon, Washington DC 20330-1480, is responsible for SCI policy. The provisions of this publication may not supersede the policies and guidance prescribed in the appropriate Director of Central Intelligence Directives governing the control, safeguarding, and dissemination of SCI as promulgated by the Cognizant Security Authority (CSA) for intelligence security

management. The CSA will, on behalf of the Senior Official of the Intelligence Community (SOIC), AF/A2, ensure appropriate resolution of actual or perceived conflicts regarding SCI and the provisions of this publication.

1.5.5. Special Access Program (SAP) Information. The Director of Security, Counterintelligence and Special Program Oversight (SAF/AAZ), 1480 Air Force Pentagon, Washington DC 20330-1480, is responsible for SAP policy and oversight of all Air Force SAPs. Should the policies and guidance in this instruction and those issued by DoD and/or the Air Force SAP Central Office (AFSAPCO) conflict, DoD and AFSAPCO policies and guidance will take precedence.

**1.6. Waivers.**

1.6.1. Commanders or equivalents, and staff agency chiefs send requests to waive provisions of DOD 5200.1-R, AFPD 31-4, or this AFI through command IP channels to SAF/AAP. FOAs also coordinate their requests with their respective functional head at Headquarters Air Force (HAF) before submitting to SAF/AAP [Reference DOD 5200.1- R, C1.4.2.].

1.6.2. Requests for waivers shall contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security should the waiver be approved.

1.6.3. Waivers or exceptions to Special Access Program (SAP) requirements are forwarded through appropriate program channels to SAF/AAZ, 1480 Air Force Pentagon, Washington DC 20330-1480.

**1.7. Reporting Requirements.** *[Reference DOD 5200.1-R, C1.6.1.]*

1.7.1. MAJCOM and DRU IPs will submit the SF Form 311, Agency Security Classification Program Data, report to SAF/AAP by 1 October of each year.

1.7.1.1. Organizations sample data for Part C, Original Classification Decisions, and Part D, Derivative Classification Decisions during a consecutive 2-week period each fiscal year quarter (Oct-Dec, Jan-Mar, Apr-Jun, and Jul-Sep). In the last quarter the 2-week period must be set early since the reports are required by 15 October. Interagency Report Control Number 0230-GSA-AN applies to this information collection requirement.

1.7.1.1.1. Count the number of classification decisions in finished products for dissemination or retention, regardless of the media.

1.7.1.1.2. Do not count reproductions or copies.

**1.8. Administrative Sanctions.**

1.8.1. Send reports through command IP channels to SAF/AAP when someone knowingly, willfully, or negligently discloses classified information to unauthorized individuals as specified in EO 12958, as amended *[Reference DOD 5200.1-R, C1.5.]*.

1.8.2. Air Force commanders or equivalents 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, C1.5.]*.

1.8.3. Commanders or equivalents, and staff agency chiefs take and process administrative sanctions/ actions for civilian appropriated fund employees IAW AFI 36-704, *Discipline and Adverse Actions*, AFMAN 34-310, *Nonappropriated Fund Personnel Program Management and Administration Procedures*, for nonappropriated fund employees, and IAW AFI 36-2907, *Unfavorable Information File (UIF) Program*, for military personnel. Contact the servicing civilian or military personnel flight office if assistance is needed. Commanders should consult their servicing legal office before taking action for serious violations.

**1.9. Self-Inspection.** See **paragraph 1.4** of this AFI *[Reference DOD 5200.1-R, C1.7.]*.

# Chapter 2

## ORIGINAL AND DERIVATIVE CLASSIFICATION

### 2.1. Original Classification Authority (OCA) *[Reference DOD 5200.1-R, C2.2.]*

2.1.1. The Secretary of the Air Force serves as the 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. SAF/AA delegates Secret and Confidential authority.

2.1.2.3. All requests for the delegation of OCA will be forwarded through command IP channels to SAF/AAP, Director of Information Protection, 1720 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 SAF/AA.

2.1.2.3.3. Only individuals in senior military or civilian positions (usually General Officer or Senior Executive Service level) at the first or second echelon of command carrying out a unique mission with responsibility for one of the eight subject areas prescribed by EO 12958, as amended, may be designated as an OCA.

2.1.2.3.4. OCA is assigned to a position, not a person. OCA will not be delegated other than identified in **paragraphs 2.1.2.1** and **2.1.2.2** above. However, deputies, vice commanders, chiefs of staff and similar other subordinates of an OCA are empowered to act as an OCA when they assume the duty position of an OCA in an "acting" capacity and have certified in writing that they have been trained in OCA responsibilities and classification principles in addition to the basic security training on the proper safeguarding of classified information and the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure before exercising this authority.

2.1.2.4. All requests will contain the full position title, functional office symbol, a detailed explanation of why the position requires OCA and an estimate of the annual use of the delegated authority.

2.1.3. SAF/AAP will maintain the master list of Air Force OCAs and post on the Information Protection Directorate Community of Practice (CoP). Periodically, SAF/AAP will request OCA validation from the MAJCOM/FOA/DRU IPMs.

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

2.1.3.2. See the Information Protection Directorate Community of Practice (CoP) web site for OCA training requirements.

**2.2. Original Classification.** *[Reference DOD 5200.1-R, Chapter 2 and Interim Information Security Guidance, April 16, 2004.]*

2.2.1. Original classification is the initial decision that an item of information could be expected to cause damage to the national security if subjected to unauthorized disclosure, and that the interests of the national security are best served by applying the safeguards of the Information Security Program to protect it. This decision may be made only by persons who have been specifically delegated the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information *[Reference: DOD 5200.1-R, C2.1.]*.

2.2.1.1. Before an original classification decision is made, it must be determined that classification guidance is not already available in the form of classification guides, plans or other memoranda.

2.2.1.2. OCAs are accountable to the Secretary of Defense for their classification decisions.

2.2.1.3. In those rare situations where the OCAs' decision must be rendered verbally due to the priorities of an on-going operation, written confirmation will be issued within seven days.

2.2.1.4. OCAs must notify users when there are changes to an original decision.

2.2.1.5. OCAs shall be prepared to present, as required, deposition and expert testimony in courts of law concerning classification of national security information and be prepared to defend and justify their original decisions.

2.2.2. Classification may be applied only to information that is owned by, produced by or for, or is under the control of the United States Government. Information may be considered for classification only if it concerns one of the categories specified in Section 1.4 of EO 12958, as amended.

**2.3. Derivative Classification.** The act of incorporating, paraphrasing, restating, or generating in a new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or a classification guide issued by an OCA. Within DOD, all cleared personnel can perform derivative classification.

2.3.1. Originating Agency's Determination Required (OADR). OADR is no longer an approved marking and should not be contained in any originally classified documents that have been created after October 14, 1995.

2.3.2. X1 through X8 are no longer approved markings and should not be contained in any originally classified documents that have been created on or after September 22, 2003.

2.3.3. When creating a derivatively classified document and using a source document that contains OADR or X1 through X8, the derivative classifier will place the following information in the Declassify On line:

**DECLASSIFY ON: Source marked OADR (or X1 thru X8, whatever is applicable)**

**Date of source: 5 October 1993 (date of source document)**

2.3.4. These documents will be subject to review for declassification 25 years after the date of the source document.

**2.4. Classification Prohibitions and Limitations.**

2.4.1. Under no circumstances shall information be classified in order to (1) conceal violation of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of the national security *[Reference EO 12958, as amended, Section 1.7, DOD 5200.1-R, and Interim Information Security Guidance 16 April 2004]*.

2.4.2. The OCA having jurisdiction over the subject matter determines if information requested under the FOIA or the mandatory declassification review (MDR) provisions of EO 12958, as amended, should be declassified *[Reference DOD 5200.1-R, C2.4.3.5.]*

**2.5. Classification Challenges.** *[Reference DOD 5200.1-R, C4.9.]*

2.5.1. If holders of information have reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their commander or equivalent, staff agency chief, security manager, or supervisor.

2.5.2. Send formal challenges to classification, in writing, to the OCA with jurisdiction over the information in question.

2.5.3. Challenges to reclassification decisions are sent through command IP channels to SAF/AAP.

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

**2.6. Security Classification/Declassification Guides.**

2.6.1. Required Elements. A security classification/declassification guide (see **Attachment 7** for sample format) is the written record of an original classification decision and appropriate declassification instructions and should be issued as early as practical in the life cycle of the classified system, plan, program or project. It shall, at a minimum:

2.6.1.1. Identify the subject matter of the classification guide.

2.6.1.2. Identify the OCA by name or personal identifier, and position.

2.6.1.3. Identify an agency Point of Contact (POC) (name, office symbol, mailing address, organizational e-mail address, DSN/commercial phone numbers) for questions regarding the classification guide.

2.6.1.4. Provide the date of issuance or last review.

2.6.1.5. State precisely the categories or elements of information to be declassified, to be downgraded, or not to be declassified.

2.6.1.6. State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified (***NOTE:*** Only one level of classification will be annotated for each element of information.)

2.6.1.7. State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in Section 1.4 of EO 12958, as amended.

2.6.1.8. State, when applicable, special handling caveats.

2.6.1.9. Prescribe declassification instructions for each element of classified information.

2.6.1.10. Identify any related files series that have been exempted from automatic declassification pursuant to Section 3.3(c) of EO 12958, as amended.

2.6.1.11. To the extent a guide is used in conjunction with the automatic declassification provisions in Section 3.3 of EO 12958, as amended, state precisely the elements of information to be exempted from declassification to include:

2.6.1.11.1. The appropriate exemption category listed in section 3.3(b), and, when citing the exemption category listed in section 3.3(b)(9), specify the applicable statute, treaty or international agreement; and

2.6.1.11.2. A date or event for declassification IAW **section 1.5**.

2.6.2. OCA Responsibilities.

2.6.2.1. It is the responsibility of the OCA to publish classification/declassification guides to facilitate the proper and uniform derivative classification and declassification of their information. ***NOTE:*** In some cases, OCAs may determine that publishing classification guidance in other forms is more effective, e.g., program protection plans, system protection guides, AFIs. In these cases, the applicable publication will be considered the guide and the publishing requirements in **paragraph 3.3** still apply.

2.6.2.2. Each OCA will revise (IAW **paragraph 2.6.2.4** below) their security classification guides to include an advisory statement in the Release of Information section:

2.6.2.2.1. 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, *Public Affairs Policy and Procedures*. If there are any doubts, do not release the information.

2.6.2.3. All guides will be reviewed by the servicing Foreign Disclosure Office before final approval.

2.6.2.4. Classification/declassification security guides shall be reviewed and updated, as circumstances require, but at least once every five years. ***NOTE:*** Due to the major changes implemented by EO 12958, as amended, all current Air Force classification/declassification guides will be reviewed no later than 31 December 2005, and every five years thereafter.

2.6.3. Publishing Requirements.

2.6.3.1. All guides which extend classification beyond 25 years must be approved by the Interagency Security Classification Appeals Panel (ISCAP). Once the OCA has signed the guide, the document will be sent to SAF/AAP who will forward it to the ISCAP for approval.

2.6.3.2. The OCA will report publication of or changes to security classification/ declassification guides to the Administrator, Defense Technical Information Center (DTIC) using DD Form 2024. DTIC will require an electronic copy of the guide.

2.6.3.3. OCAs must also forward a hard copy of the applicable publication or change to:

2.6.3.3.1. HQ AFHRA/RSA, 600 Chennault Circle, Maxwell AFB AL 36112-6424.

2.6.3.3.2. SAF/PA, 1690 Air Force Pentagon, Washington, DC 20330-1690.

2.6.3.4. All guides (to include any changes) will also be forwarded electronically to SAF/AAP at **SAF.AAP.workflow@pentagon.af.mil** and AFDO at **AFDO.Workflow@pentagon.af.mil** in PDF and Microsoft Word format.

2.6.4. Electronic Location of Guides. SAF/AAP will maintain the master list of all Air Force classification/declassification guides and will provide guides made available on the MOSIAC SIPRNET Community of Practice (CoP). Guides are also located on the DTIC web site. To access the DTIC web site you must have a DTIC account. The URL for this is **http://www.dtic.mil/dtic/registration**.

2.6.5. 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 for information relating to nuclear weapons. 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 these guides to SAF/AAP (1720 Air Force Pentagon, Washington DC 20330-1340) through command IP channels. Requests must include the name, address, and phone number of the activity POC, and the POC's level of access. IPs will validate this information before submitting the requests to SAF/AAP. 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, only OCAs have the authority to declassify or downgrade classified information.

**3.2. Declassification.** Note: Exemptions identified in this chapter are found in *ISSO Directive Number 1, Section 2001.21(3)(i)*.

3.2.1. Originally Classified Documents. The declassification decision determines the duration of protection *[Reference EO 12958, as amended, Section 1.6.(a)(4) and ISOO Directive Number 1, Section2001.12.]*. *At the time an item of information is classified, original classifiers will determine which of the following four declassification instructions will be used, selecting whenever possible, the declassification instruction that will result in the shortest duration of classification.*

3.2.1.1. A date or event less than 10 years from the date of the document; or, if unable to identify such a date or event;

3.2.1.2. A date 10 years from the date of the document;

3.2.1.3. A date greater than 10 and less than 25 years from the date of the document; or

3.2.1.4. A date 25 years from the date of the document.

3.2.2. Derivatively Classified Documents. The "Declassify on" line must include one of the following:

3.2.2.1. The date or event up to 25 years, as noted on the source document; or

3.2.2.2. Source marked OADR, date of source (cannot be a date after October 1995);

3.2.2.3. Source marked X1-X8, date of source (cannot be a date after September 2003);

3.2.2.4. 25X1 through 25X9, and a specific date or event for declassification; or

3.2.2.5. 25X1-human (the only category that does not require a date or event follow it).

**3.3. Exceptions.** RD/FRD *[Reference 10 CFR 1045.1 Subpart A]*. Documents containing RD or FRD are excluded from automatic declassification and do not require a declassification date. RD must be reviewed by the DoE prior to release. DoE and DOD must jointly review documents containing FRD prior to release.

**3.4. Automatic Declassification.** IAW EO 12958, as amended, Section 3.3, all Air Force activities that possess classified information that is of permanent historical value and is 25 years old or older should have completed a declassification review of these documents by 31 Dec 2006.

3.4.1. The Air Force Declassification Office (AFDO) has published the Air Force Declassification Plan that provides the framework for Air Force compliance with Section 3.3 of EO 12958, as amended. It pertains to all classified Air Force records that are 25 years old or older as of 31 December 2006, and have been determined under Federal law to have permanent historical value. The Air Force Declassification Plan is posted at the

AFDO web site (**http://www.afdo.hq.af.mil/Plan.htm**). It is critical that records management and information security personnel work together to ensure that requirements of both are met on classified records that are going to be sent to the National Archives or Federal Records Center.

3.4.2. All classified records shall be automatically declassified on 31 December of the year that is 25 years from the date of its original classification, unless it falls in one of the exemption categories (25X) listed in Section 3.3(b) of EO 12958, as amended.

3.4.3. The 25X categories *cannot* be used unless the specific information has been approved through the ISCAP process. This is usually done in the form of a security classification/declassification guide. (See **paragraph 2.6** and **Attachment 7**.) The Air Force has an approved list of exemption categories (listed in the Air Force Declassification Plan); however, the specific item must still be annotated in the security classification/ declassification guide before it is used on derivatively marked documents. For original classification decisions, no 25X marking, other than "25X1-human," is permitted on the "declassify on" line. All originally classified documents *will* contain either a date or event less than 10 years or a date from 10 to 25 years. The only exception is the marking "25X1-human." This marking may be used when the disclosure of the information could be expected to reveal the identity of a confidential human source or human intelligence source. This is the *only* 25X marking that does not require a date or event for declassification to be cited with the 25X marking.

**3.5. Mandatory Review.**

3.5.1. Mandatory review requests must identify the information requested with enough specificity to allow for location of the records with a reasonable amount of effort.

3.5.2. Send all requests for MDR to 11 CS/SCSL (MDR), 1000 Air Force Pentagon, Washington DC 20330-1000.

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

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

3.6.1. 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 that is 25 years from the date of its original classification.

3.6.2. Other records. Activities will set up a reasonable schedule for conducting declassification reviews for all other classified records.

**3.7. Referrals.** A referral is information that is subject to the provisions of EO 12958, as amended, Section 3.3, Automatic Declassification, and ISOO Directive No. 1, Section 2001.34, and has been referred to, within, or outside the Air Force for review. AFDO is the focal point for processing Air Force referrals. Detailed information regarding the referral process can be found in the Air Force Declassification Plan.

**3.8. Public Release.** When information is declassified, it is not releasable to the public until it has been approved for release through the security review process IAW AFI 35-101, Chapter

15. The same holds true for declassified or unclassified information that will be placed on an Internet site that can be accessed by the public.

**3.9. Downgrading.** Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection at the originally assigned level, and can be properly protected at a lower level. Any official who is authorized to classify or declassify the information and has authority over the information may downgrade information.

## Chapter 4

## MARKINGS

**4.1. General.** Air Force personnel who originally and derivatively classify information will mark those products according to DOD 5200.1-R and the ISOO Marking Booklet. Material other than ordinary paper documents, e.g., e-mail transmitted over a secure network, must have the same information either marked on it or made immediately available to holders by other means. *[Reference DOD 5200.1-R, C5.1.]*

**4.2. Required Markings.** Classified documents are required to have the following markings:

4.2.1. The overall classification of the document.

4.2.2. The agency, office of origin, and date of the document.

4.2.3. The office or source document that classified the information.

4.2.3.1. If it is originally classified, the document will reference the office. ***Example:*** **CLASSIFIED BY**: **SAF/AAP.**

4.2.3.2. If a document is derivatively classified, it will reference the source document or the security classification/declassification guide. ***Example:*** **DERIVED FROM**: **HQ USAF/A3/5 Memo dated 12 Jan 2008. Subj**: **Funding Problems.**

4.2.4. The reason for classification. Each originally classified document shall bear a concise statement of the reason for classification, determined by the original classifier. *[Reference DOD 5200.1-R, C5.2.4.]* The classification categories are listed in EO 12958, as amended, Section 1.4; DOD5200.1-R Interim Information Security Guidance, Chapter 2, Para 1. ***Example:*** **REASON: 1.4(e).**

4.2.4.1. If a document is derivatively classified, the "REASON" is not required to be carried over to the derivative document.

4.2.5. Declassification instructions, and any downgrading instructions that apply. ***Example:*** **DECLASSIFY ON: 15 MARCH 2010.**

4.2.5.1. If marking material that falls within one of the 25-year exemption categories, the correct marking will be as follows (NOTE: only derivatively classified documents will carry a 25X marking, with the exception of 25X1-human, which is allowed on originally classified documents):

**DECLASSIFY ON: 25X5, 15 February 2010**

4.2.6. Page and portion markings to identify the specific classified information in the document and its level of classification. When marking a document that is derivatively classified, ensure all markings and caveats are carried over from the source document to the derivative document.

4.2.7. Control notices and other markings that apply to the document.

4.2.8. When a document has been declassified or downgraded, the following markings shall be applied:

4.2.8.1. The word "Declassified" or the new classification if being downgraded.

4.2.8.2. The authority for the action (the OCA's office symbol and the identification of the correspondence or classification instruction that required it).

4.2.8.3. The date of declassification or downgrading action.

4.2.8.4. The overall classification markings that appear on the cover page or first page shall be marked through with a straight line. If downgraded, the new classification will be written in.

4.2.8.5. Page and portion markings will be remarked as required.

4.2.9. Notebooks, binders, folders, etc. containing classified documents will be conspicuously marked with the highest classification of the material contained. Affix the appropriate overall classification marking or classified cover sheet to the front and back of the notebook, binder, folder, etc.

**4.3. Special Control and Similar Notices.** *[Reference DOD 5200.1-R, C5.2.9.]*

4.3.1. Working Papers. Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information will be:

4.3.1.1. Dated when created.

4.3.1.2. Marked with the highest classification of any information contained in the document and annotated "WORKING PAPER".

4.3.1.3. Destroyed when no longer needed.

4.3.1.4. Protected IAW the assigned classification.

4.3.1.5. Marked in the same manner as a finished document at the same classification level when transmitted outside the facility or if retained for more than 180 days from the original creation date.

4.3.2. Communications Security (COMSEC). See AFI 33-211, *Communications Security (COMSEC) User Requirements,* for guidance on marking COMSEC documents and media.

4.3.3. Technical Documents. See AFI 61-204, *Disseminating Scientific and Technical Information,* for guidance on marking and disseminating technical documents. *[Reference DOD 5200.1-R, paragraph C5.2.9.8. and DODD 5230.24, Distribution Statements on Technical Documents.]*

4.3.4. SAPs. Documentation and information may be identified with the Phrase "Special Access Required" and the assigned nickname, codeword, trigraph, or digraph. See AFI 16-701, *Special Access Programs,* for additional guidance on SAP documents.

4.3.5. Restricted Data/Formerly Restricted Data (RD/FRD). *[Reference 10 CFR 1045.1, Subpart A.)*

4.3.5.1. Documents containing RD shall be marked:

**RESTRICTED DATA**

**"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions."**

4.3.5.2. Documents containing FRD shall be marked:

**FORMERLY RESTRICTED DATA**

**"Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954"**

4.3.6. For Official Use Only (FOUO). See chapter 4 of DOD 5400.7/AF Supplement.

**4.4. NATO.** NATO documents should be marked in compliance with AFI 31-406, *Applying North Atlantic Treaty Organization (NATO) Protection Standards*, USSAN Instruction 1-69, *United States Implementation of NATO Security Procedures*, and C-M(2002)49, *Security Within the North Atlantic Treaty Organization (NATO)*. Any new policies, principles, standards, and procedures contained in C-M(2002)49 and it's supporting directives take precedence, where they conflict, over the guidelines expressed in USSAN 1-69, dated 21 April 1982.

**4.5. Other Foreign Government Information (FGI).**

4.5.1. Classification designations for FGI often do not parallel U.S. classification designations. Moreover, many foreign governments and international organizations have a fourth level of classification that generally translates as "Restricted," and a category of unclassified information that is protected by law in the originating country and is provided on the condition that it will be treated "in confidence." A table of U.S. and foreign government classification markings can be found in DOD 5200.1-R, Appendix 6.

4.5.2. Other foreign government classified documents shall be marked in English to identify the originating country and the applicable U.S. classification designation. If a classification designation has been applied to a foreign document by the originator, and it is the applicable U.S. English language designation, only the identity of the originating country need be applied to the document. ***Examples:***

A German document marked "Geheim" would be marked: **DEU SECRET**.

A UK document marked "SECRET" would be marked: **GBR SECRET**.

4.5.3. Foreign government documents that are marked with a classification designation that equates to Restricted, and unclassified foreign government documents that are provided to a DOD Component on the condition that they will be treated "in confidence," shall be marked to identify the originating government and whether they are Restricted or provided "in confidence." Additionally, they shall be marked "CONFIDENTIAL - Modified Handling".

***Example:***

A French document marked "Diffusion Restreinte" would be marked:

**FRENCH RESTRICTED INFORMATION**

**Protect as:**

**CONFIDENTIAL - Modified Handling**

4.5.3.1. **(Ref: DOD 5200.1-R, para C6.6.3.)** In order to ensure the protection of FGI provided in confidence (e.g., foreign government "Restricted," or foreign government unclassified information provided in confidence), such information must be classified under EO 12958, as amended. Provide a degree of protection to the FGI at least equivalent to that required by the foreign government or international organization that provided the information. If the foreign protection requirement is lower than the protection required for U.S. CONFIDENTIAL information, the following requirements shall be met:

4.5.3.1.1. The information shall be provided only to those individuals who have a need-to-know and access is required by official duties.

4.5.3.1.2. Individuals given access shall be notified of applicable handling instructions.

4.5.3.1.3. Documents shall be stored so as to prevent unauthorized access.

**4.6. Marking of Foreign Government and NATO Information In DOD Documents.**

4.6.1. When used in DOD documents, FGI must be marked to prevent premature declassification or unauthorized disclosure. To satisfy this requirement, U.S. documents that contain FGI shall be marked on the cover or first page, **"THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION."** In addition, the portions shall be marked to identify the classification level and the country of origin, e.g., **(GBR-C)**; **(DEU-C)**. If the identity of the foreign government must be concealed, the cover or first page of the document shall be marked, **"THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION,"** and applicable paragraphs shall be marked FGI together with the appropriate classification (**FGI-S**). The identity of the foreign government shall be maintained with the record copy, which must be appropriately protected.

4.6.2. The "Derived From" line shall identify the U.S. as well as foreign classification sources. If the identity of the foreign government must be concealed, the "Derived From" line shall contain the marking "Foreign Government information." In that case, the identity of the foreign government will be maintained with the record copy and protected appropriately. A U.S. document shall not be downgraded below the highest level of FGI contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification shall be submitted through the DOD entity that created the document to the originating foreign government.

4.6.3. DOD classified documents that contain extracts of NATO classified information shall be marked as follows on the cover or first page: **"THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION."** Portions shall be marked to identify the NATO information (e.g., **NS**). When NATO or other foreign government RESTRICTED information is included in otherwise unclassified DOD documents, the following statement shall be affixed to the top and bottom of the page containing the information: **"This page contains (indicate NATO or country of origin) RESTRICTED information"**. The restricted portions shall be marked (e.g., **(NR) (GBR-R)**). The cover, (or first page, if no cover) of the document shall contain the following statement: **"This document contains NATO RESTRICTED information not marked for declassification (date of source) and shall be safeguarded in accordance with USSAN 1-69".**

4.6.4. Other foreign government classified documents should be marked in English to identify the originating country and the applicable U.S. classification designation.

4.6.5. Foreign government documents that are marked with a classification designation that equates to RESTRICTED, and unclassified foreign government documents that are provided to a DOD component, should be marked to identify the originating government and whether they are restricted or provided in confidence.

**4.7. 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, C5.4.]*

**4.8. Removable Information Systems Storage Media.** 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 710, Unclassified Label, SF Form 711, ADP Data Descriptor Label, on removable information systems storage media. These are available through the Air Force Publications Distribution System. *[Reference DOD 5200.1-R, Paragraphs 5-407 and 5-409a-b.]*

4.8.1. Many new removable information systems storage media are of size and shape that precludes application of the standard forms. Such media storing classified information must be permanently marked to display the highest classification of stored information.

4.8.2. Designated Approving Authorities (DAA) have the authority to impose restrictions upon, and prohibit the use of, government owned removable information systems storage media for classified systems or networks. DAA approved restrictions will outline clearing, or destruction, procedures for unauthorized devices found in areas where classified processing takes place. Personally owned information systems storage media are prohibited in areas where classified is processed.

4.8.3. The inherent risk of loss of small storage devices should be considered before using them for storing or transporting classified information. Procedures to reduce the potential

for accidental loss must be included in local operating instructions. Include a review of these procedures in the semi-annual self-inspection and ISPRs.

**4.9. Sensitive Compartmented Information (SCI).** *[Reference DOD 5200.1-R, C5.4.11.]*

4.9.1. See AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information*, for Air Force policy on intelligence information.

4.9.2. The Special Security Office (SSO) is the focal point for release and dissemination of SCI. The Director of Central Intelligence Directive (DCID) 6/6, *Security Controls on the Dissemination of Intelligence Information* and *DCID 6/7, Intelligence Disclosure Policy* provide criteria for release of intelligence to foreign officials.

**4.10. Authorized for Release To (REL TO) Markings.** *[Reference DUSD(/)I Memo 27 Sep 2004, subject: Security Classification Marking Instructions.]*

4.10.1. "REL TO" identifies classified information that an originator has predetermined to be releasable based on guidance provided by an Air Force specifically designated foreign disclosure official or has been released, through established foreign disclosure procedures and channels, to the foreign country(ies)/international organizations indicated.

4.10.2. "REL TO" cannot be used with "Not Releasable to Foreign Nationals" (NOFORN) on page markings. When a document contains both NOFORN and REL TO portions, NOFORN takes precedence for the markings at the top and bottom of the page.

4.10.3. The full marking "REL TO USA//applicable country trigraph(s), international organization or coalition force tetragraph" shall be used after the classification and will appear at the top and bottom of the front cover, if there is one, the title page, if there is one, the first page and the outside of the back cover, if there is one. "REL TO" must include country code "USA" as the first country code listed. After the USA, country trigraphic code shall be listed in alphabetical order followed by international organization/coalition tetragraphic codes listed in alphabetical order.

4.10.4. Country codes shall be separated by a comma and a space with the last country code separated by a space, a lower case "and" and a space. ***EXAMPLE:*** TOP SECRET//REL TO USA, EGY and ISR.

4.10.5. When portion marking, countries do not need to be listed unless they are different from the countries listed in the "REL TO" at the top and bottom of the page. Text that is releasable to all the countries listed at the top and bottom of the page shall be portion marked "REL". ***EXAMPLE:*** (TS//REL).

4.10.6. If the information is releasable to countries that are different than those listed in the overall "REL TO" marking, the portion marking has the same format, but with the specific countries/organizations listed alphabetically. ***EXAMPLE:*** The overall document marking is 'SECRET//REL TO USA, NZL and NATO." However, the portion marking may be: (S//REL TO USA, AUS, NZL and NATO) to indicate that information contained in this portion is also releasable to Australia.

4.10.7. "NOFORN" is an authorized control marking for intelligence information IAW DCID 6/6, Security Controls on the Dissemination of Intelligence Information. Do not use the "NOFORN" dissemination control marking on any document, including derivatively

classified documents, without first verifying that the requirements of DCID 6/6 are met and that the marking is actually warranted.

4.10.8. Countries represented with the International Organization for Standardization (ISO) 3166 trigraphic codes can be obtained from the ISPM or from INTELINK on the SIPRNET.

**4.11. Classified Electronic Mail (E-Mail).**

4.11.1. All e-mails and documents accomplished on the SIPRNET, whether classified or unclassified, will contain the correct classification markings. Classified information may not be transmitted on the NIPRNET.

4.11.2. The first marking in the **Subject** line of the e-mail will be the overall classification of the e-mail using these symbols: (S) for Secret, (C) for Confidential, and (U) for Unclassified. Following this will be the subject title, followed by the classification of the subject title. ***Example:*** Subject: (S) Unclassified E-Mail Sample (U).

4.11.3. **Do not send classified messages or mark messages as classified on an unclassified network.**

4.11.4. Place the appropriate classification of the e-mail in all uppercase letters as the first line of the e-mail message text.

4.11.5. Begin the text of the message on the third line, leaving a blank line between the classification marking and the text.

4.11.6. All paragraphs and subparagraphs will be marked with the appropriate portion marking. Use the abbreviated classification symbol at the beginning of all paragraphs and subparagraphs.

4.11.7. Place the appropriate classification of the e-mail in all uppercase letters as the last line of the e-mail message text.

4.11.8. All attachments (if any) will be marked appropriately with overall and portion markings. Indicate the classification of the attachment by placing the abbreviated classification symbol in parentheses before the attachment icon.

4.11.9. Place classification, declassification, and downgrading instructions after the signature block on the left margin.

# Chapter 5

# SAFEGUARDING

## *Section 5A—Control Measures*

**5.1. General.** Air Force personnel are responsible, both personally and officially, for safeguarding classified information for which they have access. Collecting, obtaining, recording, or removing, for any unauthorized use whatsoever, of any sensitive or classified information, is prohibited.

5.1.1. Everyone should be aware that advancing technology provides constantly changing means to quickly collect and transport information. The introduction of electronic storage or transmission devices into areas that store, process, and/or generate classified information increases the risk to that information.

5.1.2. Consult the servicing DAA for specific guidance concerning introduction into areas containing Information Systems (IS). *[Reference DODD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG).]*

## *Section 5B—Access*

**5.2. 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 clearance eligibility according to AFI 31-501, *Personnel Security Program Management*; has signed an SF 312, *Classified Information Nondisclosure Agreement (NdA)*, 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 Executive Branch or as specified by the originator of the material. Also see **paragraph 5.4.1.1** of this AFI. *[References DOD 5200.1-R, C6.2., and EO 12958, as amended, Section 4.1(c.)]*

5.2.1. The Secretary of Defense directed all military members and civilian employees with Top Secret eligibility or access to a specially controlled access category or compartmented information to make a one time verbal attestation to the first paragraph of the SF 312. The verbal attestation must be witnessed by at least one individual in addition to the official who presides over the attestation and manages the process *[Reference DOD 5200.1-PH-1.]* The procedures for personal attestation include:

5.2.1.1. The statement, "Attestation completed on (date)," is placed in the bottom of the Organization block in Item 11 of the SF 312.

5.2.1.2. The individual making the verbal attestation will complete Item 11 of the SF 312. The witness will sign in the Witness block. The presiding official will sign in the Acceptance block.

5.2.1.3. Record the date of attestation in JPAS.

5.2.2. Confirm an individual's access level. The holder of the information must confirm valid need-to-know and must verify the level of access authorization. Those granting access to classified information will confirm a person's access level by:

5.2.2.1. Checking the person's access level, clearance eligibility, and date the person signed the SF 312 and completed Non-SCI Indoctrination, in JPAS; or

5.2.2.2. Confirming it through the employee's security manager, supervisor, or commander or equivalent, or staff agency chief; or

5.2.2.3. Receiving a visit request from a non-DOD visitor's security manager or supervisor. See **paragraph 5.5** for further guidance.

**5.3. Nondisclosure Agreement (NdA).** Signing the NdA is a prerequisite for obtaining access (see **paragraph 5.2**). Unit commanders or equivalents and staff agency chiefs are responsible for ensuring their employees have signed one by checking JPAS 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. Record the NdA on-line through JPAS prior to sending the signed form for retention. ***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.

5.3.1. Retention. Security managers mail the NdA to the following organizations who will retain the NdAs for 50 years.

5.3.1.1. For active military members, to HQ AFPC/DPFFCMI, 550 C St., W, Suite 21, Randolph AFB, TX 78150-4723.

5.3.1.2. For AFRC and ANG members, to HQ ARPC/DPSFR, 6760 E. Irvington Place, #4450, Denver, CO 80280-4450.

5.3.1.3. For retired flag or general officers or civilian equivalents 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/DPFFCMR, 550 C St., W, Suite 21, Randolph AFB TX 78150-4723.

5.3.1.4. For Air Force civilians, to the servicing civilian personnel office:

5.3.1.4.1. HQ AFPC/DPCMP, 550 C St, W, Suite 57, Randolph AFB, TX, 78150-4759.

5.3.1.4.2. Hill: OO-ALC/DPC (AFMC), 6053 Elm Lane, Hill AFB UT 84056-5819.

5.3.1.4.3. Tinker: 72 MSG/DPC (AFMC), 3001 Staff Drive Ste 1AH190B, Tinker AFB OK 73145-3014.

5.3.1.4.4. Robins: 78 MSG/DPC (AFMC), 215 Page Road Ste 325, Robins AFB GA 31098-1662.

5.3.1.4.5. 11 WG and the Pentagon: HQ 11 WG/DPC, 1460 Air Force Pentagon, Washington DC 20330-1460.

5.3.1.4.6. Wright-Patterson: 88 MSG/DPC (AFMC), 4040 Ogden Ave, Wright-Patterson AFB OH 45433-5763.

5.3.1.5. For persons outside the Executive Branch who receive access according to **paragraph 5.4**, the servicing ISPM to the activity granting access will file the NdA.

5.3.2. Refusal To Sign. When a person refuses to sign an NdA, the commander or equivalent, or staff agency chief:

5.3.2.1. Initiates security incident report, in JPAS, that the person refused to sign the NdA.

5.3.2.2. Denies the individual access to classified information.

5.3.2.3. Initiate actions to establish a Security Information File (SIF) according to AFI 31-501.

**5.4. Access by Persons Outside the Executive Branch.**

5.4.1. Policy. MAJCOM/FOA/DRU commanders and HAF 2-digits 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 C6.2.2.

5.4.1.1. Authorizing Officials (those cited in **paragraph 5.4.1** above) may grant access once they have:

5.4.1.1.1. Gained release approval from the originator or owner of the information. Normally, this is the same official identified in **paragraph 5.4.1.1.2.2** below.

5.4.1.1.2. Determined the individual has a current favorable personnel security investigation as defined by AFI 31-501 and a check of JPAS 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/FOA/DRU commanders and HAF 2-digits 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 Air Force Central Adjudication Facility (AFCAF) confirms there is no unfavorable information on the individual in JPAS. When applying this exception, follow the procedures outlined in AFI 31-501, paragraph 3.11. for interim security clearance eligibility.

5.4.1.1.2.1. Authority to grant access to persons outside the Executive Branch without a previous clearance may not be delegated below the listed positions in **paragraph 5.4.1.1.2**.

5.4.1.1.2.2. Before material is released to persons outside the Executive Branch without a previous clearance, the OCA must be contacted and approve the access.

5.4.1.1.3. Determined granting access will benefit the government.

5.4.1.2. Requests for access must include:

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

5.4.1.2.2. Place of employment.

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

5.4.1.2.4. Level of access required.

5.4.1.2.5. Subject of information the person will access.

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

5.4.1.2.7. Comments regarding benefit(s) the U.S. Government may expect by approving the request.

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

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

5.4.2. 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, C6.2.2.1]*

5.4.3. Government Printing Office (GPO). The GPO processes and confirms their personnel's access. *[Reference DOD 5200.1-R, C6.2.2.2]*

5.4.4. Representatives of the Government Accountability Office (GAO). See AFI 65-401, *Relations with the General Accounting Office*, for access requirements. *[Reference DOD 5200.1-R, C6.2.2.3.]*

5.4.5. Historical Researchers. AFHRA OL-A/HOR is the authority for granting access to historical researchers on behalf of the Air Force Historian (HQ USAF/HO). *[Reference DOD 5200.1-R, C6.2.2.4.]*

5.4.5.1. 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.

5.4.5.2. Providing Access.

5.4.5.2.1. The researcher must apply to AFHRA OL-A/HOR in writing for the access. The application will fully describe the project including the sources of documentation that the researcher wants to access.

5.4.5.2.2. If AFHRA OL-A/HOR accepts the request for access, they will provide the researcher with written authorization to go to the nearest Air Force installation security forces office to complete a personnel security questionnaire for a NAC according to AFI 31-501.

5.4.5.2.3. If the results of the NAC are favorable and AFHRA OL-A/HOR 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 35-101). 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 AFHRA OL-A/HOR for retention. Classified information will not be removed from government facilities.

5.4.5.2.4. Other Terms.

5.4.5.2.4.1. 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.

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

5.4.5.2.4.3. Access based on a NAC is valid for Secret and Confidential information but does not meet the requirement for access to RD or SAP information. Access to Top Secret or SCI information is not authorized.

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

5.4.5.2.4.5. 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.

5.4.6. Former Presidential Appointees. Persons who previously occupied policy-making positions to which the President appointed them 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 OCA: *[Reference DOD 5200.1-R, C6.2.2.5.]*

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

5.4.6.2. Uses the same access determination procedures outlined in **paragraph 5.4** of this AFI;

5.4.6.3. Limits the access to specific categories of information over which the Air Force OCA has classification jurisdiction;

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

5.4.6.5. Obtains the individual's agreement to safeguard the information and to submit any notes and manuscript for a security review (AFI 35-101, Chapter 15) to ensure that the documents do not contain classified information or to determine if any classified information should be declassified.

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

5.4.8. Other Situations. Follow the guidance in **paragraph 5.4.1.1** above. *[Reference DOD 5200.1-R, C6.2.2.7.]*

5.4.9. 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/IAPD, 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.) See **Attachment 4** for guidance on transmitting classified information to foreign governments.

5.4.10. 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 or JPAS. (see **paragraph 5.3.1.3**).

**5.5. Access by Visitors.** JPAS is the primary source for confirming access eligibility for DOD and DOD contractor personnel. Visit authorization letters will not be used to pass security clearance information unless JPAS is not available. *[Reference DOD 5200.1-R, C6.2.3.]*

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

5.5.1.1. A non-DOD contractor activity, the supervisor or security manager contacts the office to be visited to determine the desired clearance verification.

5.5.1.2. A DoE activity, the supervisor or security manager prepares and processes DoE Form 5631.20, according to DODD 5210.2, *Access to and Dissemination of Restricted Data*. Also see **paragraph 1.5.1** of this AFI.

5.5.2. Incoming Visit Requests. Air Force activity visit hosts serve as the approval authority for visits to their activities. Use JPAS to confirm security clearances of DOD personnel, including DOD contractors. Installation or activity commanders or equivalents, and staff agency chiefs receiving a visit request:

5.5.2.1. From non-DOD contractors, see DOD 5220.22-M, Chapter 6.

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

**5.6. Preventing Public Release of Classified Information.** See AFI 35-101, Chapter 15, for guidance on security reviews to prevent people from publishing classified information in personal or commercial articles, presentations, theses, books or other products written for general publication or distribution.

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

**5.8. Administrative Controls.**

5.8.1. Top Secret. The security of Top Secret material is paramount. Strict compliance with Top Secret control procedures take precedence over administrative convenience. These procedures ensure stringent need to know rules and security safeguards are applied to our most critical and sensitive information. The Air Force accounts for Top Secret material and disposes of such administrative records according to *WebRims Records Disposition Schedule*.

5.8.1.1. Establishing a Top Secret Control Account (TSCA). Unit commanders or equivalents, 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 unit commander or

staff agency chief will notify the installation ISPM of the establishment of TSCAs and the names of thE TSCO. The TSCO uses AF Form143, **Top Secret Register Page**, to account for each document (to include page changes and inserts that have not yet been incorporated into the basic document) and each piece of material or equipment to include IS media. ***NOTE:*** For IS information systems or microfiche media, TSCOs must either describe each Top Secret document stored on the media on the AF Form 143 or attach a list of the documents to it. This will facilitate a damage assessment if the media are lost or stolen. ***EXCEPTIONS:***

5.8.1.1.1. Top Secret Messages. TSCOs do not 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.

5.8.1.1.2. 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. Retain as prescribed by *WebRims Records Disposition Schedule*. ***NOTE:*** TSCOs may automate their accounts as long as all of the required information is included in the information system.

5.8.1.2. Top Secret Disclosure Records.

5.8.1.2.1. 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. Each person that accesses the attached Top Secret information signs the form prior to initial access.

5.8.1.2.2. 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.

5.8.1.3. Top Secret Inventories. Unit commanders or equivalents, and staff agency chiefs:

5.8.1.3.1. 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 accounted for, discrepancies resolved, and its status is correctly reflected on the corresponding AF Form 143.

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

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

5.8.1.3.4. May authorize the annual inventory of Top Secret documents and material in repositories, libraries, or activities storing large volumes of Top Secret documents and material be limited to a random sampling using the percentage scale indicated

below. If account discrepancies are discovered the commander or equivalent, or staff agency chief must determine if the random sample percentage method will suffice or if a higher percentage inventory will be accomplished. If the higher percentage inventory is chosen, the inventory percentage will increase by no less than 20 percent.

5.8.1.3.4.1. One hundred percent, if there are fewer than 300 Top Secret documents.

5.8.1.3.4.2. No less than 90 percent if the holdings range from 301 to 400 Top Secret documents.

5.8.1.3.4.3. No less than 80 percent if the holdings range from 401 to 500 Top Secret documents.

5.8.1.3.4.4. No less than 70 percent if the holdings range from 501 to 600 Top Secret documents.

5.8.1.3.4.5. No less than 60 percent if the holdings range from 601 to 800 Top Secret documents.

5.8.1.3.4.6. No less than 50 percent if the holdings range from 801 to 1,000 Top Secret documents.

5.8.1.3.4.7. No less than 40 percent if the holdings range from 1,001 to 1,300 Top Secret documents.

5.8.1.3.4.8. No less than 30 percent if the holdings range from 1,301 to 1,800 Top Secret documents.

5.8.1.3.4.9. No less than 20 percent if the holdings range from 1,801 to 2,800 Top Secret documents.

5.8.1.3.4.10. No less than 10 percent if the holdings exceed 2,800 Top Secret documents.

5.8.1.4. Special Access Programs will follow the inventory and accountability requirements prescribed by the AFSAPCO.

5.8.1.5. 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.

5.8.1.6. 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.

5.8.2. Secret. Unit commanders or equivalents, and staff agency chiefs set up procedures for internal control of Secret material. When entering Secret material into a mail distribution system, a receipt is required. Personnel may use AF Form 310, as a receipt.

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

5.8.4. Foreign Government and NATO Information. See DOD 5200.1-R, C6.6., for receipting requirements.

5.8.5. Retention of Receipts. Retain receipt and other accountability records IAW *WebRims Records Disposition Schedule.*

***Section 5C—Safeguarding***

**5.9. Care During Working Hours.**

5.9.1. Personnel removing classified material from storage must:

5.9.1.1. For Top Secret material use AF Form 144, instead of SF Form 703, **Top Secret Cover Sheet** (see **paragraph 5.8.1.2.1**) except as specified in **paragraph 5.8.1.2.2** above. *[Reference DOD 5200.1-R, C6.3.2.1.]*

5.9.1.2. 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.

5.9.1.3. Use the SF Form 702, to record openings and closings for all General Services Administration (GSA)-approved security containers, vaults, and approved secure storage rooms.

5.9.2. The nature of the classified material typically stored within a secure room or vault may preclude the use of cover sheets. Use cover sheets when feasible.

**5.10. End-of-Day Security Checks.** Each unit and staff agency that processes, stores, or generates 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, when security containers are present, even if the container was not opened that day. The "Checked By" column of the SF 702 does not require end-of-day documentation. Activities that are continuously staffed will establish local procedures to provide for daily security checks. Document those daily security checks on the SF 701. Note: Additional security and safety checks may be added in the blanks on the SF 701. All security containers will be listed on the SF 701 for end-of-day checks.

**5.11. Residential Storage Arrangements.**

5.11.1. SECAF and SAF/AA authorize the removal of Top Secret information from designated working areas. Requesters send requests through command IP channels to SAF/AAP [Reference DOD 5200.1-R, C6.3.7.1.].

5.11.2. MAJCOM/FOA/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, C63.7.2.]*.

5.11.3. Contingency Plans. The written procedures will be developed as required by DOD 5200.1-R, C6.3.7.3. to 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, C6.3.4.]*.

**5.12. In-Transit Storage.** Installation commanders:

5.12.1. Provide an overnight repository for classified material. A locally developed awareness program ensures operations dispatch, passenger services, base entry controllers, and billeting staff are aware of the availability.

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

**5.13. Classified Meetings and Conferences.** *[Reference DOD 5200.1-R, C6.3.8.]*

5.13.1. Classified information at meetings, conferences, symposia, portions or sessions of meetings, conferences, etc., during which classified information is to be disseminated shall be limited to appropriately cleared U.S. Government or U.S. Government contractor locations. Auditoriums, assembly halls, or gymnasiums that are primarily for public gatherings at cleared contractor facilities will not be used for a classified meeting at which Top Secret or Secret information would be disclosed, even though it is located on a portion of the contractor's cleared facility *[DOD 5220.22-R, Para C1.4.5.1]*.

5.13.2. Facility Approval Authority. Installation commanders or their designees assess the need to establish and approve secure conference and classified training facilities. Normally, secure conference or classified training facilities are only established at locations where frequent classified meetings or forums occur. If such a facility does not openly 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 7 as a guide for constructing the facility.

5.13.3. Foreign Participation. Hosting officials refer to AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations,* for specific guidance.

5.13.4. Technical Surveillance Countermeasures (TSCM) Surveys. Commanders or equivalents, and staff agency chiefs or their designees determine to do TSCM surveys based on mission sensitivity and threat. See AFI 71-101, Volume 3, *The Air Force Technical Surveillance Countermeasures Program* for additional guidance.

**5.14. 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.

5.14.1. 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 IAW DOD 5200.1-R, paragraph C6.3.9. Aircraft commanders should consult with the local ISPM or senior security forces representative for assistance in complying with these requirements.

5.14.2. 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.

5.14.2.1. Lock the aircraft, when possible, using a GSA-approved changeable combination padlock (Federal Specification FF-P-110) series available from GSA at 800-525-8027, under NSN 5340-00-285-6523 to secure the crew entry door, and/or

5.14.2.2. 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.

5.14.2.2.1. 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.

5.14.2.2.2. Zeroize keyed COMSEC equipment as required by AFKAG-1N, *Air Force Communications Security (COMSEC) Operations*.

5.14.2.3. 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.

5.14.3. 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.

5.14.3.1. Lock the aircraft using a GSA-approved changeable combination padlock (Federal Specification FF-P-110) series available from GSA under NSN 5340-00-285-6523 to secure the crew entry door, and

5.14.3.2. Secure removable classified material IAW **paragraph 5.14.2.2** or **5.14.2.3**.

5.14.4. 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 5.14.2** for restricted areas and **paragraph 5.14.3** for controlled areas.

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

5.14.5.1. Place removable classified material in a storage container and secure the container as described in **paragraph 5.14.2.2** 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.

5.14.5.2. 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.

5.14.5.3. 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.

5.14.5.4. 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.

5.14.6. MAJCOM/FOA/DRUs determine specific risk management security standards for weather diverts and in-flight emergencies. Review AFKAG-1N if the classified information is COMSEC material.

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

**5.15. Information Processing Equipment.**

5.15.1. Machines with Copying Capability. For copiers and facsimile machines or any machines with copying capability (e.g., microfiche machines), personnel consult their unit information manager (3A0X1) 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. Networked copiers present unique security hazards that require DAA approval. Also see **paragraph 5.24** for reproduction authority *[Reference DOD 5200.1-R, C6.3.10.]*.

5.15.2. Protect information system equipment or removable hard disk drive and the information system media at the highest security classification processed by the system *[Reference Air Force Special Security Instruction (AFSSI) 5020, paragraph 2.2.2.]*.

5.15.3. 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. See DOD 5200.1-R, Chapter 6 for storage requirements.

5.15.4. Used toner cartridges may be treated, handled, stored, and disposed of as unclassified, when removed from equipment that has successfully completed its last print cycle.

**5.16. General Safeguarding Policy.** *[Reference DOD 5200.1-R, C6.4.]*

5.16.1. See DOD 5200.1-R, C1.4 and **paragraph 1.6** when requesting waivers to provisions of DOD 5200.1-R, AFPD 31-4, or this publication.

5.16.2. The Air Force does not authorize use of security controls listed in DOD 5200.1-R, paragraph C6.8. *[Reference DOD 5200.1-R, Paragraph C6.8.]*

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

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

5.16.5. Retention of Classified Records. Personnel follow the disposition guidance in *WebRims Records Disposition Schedule.*

**5.17. Standards for Storage Equipment.** GSA-approved security containers must have a label stating "General Services Administration Approved Security Container" affixed to the front of the container usually on the control or top drawer.

5.17.1. If the label is missing or if the container's integrity is in question, the container shall be inspected by a GSA certified inspector.

5.17.2. Organizations without GSA certified inspectors must confirm that contractor inspectors have current GSA inspector training certificates prior to allowing them to determine the security integrity of GSA-approved containers.

5.17.3. Information on obtaining inspections and recertification of containers can be found in FED-STD -809A on the DoD lock program website at: (**https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks**) or by calling DSN 312-551-1212.

5.17.4. Inspecting personnel must note their findings and the source of confirmation on an AFTO Form 36**,** (available on the AFEPL), and retain that record in the container *[Reference DOD 5200.1-R, C6.4.]*.

**5.18. Storage of Classified Information.** *[Reference DOD 5200.1-R, C6.4.]*

5.18.1. Replacement of Combination Locks. Commanders or equivalents, and staff agency chiefs 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 7.

5.18.2. Due to operational necessity or the size and nature of some classified materials, it may be necessary to construct secure rooms for storage because GSA-approved containers or vaults are unsuitable or impractical. Secure rooms must be approved by the ISPM and be constructed IAW DOD 5200.1-R Appendix 7. Access to secure rooms must be controlled to preclude unauthorized access. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. The nature of the classified material typically stored within a secure room or vault may preclude the use of cover sheets.

**5.19. Use of Key-Operated Locks** *[Reference DOD 5200.1-R, C6.4.3.6.1.]*

5.19.1. The authority to determine the appropriateness of using key-operated locks for storage areas containing bulky Secret and Confidential material is delegated to the unit commanders or equivalents, and staff agency chiefs having this storage requirement. When key-operated locks are used, the authorizing official will designate lock and key custodians.

5.19.2. Lock and key custodians use AF Form 2427, (available on the AFEPL) to identify and keep track of keys.

**5.20. Procurement of New Storage Equipment.** *[Reference DOD 5200.1-R, C6.4.5.]*

5.20.1. Requesters of exceptions send their requests through command IP channels to SAF/AAP who will then notify USD/I of the exception *[Reference DOD 5200.1-R, C6.4.2.]*.

5.20.2. See AFMAN 23-110, Volume II, *Standard Base Supply Customer's Procedures [Reference DOD 5200.1-R, C6.4.2.]*.

**5.21. Equipment Designations and Combinations.**

5.21.1. See AFMAN 14-304 for guidance on marking security containers used to store SCI *[Reference DOD 5200.1-R, C6.4.1.]*.

5.21.2. 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. Applying classification marking to SF 700, Part 1, is not required when separated from Part 2 and 2a.

5.21.2.1. Affix the form to the vault or secure door or to the inside of the locking drawer of the security container. Post SF Form 700 to each individual locking drawer of security container with more than one locking drawer, if they have different access requirements.

5.21.2.2. The SF 700 contains Privacy Act information and must be safeguarded from casual view, but must be readily identifiable by anyone that finds the facility unsecured.

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

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

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

**5.22. Repair of Damaged Security Containers** *[Reference DOD 5200.1-R, C6.4.7.]*

5.22.1. Locksmiths or technicians must be GSA certified and either have a favorable NAC or must be continuously escorted while they are repairing security containers. See guidance for unescorted entry to restricted areas in AFI 31-501.

5.22.2. **(DELETED)**

5.22.3. Federal Standard 809, Neutralization and Repair Of GSA-approved Containers can be obtained from the NFESC, 1100 23rd Avenue, Code ESC66, Port Hueneme, California 93043-4370 or at: **http://locks.nfesc.navy.mil/pdf_files/fs809.pdf**.

5.22.4. Locksmiths or technicians who open or repair GSA approved containers must document their actions on an AFTO Form 36 retained in the container.

**5.23. Maintenance and Operating Inspections.** Personnel will follow maintenance procedures for security containers provided in AFTO 00-20F-2, *Inspection and Preventive Maintenance Procedures for Security Type Equipment*. Commanders or equivalents and staff agency chiefs

may authorize trained security managers and security container custodians to perform inspections and preventive maintenance on safes and vaults. Note: Training is conducted by locksmiths or other personnel who are qualified as to technical construction, operation, maintenance, and purpose of such security type equipment *[Reference DOD 5200.1-R, C6.4.7.]*.

**5.24. Reproduction of Classified Material.**

5.24.1. Unit commanders or equivalents, and staff agency chiefs designate equipment for reproducing classified material.

5.24.2. The DAA approves networked equipment used to reproduce classified information. Information managers (3A0X1) issue procedures for clearing copier equipment of latent images.

5.24.3. Security managers:

5.24.3.1. Should display procedures for clearing latent images of equipment used to copy classified material in a location clearly visible to anyone using the equipment;

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

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

**5.25. Control Procedures.** Unit commanders or equivalents and staff agency chiefs designate people/ positions to exercise reproduction authority for classified material in their activities *[Reference DOD 5200.1-R, C6.5.1.]*.

**5.26. Emergency Authority.** *(*See *EO 12958, as amended, Section 4.2(b) and ISOO Directive No. 1, Section 2001.51.)*

5.26.1. In emergency situations, in which there is an imminent threat to life or in defense of the homeland; Military Department or other DOD Component Agency, MAJCOM/FOA/DRU commanders may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

5.26.1.1. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

5.26.1.2. Limit the number of individuals who receive it;

5.26.1.3. Transmit the classified information via approved federal government channels by the most secure and expeditious method according to DOD 5200.1-R, or other means deemed necessary when time is of the essence;

5.26.1.4. Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized federal government entity, in all but the most extraordinary circumstances;

5.26.1.5. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed NdA.

5.26.2. Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information and USD/I by providing the following information through ISPM channels;

5.26.2.1. A description of the disclosed information;

5.26.2.2. To whom the information was disclosed;

5.26.2.3. How the information was disclosed and transmitted;

5.26.2.4. Reason for the emergency release;

5.26.2.5. How the information is being safeguarded, and;

5.26.2.6. A description of the briefings provided and a copy of the signed NdA.

***Section 5D—Disposition and Destruction of Classified Material***

**5.27. Retention of Classified Records.**

5.27.1. Personnel follow the disposition guidance in *WebRims Records Disposition Schedule.*

5.27.2. Unit commanders or equivalents, 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, C6.7.2.1.]*.

**5.28. Disposition and Destruction of Classified Material** *[Reference DOD 5200.1-R, C6.7.2.]*

5.28.1. Shredders purchased from an approved product list that produces a crosscut shred size of ½" x 1/32" or smaller, may continue to be used for destruction of collateral information until 1 October 2008. Employ compensatory measures such as mixing unclassified material with the shredding and stirring of the shredded material. Replacement shredders for destruction of classified information must be purchased from the National Security Agency (NSA)-approved Equipment Product List. Obtain information on approved destruction devices from the NSA Information Assurance web site (**http://www.nsa.gov/ia/government/mdg.cfm**). Please note that this list is FOUO and is updated quarterly on the restricted NSA site.

5.28.2. Records of Destruction Process.

5.28.2.1. Top Secret. TSCOs will ensure:

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

5.28.2.1.2. Destruction is recorded on one of these forms: AF Form 143; AF Form 310; or, AF Form 1565, and,

5.28.2.1.3. 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.

5.28.2.2. Secret and Confidential. A record of destruction is not required. A cleared person must perform the destruction.

5.28.2.3. FGI. See DOD 5200.1-R, C6.6, for destruction of FGI.

5.28.2.4. Destruction of Information System Media. Dispose of information system media according to AFSSI 5020, *Remanence Security*.

5.28.2.5. Disposition of Destruction Records. Dispose of destruction records according to *WebRims Records Disposition Schedule.*

5.28.3. Central Destruction Facility (CDF). The installation commander determines the need for a CDF to destroy classified information, who manages the CDF, and who funds for maintenance. Usually, the decision is based on the amount of classified that is destroyed at the installation and the cost of building and maintaining a CDF, versus purchasing and maintaining other authorized equipment for destruction within individual units.

# Chapter 6

# TRANSMISSION AND TRANSPORTATION

## *Section 6A—Methods of Transmission or Transportation*

### 6.1. General Policy.

6.1.1. Hand carrying Classified Material During Temporary Duty (TDY) Travel. Hand carrying 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 hand carrying 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 confiscated by unauthorized personnel. The servicing AFOSI 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 6.6.3**. 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. SAF/AAP establishes Air Force policy and procedures for transmission and transportation of classified information and material *[Reference DOD 5200.1-R, C7.1.1.1.]*.

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, C7.1.1.1.]*.

6.1.5. Electronic Transmission and Physical Transportation of COMSEC Material. Personnel may acquire information on electronic transmission and physical transportation of COMSEC information and material from their supporting COMSEC manager. *[Reference AFI 33-201, AFI 33-211, AFI33-275, and DOD 5200.1-R, C7.1.1.2.]*

6.1.6. Releasing Other Agency Information Outside of the DoD. Personnel go direct to owners of other agency information to request permission to release the information outside the DoD *[Reference DOD 5200.1-R, C7.1.1.4.]*.

**6.2. Transmission and Transporting Top Secret Information.** *[Reference DOD 5200.1-R, C7.1.2.]*

6.2.1. Electronic Means. Obtain information about transmitting Top Secret information via electronic means from their Information Assurance office. See **paragraph 5.8** *[Reference DOD 5200.1-R, C7.1.2.2.]*.

6.2.2. DOD Component Courier Service. The Air Force does not have its own courier service *[Reference DOD 5200.1-R, C7.1.2.4.]*.

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 C7.1.2.5.]*

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

6.2.3.2. Transporting 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 and Transporting Secret Information.** *[Reference DOD 5200.1-R, C7.1.3.]*

6.3.1. Also see AFI 31-601 *[Reference DOD 5200.1-R, C7.1.3.2.]*.

6.3.2. The Air Force authorizes the use of the current holder of the GSA contract for overnight delivery of Secret information in urgent cases and when the delivery is between DOD Components and their cleared contractor facilities within the United States and its Territories. This applies to locations in Alaska, Hawaii, and Puerto Rico when overnight delivery is possible. USD/I has already ensured the conditions cited in DOD 5200.1-R, paragraph C7.1.3.3, have been met *[Reference DOD 5200.1-R, C7.1.3.3.]*

6.3.2.1. The Defense Security Service maintains a list of authorized GSA contract overnight delivery services at **http://www.dss.mil/isec/approved_overnight.htm**.

6.3.2.2. The carriers identified on the DSS list may be used for urgent overnight delivery of Secret and Confidential material within the continental United States (CONUS) when overnight delivery cannot reasonably be accomplished by the U.S. Postal Service. However, classified COMSEC information may not be transmitted overnight. Controlled Cryptographic Information (CCI) that is unclassified may be shipped overnight.

6.3.2.3. Carrier personnel should not be notified that the package contains classified material.

6.3.2.4. Packages are typically shipped on Monday through Thursday only. This ensures that the package does not remain in the possession of the carrier service over a weekend. However, the security manager may approve shipment on other days providing the receiver has appropriate procedures in place. These procedures must ensure that a cleared person will receive and sign for the package on Saturday, Sunday, or holidays, and that he or she is able to secure the package in approved storage. *[DOD 4525.8-M.]*

6.3.2.5. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and for verification of the correct mailing address.

6.3.3. For more information on protective security service carriers see DOD 5220.22-R, *Industrial Security Regulation*, AFI 31-601, AFPD 24-2, *Preparation and Movement of Air Force Materiel*, and AFI 24-201, *Cargo Movement. [Reference DOD 5200.1-R, C7.1.3.8.]*

6.3.4. Electronic Means. Obtain information about transmitting Secret information via electronic means from the supporting Information Assurance office.

**6.4. Transmitting Confidential Information.** *[Reference DOD 5200.1-R, C7.1.4.]*

6.4.1. Since first class mail bearing the "Return Service Requested" notice is an option for transmitting Confidential material, recipients must protect it as Confidential material unless they determine the contents are unclassified. ***EXCEPTION:*** Official Mail Center (OMC) and Activity Distribution Offices (ADO) will comply with the provisions of *DOD 4525.8-M/AF* Sup.

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

**6.5. Transmission of Classified Material to Foreign Governments.** *[Reference DOD 5200.1-R , C7.1.5.]*

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, C7.1.5.1.]*.

6.5.2. US classified material will not be shipped from a US industrial activity to a foreign entity *[Reference DOD 5200.1-R, C7.1.5.1.]*.

***Section 6B—Preparation of Material for Transmission***

**6.6. Envelopes or Containers.** *[Reference DOD 5200.1-R, C7.2.]*

6.6.1. For the purpose of this policy, an activity is a facility *[Reference DOD 5200.1-R, C7.2.1.1.5.]*.

6.6.2. Receipts. See receipting requirements at **paragraph 5.8**.

6.6.2.1. Senders trace unacknowledged receipts:

6.6.2.1.1. Within 30 days for material sent within CONUS.

6.6.2.1.2. Within 45 days for material sent outside CONUS.

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

6.6.2.3. 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.

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

6.6.3.1. Laptops are password protected.

6.6.3.2. Laptops and disks are marked according to DOD 5200.1-R, paragraphs C5.4.8, C5.4.9, and C5.4.10.

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

6.6.3.4. Classified media or systems will be wrapped or secured within a container if outer classification markings are visible.

***Section 6C—Escort or Handcarrying of Classified Material***

**6.7. General Provisions.** *[Reference DOD 5200.1-R, C7.3.]*

6.7.1. Authorization. *[Reference DOD 5200.1-R, C7.3.1.1.]*

6.7.1.1. The unit commander or equivalent, or staff agency chief authorizes appropriately cleared couriers to handcarry classified material on commercial flights. See DOD 5200.1-R, paragraph C7.3.1.2., for required documentation and this AFI, **paragraph 6.1.1**, for a cautionary statement regarding handcarrying classified material.

6.7.1.2. The unit commander or equivalent, 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, C7.3.1.2.]*.

6.7.3. Each Air Force activity or unit that releases classified material to personnel for handcarrying: *[Reference DOD 5200.1-R, C7.3.1.1.]*

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 or equivalents, staff agency chiefs, or security managers issue and control DD Form 2501 (Safeguard), **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 situations. ***EXCEPTION:*** Documentation is not necessary when handcarrying classified information to activities within an installation (i.e., Air Force installation, missile field, or leased facilities within the local commuting area). ***NOTE:*** Account for DD Form 2501 (Safeguard) as prescribed in AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT) [Reference DOD 5200.1-R, C73.2.2.]*.

# Chapter 7

## SPECIAL ACCESS PROGRAMS (SAPS)

**7.1. Control and Administration** *[Reference DOD 5200.1-R, C8.1.3.3.]*

7.1.1. SAF/AAZ administers SAPs for the Air Force. See AFPD 16-7, *Special Access Programs.* ***EXCEPTION:*** HQ USAF/XOI controls SCI programs.

7.1.2. Contractor personnel associated with Special Access Programs (SAPs) administered under DOD 5220.22-M Sup 1 and AFI 16-701 may be nominated and approved by the cognizant Program Security Officer (PSO) to fulfill the roles and responsibilities of a security manager.

**7.2. Code Words and Nicknames.** Unit commanders or equivalents, and staff agency chiefs obtain code words and nicknames through channels from the servicing control point (normally, the MAJCOM/FOA/ DRU Information Management activity) *[Reference DOD 5200.1-R, C8.1.4.6.1]*.

# Chapter 8

## SECURITY EDUCATION AND TRAINING

### *Section 8A—Policy*

**8.1. General Policy.** Effective information security training is a cornerstone of the Air Force Information Security Program. All Air Force personnel need information security training whether they have access to classified information or not. All Air Force personnel are 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 or equivalents, and staff agency chiefs are responsible for ensuring that personnel are knowledgeable and understand their responsibility to protect information and resources deemed vital to national security.

**8.2. Methodology.** The Air Force 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 Air Force 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. SAF/AAP is responsible for coordinating development of Air Force specific information security training course materials and curriculums.

8.3.3. Commanders or equivalents, and staff agency chiefs 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, they will:

8.3.3.1. Ensure appointed security managers receive training through the ISPM 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 name 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, as appropriate.

8.3.5. ISPMs that oversee security managers 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 as part of the annual ISPR (see **para 1.4.2**).

8.3.5.3. Developing and conducting classroom or one-on-one training for newly appointed security managers.

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 training file.

8.3.5.8. Providing military members who complete information security managers training with a certificate, which they can use to enter course completion into their on-the-job training record or other official records, as appropriate.

8.3.5.9. If full-time contractor performance or services is required or anticipated to support the Information Security work center or a specific security discipline (information, personnel, or industrial), the ISPM will assure the following language is inserted into the statement of work (SOW). "The contractor will be required to participate in the government's in-house and web-based security training program under the terms of the contract. The government will provide the contractor with access to the on-line system."

8.3.5.10. When contractors require Information Security work center training, the ISPM must approve the contractor's enrollment in any web-based training course. In addition, the ISPM must notify, in writing, the 37 TRS/DORM Training Manager of this action, to include the contractor's name, SSAN, contract number, and contractor's cage code and contract performance location. The request may be Faxed to DSN 473-4150.

8.3.6. 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, as necessary.

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. Providing security management, awareness, and training to on-base contractor visitor groups integrated into the organization unless the mission, operational requirements, autonomous nature or other factors require them to establish and maintain their own security program under the NISPOM.

***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 or within 90 days of assignment to the unit, whichever is shorter.

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. Note: Security manager records initial security training for cleared personnel in the appropriate JPAS "Indoctrinate Non-SCI Access" field. Document training of "Uncleared" personnel in local training records.

8.4.1.1.1. Indoctrinate to the investigation position code reflected in the Unit Manpower Document.

8.4.1.1.2. Verify that current eligibility meets or exceeds the access level.

8.4.1.1.3. Do not document indoctrination before the NdA execution has been recorded in JPAS.

8.4.1.2. The Air Force Information Security Training Standards establish initial information security training for cleared personnel, under column heading (C). ***Note:*** A standard lesson plan meeting the requirements of the training standard is available from the AFSFC web site that includes the NATO training prescribed below.

8.4.1.3. Due to the need for expeditious access to NATO classified information associated with ongoing operations and the Air Force's Aerospace Expeditionary Force (AEF) mission, all cleared military, civilian, and contractor personnel will receive a NATO security briefing. This does not mean every cleared military, civilian, or contractor will be granted access to NATO classified information. The access determination will be made by the access granting authority IAW AFI31-406, paragraph 4.2. A written acknowledgement of the NATO training will be maintained. If the member has access to NATO, also record in JPAS.

**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. The Air Force Information Security Program Training Standards establish initial security education orientation training for uncleared personnel. ***NOTE:*** A standard lesson plan meeting the requirements of the training standard is available from the AFSFC web site: **https://www.mil.lackland.af.mil/afsf/** that includes the initial NATO training required of all uncleared personnel.

8.5.2. Initial training for uncleared personnel will be documented locally.

***Section 8C—Special Requirements***

**8.6. Original Classification Authorities (OCAs).** IPOs are responsible for administering specialized training to OCAs IAW DOD 5200.1-R. Training must be conducted prior to OCA authority being exercised. Personnel who propose, prepare, develop, or facilitate original classification decision actions for OCAs will be trained in original and derivative classification, marking, and preparation of security classification guidance. SAF/AAP has developed training standards for OCA training which can be found on the Information Protection Community of Practice (CoP) at: **https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SF-AF-10**. This specialized training is in addition to the other information security training also available on this CoP.

**8.7. Derivative Classifiers, Security Personnel, and Others.** Security managers are responsible for administering information security training to all personnel IAW DOD 5200.1-R. The training standards can be found on the Information Protection Community of Practice (CoP) at: **https://wwwd.my.af.mil/afknprod/ASPs/CoP/OpenCoP.asp?Filter=OO-SF-AF-10**.

**8.8. Restricted Data (RD)/Formerly Restricted Data (FRD).** Within the DOD, an RD management official shall be appointed in each agency. SAF/AA is appointed the Air Force Management Official.

***Section 8D—Continuing Security Education/Refresher Training***

**8.9. Continuing and Refresher Training.** Commanders or equivalents, and staff agency chiefs ensure that each person receives continuing training throughout their duty assignment.

8.9.1. All personnel will receive Continuing Security Education/Refresher Training annually IAW the Air Force Information Security Training Standards.

8.9.2. 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.

8.9.3. Tailor training to mission needs.

8.9.4. Continuing Security Education/Refresher Training must include ensuring individuals have the most current security guidance applicable to their responsibilities. The annual Air Force Total Force Awareness Training (TFAT) Information Protection block of instruction is mandatory for all Air Force personnel, and meets the general security awareness required. Additional training relating to job requirements (functional, program, security clearances, etc.), or assignments (NATO, PCS, etc.) will be required.

8.9.5. Other related material to be considered include a general overview of the unclassified controlled information (**Attachment 2**), foreign disclosure, security and policy review processes and protection requirements.

***Section 8E—Access Briefings and Termination Debriefings***

**8.10. Access Briefings.**

8.10.1. Supervisors, security managers or designated officials conduct and document the following access briefings, as appropriate. The exception is **para 8.10.1.6** All documentation of SCI indoctrinations, debriefs, and NdAs are maintained only within the SSO.

8.10.1.1. Brief and execute the SF 312, prior to granting individual access to classified information. The SF 312 may also be used to document attestations. Both SF 312 completion and attestations will be recorded in JPAS *[Reference AFI 31-401,* **paragraph 5.3***]*.

8.10.1.2. Brief and execute the DD Form 2501 (Safeguard), Courier Authorization, as necessary, when an individual is authorized to escort or handcarry classified information. *[Reference AFI 31-401,* **paragraph 6.8***]*

8.10.1.3. 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.]*

8.10.1.4. 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.]*

8.10.1.5. 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, Safeguarding the Single Integrated Operational Plan (SIOP), paragraph 7.1.]*

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

8.10.2. JPAS will also be used to record NATO, CNWDI, and SIOP-ESI access authorizations.

**8.11. Termination Debriefings.**

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

8.11.1.1. 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.

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

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

8.11.1.3.1. Protect classified and unclassified controlled information (**Attachment 2**) to which they have had access.

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

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

8.11.1.3.4. Potential civil and criminal penalties for failure to fulfill their continuing security responsibilities.

8.11.2. For NATO access termination debriefing, see AFI 31-406, paragraph 4.10.

8.11.3. Commanders or equivalents, and staff agency chiefs ensure personnel accessed to SCI receive a termination debriefing from the Special Security Officer when access is no longer required, is suspended, or is revoked.

8.11.4. For SIOP-ESI termination briefing, see AFI 10-1102.

8.11.5. Dispose of AF Form 2587 according to *WebRims Records Disposition Schedule.*

8.11.6. Update JPAS to reflect termination of accesses.

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

8.12.1. Debriefs the individual orally.

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

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

8.12.4. Forwards the AF Form 2587 to the servicing ISPM for SIF processing according to AFI31-501.

***Section 8F—Program Oversight***

**8.13. General.**

8.13.1. Commanders or equivalents, and staff agency chiefs are responsible for ensuring systems are set up to determine training requirements, develop training, and evaluate effectiveness of the training.

8.13.2. ISPMs will make security education and training a special interest item during annual ISPRs.

8.13.3. Commanders or equivalents, and staff agency chiefs will ensure that their security education and training program is given close scrutiny during inspections, self-inspections and SAVs.

8.13.4. 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***

**8.14. Coordinating Requests for Training.**

8.14.1. Commanders or equivalents, and staff agency chiefs will ensure that requests for formal training are coordinated through unit, installation and MAJCOM training channels.

8.14.2. **(DELETED)**

# Chapter 9

## ACTUAL OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

**9.1. Policy.** *[Reference DOD 5200.1-R, C10.]*

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 potential compromise of classified information, a damage assessment will be conducted to judge the effect that the compromise has on national security.

9.1.2. Suspected instances of unauthorized public disclosure of classified information shall be reported promptly and investigated to determine the nature and circumstances of the suspected disclosure, the extent of the damage to national security, and the corrective and disciplinary action to be taken *[DODD 5210.50, Para 4.]*.

**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, as amended. 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 its implementing directives.

9.2.1.1.3. To create or continue a SAP contrary to the requirements of EO 12958, as amended.

9.2.1.2. Security Infraction. Any knowing, willful or negligent action contrary to the requirements of EO 12958, as amended 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. Unauthorized individuals include those individuals with the appropriate security clearance but do not have a valid need-to-know.

9.2.3. A potential 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. Information System (IS) Deviations.** Coordinate all security deviations involving information systems with the local ISPM and the supporting information assurance office to begin an evaluation on the impact of the incident to national security and the organization's operations. If COMSEC material is involved, refer to AFI 33-212, *Reporting COMSEC Deviations* (will be incorporated in AFI 33-201, Volume 3, *COMSEC User Requirements*).

**9.4. Sensitive Compartmented Information (SCI) Incidents.** Safeguard all SCI material and report incidents involving SCI to the Special Security Officer.

**9.5. Special Access Program (SAP) Incidents** Report security incidents involving DOD SAP materiel through local SAP channels to the Director, Special Programs OUSD(P).

**9.6. Classification.**

9.6.1. 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 unsecured 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 information system environment when the system has been appropriately purged and the correspondence does not contain other classified information.

9.6.1.1. 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.

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

9.6.2. All security incident reports will, as a minimum, be marked "For Official Use Only." Refer to DOD Regulation 5400.7/Air Force Supplement, *Freedom of Information Act Program*.

**9.7. Public Release.** Security incident reports cannot be released into the public domain until they have undergone a security review *[Reference AFI 35-101, Chapter 15.]* Unauthorized disclosure of classified information to the public must be processed IAW DODD 5210.50.

**9.8. Reporting and Notifications.**

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

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

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

9.8.2.2. Report compromises/potential compromises for the following incidents through command IP channels to SAF/AAP:

9.8.2.2.1. Classified in the public media.

9.8.2.2.2. Foreign intelligence agencies.

9.8.2.2.3. Criminal activity.

9.8.2.2.4. NATO classified information.

9.8.2.2.5. FGI.

9.8.2.2.6. RD or FRD.

9.8.2.2.7. Disclosure to foreign nationals.

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

9.8.2.4. Notify SAF/AAZ through the appropriate SAP channels when the compromise involves special access information.

9.8.3. The appointing authority will notify the OCA, or the originator when the OCA is not known, when it is determined there is a compromise, potential compromise, or loss of classified information. Refer to **paragraph 9.6.1** of this AFI for security classification marking requirements.

**9.9. 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.

9.9.1. The commander or equivalent, or staff agency chief of the activity responsible for the security incident will appoint an inquiry official to conduct a preliminary inquiry. See **Attachment 5** for a sample appointment memorandum. Refer to **paragraph 9.6.1** of this AFI for appointment memorandum classification requirements. The guidelines for selection of the inquiry/investigative official are found in **paragraph 9.11.2**.

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

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

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

9.9.3. A preliminary inquiry report will be completed using the sample report format at **Attachment 6** 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 9.6** of this AFI for report classification requirements.

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

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

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

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

9.9.5. 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 potential compromise the appointing authority notifies the OCA to perform a damage assessment.

9.9.6. If the inquiry reveals suspected unauthorized disclosure to the public notify SAF/AAP through IP channels [DODD 5210.50, Para 5.2.1.]. 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. Specifically address:

9.9.6.1. When, where, and how the incident occurred.

9.9.6.2. Was classified information compromised?

9.9.6.3. If compromise occurred, what specific classified information and/or material was involved?

9.9.6.4. If classified information is alleged to have been lost, what steps were taken to locate the material?

9.9.6.5. In what specific media article or program did the classified information appear?

9.9.6.6. To what extent was the compromised information disseminated?

9.9.6.7. Was the information properly classified?

9.9.6.8. Was the information officially released?

9.9.6.9. Are there any leads to be investigated that might lead to the identification of the person responsible for the compromise?

9.9.6.10. Will further inquiry increase the damage caused by the compromise?

9.9.7. Submit a completed Department of Justice (DoJ) Media leak Questionnaire, available from **https://wwwmil.lackland.af.mil/afsf/** through ISPM channels to USD(I), who will coordinate with DOD General Counsel to determine whether a referral to the DoJ for prosecution is warranted.

**9.10. Damage Assessment.**

9.10.1. A damage assessment is an analysis to determine the effect of a compromise of classified information on the national security. It will be initiated by the OCA upon notification of a potential 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.

9.10.2. The OCA must:

9.10.2.1. Verify the classification and duration of classification initially assigned to the information. If the OCA determines the information should be declassified, the reporting activity will be notified.

9.10.2.2. Set up damage assessment controls and procedures.

9.10.2.3. Provide a copy of the damage assessment to the inquiry or investigating official.

**9.11. Formal Investigation.**

9.11.1. A formal investigation is 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.

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

9.11.2.1. The appointment letter provides authority to conduct an investigation, swear witnesses, and examine/copy documents, files and other data relevant to the inquiry.

9.11.2.2. The investigative official is the personal representative of the Appointing Authority and/ or the Commander. The investigative official must be impartial, unbiased, objective, thorough, and available.

9.11.2.3. The investigative official must be a commissioned officer, senior NCO (E-7 and above), or a civil service employee equivalent (GS-9 and above).

9.11.2.4. The investigation will be the investigative official's only duty (unless the Appointing Authority determines otherwise) until the report is completed and approved by the Appointing Authority.

9.11.2.5. Appointing Authorities will not appoint an investigative official who is retiring, separating, or being reassigned within 180 days.

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

**9.12. Management and Oversight.**

9.12.1. The inquiry/investigative official will route the completed report through the servicing ISPM for review before forwarding it to the appointing authority.

9.12.2. The appointing authority will:

9.12.2.1. Close the inquiry/investigation unless MAJCOM/FOA/DRU directives indicate otherwise.

9.12.2.2. Determine if administrative or disciplinary action is appropriate. See AFI 31-501, Chapter 8 and applicable military and civilian personnel publications.

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

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

9.12.2.5. Dispose of the report according to the instructions in *WebRims Records Disposition Schedule.*

9.12.3. The ISPM will:

9.12.3.1. Provide technical guidance and review of preliminary inquiry and formal investigation reports.

9.12.3.2. Monitor the status of security incidents.

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

**9.13. Unauthorized Absences.** Report all unauthorized absences to the ISPM and appropriate AFOSI detachment *[Reference DOD 5200.1-R, C10.1.9.]*.

**9.14. Prescribed Forms. These forms are prescribed throughout this AFI and are available through the Air Force Publications Distribution system:**

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 349, *Receipt for Documents Released to Accredited Representatives of Foreign Nations*

AF Form 1565, *Entry, Receipt, and Destruction Certificate*

AF Form 2427, *Lock and Key Control Register*

AF Form 2587, *Security Termination Statement; Air Force Technical Order Form (AFTO) 36, Maintenance Record for Security Type Equipment*

SF 311, *Agency Security Classification Management Program Data*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Information*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check Sheet*

SF 703, *Top Secret Cover Sheet*

SF704, *Secret Cover Sheet*

SF 705, *Confidential Cover Sheet*

SF706, *Top Secret Label*

SF 707, *Secret Label*

SF 708, *Confidential Label*

DD Form 1847, *Sensitive Compartmented Information Indoctrination Memorandum*

DD Form 1847-1, *Sensitive Compartmented Information Nondisclosure Statement*

DD Form 1848, *Sensitive Compartmented Information Debriefing Memorandum*

DD Form 2024, *DOD Security Classification Guide Data Elements*

DD Form 2501 *(Safeguard), Courier Authorization*

DoE Form 5631.20, *Request for Visit or Access Approval*

**9.15. Adopted Forms.**

AF 349, AF 2587, 2427, and AFTO 36

CARROL H. CHANDLER, Lt. Gen, USAF
Deputy Chief of Staff Air & Space Operations

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

***References***

Executive Order 12958, as amended. *Classified National Security Information*

Executive Order 12829, *National Industrial Security Program*

ISOO Directive Number 1, *Classified National Security Information*

10 C.F.R. 1045.1 Subpart A, *Program Management of the Restricted Data and Formerly Restricted Data Classification System*

DCID 6/6, *Security Controls on the Dissemination of Intelligence Information*

DCID 6/7, *Intelligence Disclosure Policy*

DOD 4000.25-8-M, *Military Assistance Program Address Directory System*

DOD 4528.8-M, *DOD Official Mail Manual*

DODD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs*

DODD 5210.50, *Unauthorized Disclosure of Classified Information to the Public*

DOD 5200.1-H, *DOD Handbook for Writing Security Classification Guidance*

DOD 5200.1-R, *Information Security Program*

DOD 5200.1-PH, *DOD Guide to Marking Classified Documents*

DOD 5200.1-PH-1, *Classified Information Nondisclosure Agreement (Standard Form 312)*

DODD 5210.2, *Access to and Dissemination of Restricted Data*

DODD 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*

DODD 5230.24, *Distribution Statements on Technical Documents*

DOD 5220.22-M, *National Industrial Security Program Operating Manual*

DOD 5220.22-R, *Industrial Security Regulation*

DODI 5240.11, *Damage Assessments*

DOD 5400.7-R/Air Force Supplement, *DOD Freedom of Information Act Program*

DODD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG).]*

Naval Facilities Engineering Service Center Technical Data Sheet, TDS-2000-SHR, *Neutralizing "Locked-Out" Security Containers* (Available from DOD Lock Program website.)

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, *Air Force Foreign Disclosure and Technology Transfer Program*

AFPD 16-7, *Special Access Programs*

AFI 16-701, *Special Access Programs*

AFMAN 23-110, *USAF Supply Manual*

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

AFI 24-201, *Cargo Movement*

AFI 31-101, *Air Force Installation Security Program*

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

AFPD 31-4, *Information Security*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFPD 33-2, *Information Protection* (will be *Information Assurance)*

AFI 33-201, Volume 1, *Communications Security* (COMSEC)

AFI 33-201, Volume 2, *COMSEC User Requirements*

AFI 33-202 Volume 1, *Network and Computer Security*

AFI 33-204, *Information Assurance (IA) Awareness, Program*

AFI 33-211, *Communications Security (COMSEC) User Requirements (will be incorporated in AFI 33-201 V2,* COMSEC Users Requirements)

AFI 33-212, *Reporting COMSEC Deviations (will be incorporated in AFI 33-201 V2,* COMSEC Users Requirements

AFI 33-275, *Controlled Cryptographic Items (CCI )* (will be incorporated in AFI 33-201 V1)

AFI 33-360, *Air Force Privacy Act Program*

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

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

AFMAN 36-2108, *Enlisted Classification*

AFPD 36-22, *Air Force Military Training*

AFI 36-2201, Volume 1, *Training, Development, Delivery, and Evaluation*

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

AFMAN 36-505, *Skill Coding*

AFI 36-704, *Discipline and Adverse Actions*

AFI 36-2406, *Officer and Enlisted Evaluation Systems*

AFMAN 37-138, *Records Disposition – Procedures and Responsibilities*

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*

AFI 90-301, *Inspector General Complaints Resolution*

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

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

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

AFSSI 5020, *Remanence Security* (will be incorporated in forthcoming AFI 33-202 V3, *Network Security Program) WebRims Records Disposition Schedule*

***Abbreviations and Acronyms***

**ADO**—Activity Distribution Offices

**ADP**—Automatic Data Processing

**AEF**—Aerospace Expeditionary Force

**AF**—Air Force

**AFCAF**—Air Force Central Adjudication Facility

**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

**ANACI**—Access National Agency Check with Inquiry

**AIS**—Automated Information System

**BITC**—Base Information Transfer Center

**CCI**—Controlled Cryptographic Information

**CDF**—Central Destruction Facility

**CNWDI**—Critical Nuclear Weapon Design Information

**COMSEC**—Communications Security

**CONUS**—Continental United States

**CSA**—Cognizant Security Authority

**DAA**—Designated Approving Authority

**DCID**—Director Central Intelligence Directive

**DCII**—Defense Clearance and Investigations Index

**DCS**—Defense Courier Service

**DD**—Department of Defense (Used for DOD Forms)

**DIA**—Defense Intelligence Agency

**DEA**—Drug Enforcement Administration

**DOD**—Department of Defense

**DODD**—Department of Defense Directive

**DODI**—Department of Defense Instruction

**DODSI**—Department of Defense Security Institute (Now DSSA)

**DoE**—Department of Energy

**DRU**—Direct Reporting Unit

**DSS**—Defense Security Service (Formerly DIS and DODSI)

**DSSA**—Defense Security Service Academy

**DTIC**—Defense Technical Information Center

**EES**—Enlisted Evaluation System

**EO**—Executive Order

**FGI**—Foreign Government Information

**FMS**—Foreign Military Sales

**FOA**—Field Operating Agency

**FOIA**—Freedom of Information Act

**FOUO**—For Official Use Only

**FRD**—Formerly Restricted Data

**GAO**—Government Accountability Office

**GILS**—Government Information Locator System

**GPO**—Government Printing Office

**GSA**—General Services Administration

**HAF**—Headquarters Air Force

**IDS**—Intrusion Detection System

**IG**—Inspector General

**IMT**—Information Management Tool

**INTELINK**—Intelligence Link

**IO**—Investigating Officer

**ISCAP**—Interagency Security Classification Appeals Panel

**ISO**——International Organization for Standardization

**ISOO**—Information Security Oversight Office

**ISPM**—Information Security Program Manager

**ISPR**—Information Security Program Review

**JPAS**—Joint Personnel Adjudication System

**LFC**—local files check

**MAJCOM**—Major Command

**MDR**—Mandatory Declassification Review

**MIS**—Management Information System

**NAC**—National Agency Check

**NACLC**—National Agency Check, Local Agency Check, Credit Check

**NARA**—National Archives and Records Administration

**NATO**—North Atlantic Treaty Organization

**NCR**—National Capital Region

**NdA**—Nondisclosure Agreement

**NFESC**—Naval Facilities Engineering Services Center

**NGA**—National Geospatial-Intelligence Agency

**NIMA**—National Imagery and Mapping Agency

**NIPRNET**—Non-Secure Internet Protocol Router Network

**NISPOM**—National Industrial Security Program Operating Manual

**NOFORN**—Not Releasable to Foreign Nationals

**NSA**—National Security Agency

**NSN**—National Stock Number

**OADR**—Originating Agency's Determination Required

**OCA**—Original Classification Authority

**OMB**—Office of Management and Budget

**OMC**—Official Mail Center

**OPF**—official personnel file

**ORCON**—Originator Control

**PA**—Privacy Act

**PCS**—permanent change of station

**PKI**—Public Key Infrastructure

**PL**—Protection Level

**POC**—point of contact

**RCS**—Report Control Symbol

**RD**—Restricted Data

**REL TO**—Release To

**SAF**—Secretary of the Air Force

**SAP**—Special Access Program

**SAV**—staff assistance visit

**SBU**—Sensitive But Unclassified

**SCG**—Security Classification Guide

**SCI**—Sensitive Compartmented Information

**SCIF**—Sensitive Compartmented Information Facilities

**SEI**—Special Experience Identifier

**SF**—standard form

**SIF**—security information file

**SIOP—ESI—**Single Integrated Operational Plan-Extremely Sensitive Information

**SIPRNET**—Secret Internet Protocol Router Network

**SOIC**—Senior Official of the Intelligence Community

**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

**URL**—uniform resource locator

**VAL**—visit authorization letter

**VGSA**—visitor group security agreement

***Terms***

**Access**—the ability or opportunity to gain knowledge of classified information.

**Agency**—any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

**Automated Information System (AIS)**—Any telecommunications and/or computer- related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. The entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02).

**Automatic Declassification**—the declassification of information based solely upon (1) the occurrence of a specific date or event as determined by the OCA; or (2) the expiration of a maximum time frame for duration of classification established under EO 12958, as amended.

**Classification**—the determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

**Classification/Declassification Guide**—a documentary form of classification/declassification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

**Classification Guidance**—any instruction or source that prescribes the classification of specific information.

**Classified National Security Information or Classified Information**—official information that has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

**Confidential Source**—any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

**Damage to The National Security**—harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

**Declassification**—the determination that, in the interests of national security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation.

**Declassification Authority**—the official who authorized the original classification, if that official is still serving in the same position; the originator's current successor in function; a

supervisory official of either; or officials delegated declassification authority in writing by the agency head or the senior agency official.

**Derivative Classification**—the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

**Direct Reporting Unit (DRU)**—A DRU has a specialized and restricted mission, and is directly subordinate to the Chief of Staff, United States Air Force or to his representative at HAF.

**Document**—any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

**Downgrading**—a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

**Field Operating Agency (FOA)**—A subdivision of the Air Force, directly subordinate to a HQ USAF functional manager. FOAs perform field activities beyond the scope of any of the major commands. Their activities are specialized or associated with an Air Force wide mission.

**File Series**—file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

**Foreign Government Information (FGI)**—(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as ―foreign government information‖ under the terms of a predecessor order.

**Formerly Restricted Data (FRD)**—defined by the Atomic Energy Act as classified information which has been removed from the RD category after DoE and the DOD have jointly determined that it relates primarily to the military utilization of atomic weapons, and can be adequately safeguarded as national security information.

**Information**—any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the United States Government. ―Control‖ means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

**Information System (IS)**—1. Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice, and/or data, including software, firmware, and hardware. (***NOTE:*** This includes automated information systems). 2. (DOD) The entire infrastructure, organization, and

components that collect, process, store, transmit, display, disseminate, and act on information. (JP 1-02).

**Infraction**—any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a violation, as defined below.

**Integral File Block**—a distinct component of a file series, as defined in this section, which should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

**Integrity**—the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

**Mandatory Declassification Review (MDR)**—the review for declassification of classified information in response to a request for declassification.

**Multiple Sources**—two or more source documents, classification guides, or a combination of both.

**National Security**—the national defense or foreign relations of the United States.

**Need—To-Know—**a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

**Network**—a system of two or more computers that can exchange data or information.

**Original Classification**—an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

**Original Classification Authority (OCA)**—an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

**Records**—the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

**Records Having Permanent Historical Value**—Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently IAW Title 44, United States Code.

**Records Management**—the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

**Restricted Data (RD**—defined by the Atomic Energy Act as all data concerning design, manufacture, or utilization of atomic weapons, production of special nuclear material, and use of Special Nuclear Material in the production of energy.

**Safeguarding**—measures and controls that are prescribed to protect classified information.

**Self—Inspection—**the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

**Sensitive But Unclassified (SBU) Information**—information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA.

**Source Document**—an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

**Special Access Program (SAP)—**a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

**Staff Agency Chief**—For the purpose of this instruction, staff agency chiefs are those individuals serving in 2-digit positions reporting to the commander or vice commander above the Wing level, and 2 and 3 digit positions at HAF.

**Systematic Declassification Review**—the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value IAW title 44, United States Code.

**Telecommunications**—the preparation, transmission, or communication of information by electronic means.

**Unauthorized Disclosure**—a communication or physical transfer of classified information to an unauthorized recipient.

**Violation**—(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or (3) any knowing, willful, or negligent action to create or continue a SAP contrary to the requirements of this order.

## Attachment 2

## CONTROLLED UNCLASSIFIED INFORMATION

**A2.1. For Official Use Only (FOUO).** FOUO is a designation that is applied to unclassified information that is exempt from automatic release to the public under FOIA. See DOD 5400.7-R/AF Supplement for further guidance *[Ref: DOD 5200.1-R, Appendix 3, Para AP3.2.]*.

A2.1.1. Access to FOUO Information.

A2.1.1.1. No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.

A2.1.1.2. The final responsibility for determining whether an individual has a valid need for access to information designated as FOUO rests with the individual who has authorized possession, knowledge or control of the information and not on the prospective recipient.

A2.1.1.3. Information designated as FOUO may be disseminated within the DOD Components and between officials of DOD Components and DOD contractors, consultants, and grantees to conduct official business for the DOD, provided that dissemination is not further controlled by a Distribution Statement.

A2.1.1.4. DOD holders of information designated as FOUO are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a government function. If the information is covered by the Privacy Act, disclosure is only authorized if the requirements of AFI 33-332, Air Force Privacy Program, are satisfied.

A2.1.1.5. Release of FOUO information to Congress is governed by AFI 90-401, *Air Force Relations With Congress*. If the Privacy Act covers the information, disclosure is authorized if the requirements of DOD 5400.11-R are also satisfied.

A2.1.1.6. DOD Directive 7650.01, *General Accounting Office (GAO) and Comptroller General Access to Records*, governs release of FOUO information to the Government Accountability Office (GAO). If the Privacy Act covers the information, disclosure is authorized if the requirements of DOD 5400.11-R are also satisfied.

A2.1.2. Protection of FOUO Information.

A2.1.2.1. During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, store FOUO information in unlocked containers, desks or cabinets if Government or Government-contract building security is provided. If such building security is not provided, store the information in locked desks, file cabinets, bookcases, locked rooms, etc.

A2.1.2.2. FOUO information and material may be transmitted via first class mail, parcel post or, for bulk shipments, via fourth-class mail. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, shall be by approved secure communications systems or systems utilizing access controls such as Public Key Infrastructure (PKI), whenever practical.

A2.1.2.3. FOUO information may only be posted to DOD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum, dated 25 November 1998, Subject: "*Web Site Administration*".

A2.1.2.4. Record copies of FOUO documents shall be disposed of according to the Federal Records Act and the DOD Component records management directives. Non-record FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information.

A2.1.3. Unauthorized Disclosure. The unauthorized disclosure of FOUO does not constitute an unauthorized disclosure of DOD information classified for security purposes. However, appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DOD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

**A2.2. FOR OFFICIAL USE ONLY Law Enforcement Sensitive.**

A2.2.1. Law Enforcement Sensitive is a marking sometimes applied, in addition to/conjunction with the marking FOR OFFICIAL USE ONLY, by the Department of Justice and other activities in the law enforcement community. It is intended to denote that the information was compiled for law enforcement purposes and should be afforded appropriate security in order to protect certain legitimate government interests, including the protection of: enforcement proceedings; the right of a person to a fair trial or an impartial adjudication; grand jury information; personal privacy including records about individuals requiring protection under the Privacy Act; the identity of a confidential source, including a State, Local, or foreign agency or authority or any private institution which furnished information on a confidential basis; information furnished by a confidential source; proprietary information; techniques and procedures for law enforcement investigations or prosecutions; guidelines for law enforcement investigations when disclosure of such guidelines could reasonably be expected to risk circumvention of the law, or jeopardize the life or physical safety of any individual, including the lives and safety of law enforcement personnel.

A2.2.2. Markings.

A2.2.2.1. In unclassified documents containing Law Enforcement Sensitive information, the words "Law Enforcement Sensitive" shall accompany the words "FOR OFFICIAL USE ONLY" at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

A2.2.2.2. In unclassified documents, each page containing FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" at the top and bottom. Classified documents containing such information shall be marked as required by Chapter 5, DOD 5200.1-R except that pages containing Law Enforcement Sensitive information but no classified information will be marked "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" top and bottom.

A2.2.2.3. Portions of DOD classified or unclassified documents that contain FOR OFFICIAL USE ONLY Law Enforcement Sensitive information shall be marked "(FOUO-LES)" at the beginning of the portion. This applies to classified, as well as to unclassified documents. If a portion of a classified document contains both classified and FOR OFFICIAL USE ONLY Law Enforcement Sensitive information, the appropriate classification designation is sufficient to protect the information.

A2.2.3. Access to FOR OFFICIAL USE ONLY Law Enforcement Sensitive. The criteria for allowing access to FOR OFFICIAL USE ONLY Law Enforcement Sensitive are the same as those used for FOUO information, except that if the information also bears the marking "Originator Control" or "ORCON" the information may not be disseminated beyond the original distribution without the approval of the originating office.

A2.2.4. Protection of FOR OFFICIAL USE ONLY Law Enforcement Sensitive. Within the DOD, FOR OFFICIAL USE ONLY Law Enforcement Sensitive shall be protected as required for FOUO information.

**A2.3. Sensitive But Unclassified (SBU) Information.** SBU information is information originated within the Department of State that warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under FOIA. When SBU information is included in DOD documents, it shall be marked as if the information were FOUO *[Ref: DOD 5200.1-R, Appendix 3, Para AP3.3.]*.

**A2.4. Protection of Drug Enforcement Administration (DEA) Sensitive Information.** Unclassified information that is originated by the DEA and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports *[Reference DOD 5200.1-R, Appendix 3, Para AP3.4.]*.

**A2.5. Unclassified Controlled Nuclear Information (UCNI).** Unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of Special Nuclear Material equipment or facilities *[Reference DOD 5200.1-R, Appendix 3, Para AP3.5.]*.

A2.5.1. The Director of Information Protection (SAF/AAP) has primary responsibility within the Air Force for the implementation of DODD 5210.83, *Department of Defense Unclassified Controlled Nuclear Information* (DOD UCNI).

A2.5.2. The following positions have been designated UCNI Officials within the Air Force:

A2.5.2.1. HAF staff agency chiefs.

A2.5.2.2. MAJCOM/FOA/DRU commanders, Chiefs of IP.

A2.5.2.3. Installation commanders and equivalent commander positions, Chiefs of IP.

A2.5.2.4. **(DELETED)**

A2.5.3. UCNI Officials' Responsibilities:

A2.5.3.1. Identify information meeting definition of UCNI.

A2.5.3.2. Determine criteria for access to UCNI and approve special access requests.

A2.5.3.3. Approve or deny the release of UCNI information.

A2.5.3.4. Ensure all UCNI information is properly marked, safeguarded, transmitted, and destroyed properly. Transmission of UCNI on the NIPRNet may only occur when the material is encrypted and digitally signed and the recipient has a ".mil" or ".gov" address extension.

A2.5.3.5. Document decisions and report them through their command IP channels to SAF/AAP. RCS Number DD-C3I(AR)1810 applies to this data collection.

**A2.6. Sensitive Information (Computer Security Act of 1987).** *The Computer Security Act of 1987* established requirements for protection of certain information in Federal Government AIS. It applies only to unclassified information that deserves protection and is concerned with protecting the availability and integrity, as well as the confidentiality, of information. See AFI 33-200 for Air Force policy on protecting information in Federal Government information systems *[Reference DOD 5200.1-R, Appendix 3, Para AP3.6.]*.

**A2.7. Technical Documents.** DOD Directive 5230.24 requires distribution statements to be placed on technical documents, both classified and unclassified. These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. See AFI 61-204 for Air Force policy on technical documents *[Reference DOD 5200.1-R, Appendix 3, Para AP3.7.]*.

**A2.8. LIMITED DISTRIBUTION Information**

A2.8.1. Description. LIMITED DISTRIBUTION is a caveat used by the National Imagery and Mapping Agency/National Geospatial-Intelligence Agency (NIMA/NGA) to identify a select group of sensitive but unclassified imagery or geospatial information and data created or distributed by NIMA/NGA or information, data, and products derived from such information. DOD Instruction 5030.59, *NATIONAL GEOSPATIAL- INTELLIGENCE AGENCY (NGA) LIMITED DISTRIBUTION GEOSPATIAL INTELLIGENCE*, contains details of policies and procedures regarding use of the LIMITED DISTRIBUTION caveat. These policies and procedures are summarized in **subparagraphs A2.8.2** through **A2.8.4**, below.

A2.8.2. Marking. Information or material designated as LIMITED DISTRIBUTION, or derived from such information or material shall, unless otherwise approved by the Director, NGA be marked with the notation shown in Figure A2.F1 as follows:

LIMITED DISTRIBUTION Notation

UNCLASSIFIED/LIMITED DISTRIBUTION

Distribution authorized to DOD, IAW 10 U.S.C. § 130 and 455. Release authorized to U.S. DOD Contractors IAW 48 C.F.R. §252.245-7000. Refer other requests to Headquarters, NGA, ATTN: Release Officer, Stop D-136. Destroy as "For Official Use Only." Removal of this caveat is prohibited.

A2.8.3. Access to LIMITED DISTRIBUTION Information or Material.

A2.8.3.1. Information bearing the LIMITED DISTRIBUTION caveat shall be disseminated by NGA to Military Departments or other DOD Components, and to authorized grantees for the conduct of official DOD business.

A2.8.3.2. DOD civilian, military and contractor personnel of a recipient DOD Component, contractor or grantee may be granted access to information bearing the LIMITED DISTRIBUTION caveat provided they have been determined to have a valid need to know for such information in connection with the accomplishment of official business for the DoD. Recipients shall be made aware of the status of such information, and transmission shall be by means to preclude unauthorized disclosure or release. Further dissemination of information bearing the LIMITED DISTRIBUTION caveat by receiving contractors or grantees to another Military Department, other DOD Component, contractor or grantee, or dissemination by any recipient Component, contractor, or grantee to any person, agency or activity outside DOD, requires the express written approval of the Director, NGA.

A2.8.3.3. Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be released, made accessible to or sold to foreign governments or international organizations, to include through Foreign Security Assistance transactions or arrangements, or transfer or loan of any weapon or weapon system that uses such information, or intended to be used in mission planning systems, or through the Foreign Military Sales (FMS) process, without the express, written approval of the Director, NGA.

A2.8.3.4. All FOIA requests for information bearing the LIMITED DISTRIBUTION caveat or derived there from, shall be referred to NGA consistent with DOD Instruction 5030.59.

A2.8.4. Protection of LIMITED DISTRIBUTION Information.

A2.8.4.1. Information bearing the LIMITED DISTRIBUTION caveat, or derivative information, shall not be stored on systems accessible by contractors, individuals who are not directly working on a DOD contract, or those who do not require access to such information in connection with the conduct of official DoD business.

A2.8.4.2. LIMITED DISTRIBUTION information or derivative information, may only be posted to DOD Web sites consistent with security and access requirements specified in Deputy Secretary of Defense Memorandum dated December 1998. Such information shall not be transmitted over the World Wide Web or over other publicly accessible and unsecured systems. Electronic transmission of such information, e.g., voice, data or facsimile, shall be by approved secure communications systems or systems utilizing other protective measures such as PKI.

A2.8.4.3. During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, LIMITED DISTRIBUTION information may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided. If such building security is not provided, LIMITED DISTRIBUTION information shall be stored in locked buildings, rooms, desks, file cabinets, bookcases, or similar items. Store LIMITED DISTRIBUTION information in the same manner approved for FOUO.

A2.8.4.4. When no longer required, all LIMITED DISTRIBUTION information and copies, shall be returned to NIMA/NGA or destroyed in a manner sufficient to prevent its reconstruction.

## Attachment 3

## PHYSICAL SECURITY STANDARDS

**A3.1. Intrusion Detection Systems (IDS) Standards.** *[Reference DOD 5200.1-R, Appendix 7, AP7.2.]*

A3.1.1. Air Force IDS Standards. See AFI 31-101, *Air Force Installation Security Program*, Chapter 12, for Air Force policy on IDS.

A3.1.2. Trustworthiness Determinations. See AFI 31-501 for Air Force policy on trustworthiness determinations.

**A3.2. Physical Security Design Guidelines.** See the Military Handbook Design Guidelines for Physical Security of Facilities (MIL-HDBK-1013/1A) at **http://assist.daps.dla.mil/docimages/0000/57/10/54120.PD2** for facility design standards. DOD 5200.1-R, Appendix 7 provides vault and secure room construction standards.

A3.2.1. The ISPM certifies vaults and secure rooms in concert with appropriate engineering and communications technical representatives IAW DOD 5200.1-R, Appendix 7.

A3.2.2. Commander, equivalent, or staff agency chief approves open storage.

A3.2.3. Defense Intelligence Agency (DIA) standards for Sensitive Compartmented Information Facilities (SCIF) are included in Director Central Intelligence Agency Directive 6/9.

## Attachment 4

## TRANSMISSION TO FOREIGN GOVERNMENTS

**A4.1. General.** Comply with provisions of DOD 5200.1-R, Appendix 8 for movement of classified information or material to foreign governments. Air Force contracting officials ensure that US industrial activities have a government approved transportation plan or other transmission instructions.

A4.1.1. Receipts. Air Force personnel: *[Reference DOD 5200.1-R, Appendix 8, Paragraph a]*

A4.1.2. Use AF Form 349, Receipt for Documents Released to Accredited Representatives of Foreign Nations (available on the AFEPL);

A4.1.3. 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,

A4.1.4. **(DELETED)**

**A4.2.** Whenever possible, shippers should use military airlift for shipping classified to foreign recipients. ***NOTE:*** When Air Mobility Command airlift cannot deliver, determine an alternate secure method of direct delivery to a designated representative on a case-by-case basis *[Reference DOD 5200.1-R, AP8.1.1.3.]*

**A4.3.** 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.

**A4.4.** See AFPD 24-2 and AFI 24-201 for instructions on "Report of Shipment."

**A4.5. Foreign Military Sales (FMS).** Air Force activities having primary management responsibility for processing FMS cases ensure that personnel include transmission instructions *[Reference DOD 5200.1-R, AP8.1.1.3.4.]*

A4.5.1. FMS processors must coordinate with ISPMs/IP and transportation officials on transportation plans submitted by foreign purchasers before giving final approval.

## Attachment 5

## APPOINTMENT OF INQUIRY OFFICIAL MEMORANDUM

**DEPARTMENT OF THE AIR FORCE**

**AIR FORCE UNIT HEADING**

MEMORANUM 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 as either a security violation or a 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 potential 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 of Commander, Staff Agency Chief, or equivalent)

## Attachment 6

## 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 Management*, **paragraph 9.5.**, for security classification requirements.

Personnel Interviewed: (list all personnel interviewed, 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, potential compromise or no compromise; and, if this inquiry should be closed without further investigation or with a recommendation for a formal investigation).

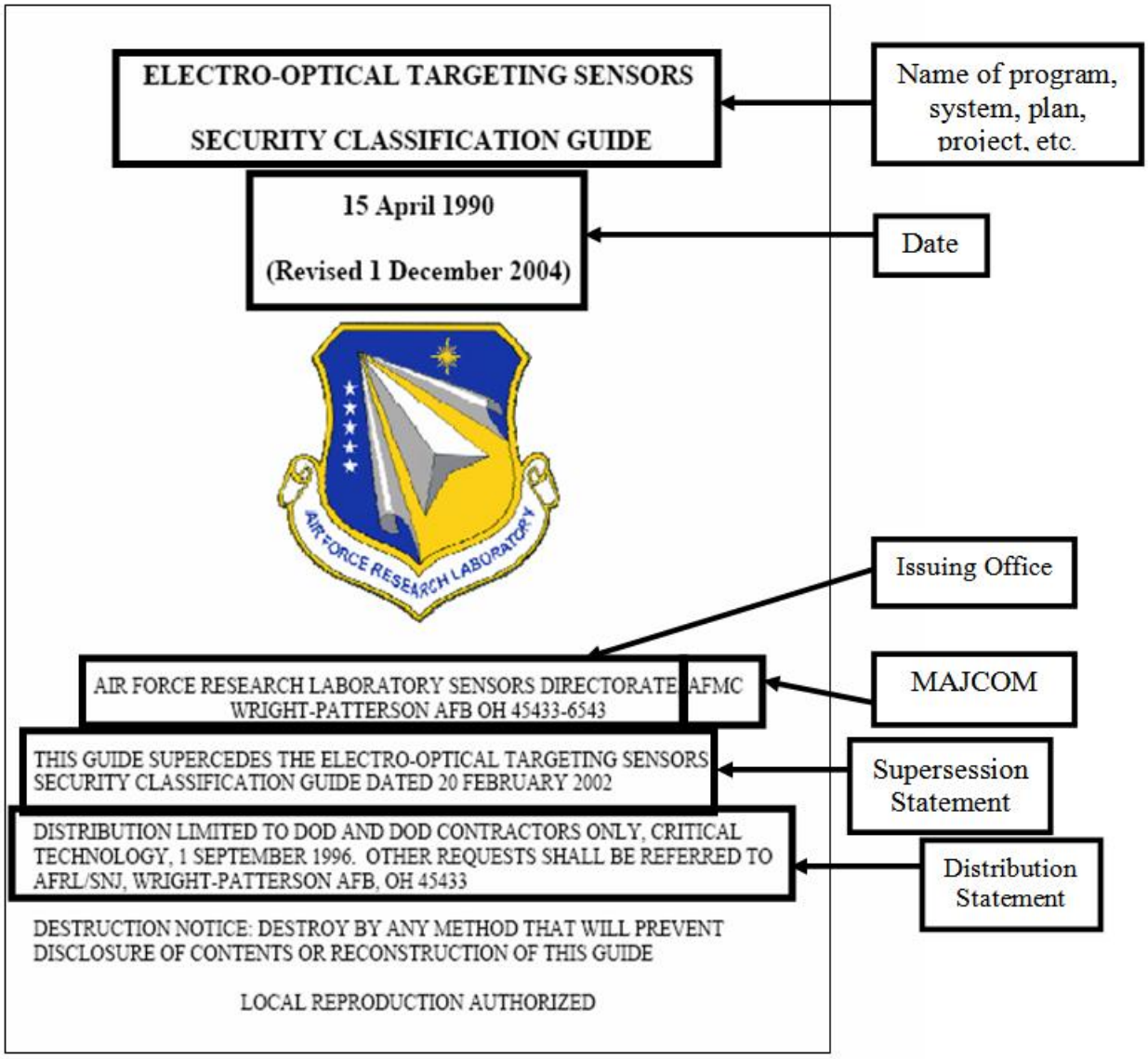
(Signature block of inquiry official)

Attachment:
Appointment of Inquiry Official Memo, (date)

## Attachment 7

## FORMAT FOR CLASSIFICATION/DECLASSIFICATION GUIDE

### A7.1. Front page format:



## SECTION 1

**A7.2.** General Instructions (Minimum Required Items Are Circled)

**FOREWORD**

**DESCRIPTION:** The AN/AAQ-26 Infrared Detecting Set (IDS) enables an observer in an aircraft to view patterns of heat emissions (infrared radiation) from a target area concealed by darkness or camouflage. The AN/AAQ-26 IDS consists of four major components: Infrared Receiver, LRU 1; Control Converter, LRU 2; Gimbal Position Control, LRU 3; and the Infrared Set Control, LRU 4.

**Coordinated by:**

CHRISTOPHER C. BOGDAN, Col, USAF
Director, Special Operations Forces
System Program Office

**Approved by:**

OCA

WILLIAM R. ROONEY III
Lieutenant General, USAF
Commander

General Instructions Continued:

**SECTION I**

**GENERAL INSTRUCTIONS**

1. **Purpose.** This guide provides a basis for evaluating the degree of protection necessary for documentation, photographs, equipment, material, and information applicable to the AN/AAQ-26 IDS.

2. **Authority.** DoD 5200.1-R/AFI 31-401. Cite this guide as the basis for classifying, downgrading, or declassifying information about the AN/AAQ-26 IDS.

3. **Office of Primary Responsibility (OPR).** This guide is issued by ASC/LU, 1895 5th Street, Bldg 46, Wright-Patterson AFB OH 45433-7200, telephone COM (937) 255-4152/DSN 785-4152. Address all inquiries concerning content and interpretation to 88 SFS/SFA, 1801 Tenth Street, Room 103, Wright-Patterson AFB OH 45433-7625.

4. **Classification Recommendations.** Send completely documented and justified recommendations through 88 SFS/SFA, to the OPR if the security classifications or declassification instructions in this guide impose impractical requirements or when scientific or technological changes in the state of the art indicate a need for changes. Pending final decision, handle and protect the information at the highest of the present or the recommended classifications. All users of this guide are encouraged to assist in improving and maintaining the currency and adequacy of this guide.

5. **Classification Currency.** Changes to this guide will be affected by the issuance of a letter, Subject: Letter Change No. _____ to the AN/AAQ-26 IDS Security Classification Guide (SCG), 30 December 2004. This letter will indicate the appropriate change(s) and will constitute the authority for such change(s). Upon receipt of a letter change, the appropriate change(s) will be made and the letter of authority will be inserted in back of the guide.

6. **Reason for Classifying.** The reasons for classifying information are in accordance with Executive Order (EO) 12958, as amended by EO 13292. The categories for classification, as identified throughout the guide, are as follows:

Category 1.4g: Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security, which includes defense against and transnational terrorism.

7. **Explanation of Declassification Instructions.** Choose one of the following four declassification instructions, selecting, whenever possible, the declassification instruction that will result in the shortest duration of classification.

a. A date or event less than 10 years, or if unable to identify such a date or event;

b. a date 10 years from the date of the document; or

General Instructions Continued:

c. a date greater than 10 and less than 25 years from the date of the document; or

d. a date 25 years from the date of the document.

When determining the duration of classification, the Original Classification Authority should consider the four options listed above sequentially; first, consider the least amount of time that information needs to be classified, that is, a time frame that is less than 10 years; if unable to determine a date or event of less than 10 years then 10 years; third, between 10 years and up to 25 years based upon the sensitivity of the information as determined by the Original Classification Authority; and then finally, 25 years from the date of the decision.

All originally classified documents must contain a date or event of 25 years or less on the "Declassify on" line.

**8. Prior Declassification Instructions.** To comply with EO 12958, as amended by EO 13292, previously classified information with a declassification instruction of Originating Agency Determination Required (OADR) or X1 through X8 must be readdressed and now have a declassification date or event as identified in section 7 above. **NOTE**: The declassification date or event cannot exceed 25 years from the **original** classification date (the date the information was first classified).

**9. Other Applicable Security Classification Guides.** Refer to aircraft Security Classification Guides for aircraft/mission specific information.

**10. Application, Reproduction, and Dissemination.** Specified groups involved in the AN/AAQ-26 IDS program, including industrial activities, may make reproductions and extracts or selections of portions of this guide.

**11. Manufacture, Test, and Assembly.** During manufacture, test, or assembly processes, the classification as assigned by this guide shall apply at the earliest point where design, performance, or other classified characteristics can be derived and traced to the system(s) identified herein.

**12. Disassembly and Repair.** During disassembly and repair, the classification assigned by this guide no longer applies at the earliest point where design, performance, or other classified characteristics can no longer be derived from or traced to the system(s) identified herein.

**13. Technology Transfer.** A major goal of DoD classification policy is to deny our adversaries access to documents, hardware, and technologies that will accelerate their military programs and simultaneously cause an increase in our defense efforts and costs. During development of a system, numerous areas of advanced technology may be exploited. It is the intent of this guide to safeguard the following information:

**A7.3.** Release Information:

1. **Public Release of Official Information.** Although this guide shows certain details of information as unclassified, it does not permit automatic public release. Unclassified, unlimited distribution information proposed for public release about the AC-130U Gunship must be submitted to Aeronautical Systems Center Public Affairs; ATTN: Security and Policy Review (ASC/PA); Building 14, Room 240; 1865 4th Street; Wright-Patterson AFB OH 45433-7129, Telephone (937) 255-3334.

2. **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. If there are any doubts, do not release the information!

3. **Release of Classified and Unclassified Information to Foreign Governments or Their Representatives.** In accordance with AFI 16-201, Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations (C), advise a foreign national soliciting or requesting classified and/or unclassified USAF information to request it through their embassy in Washington DC. Any military activity or contractor receiving such a request from a foreign government, foreign contractor, or representative thereof must forward the request to ASC/XPD, 1865 4th St, Wright-Patterson AFB OH 45433-7127. Any military activity desiring to release classified and/or unclassified information to a foreign government, foreign contractor, or representative thereof, must forward the request to ASC/XPD according to AFI 16-201. Defense contractors desiring to release classified and/or unclassified information controlled by the International Traffic in Arms Regulation (ITAR) to a foreign government, foreign contractor, or representative thereof must request a munitions export license from: Department of State, Office of Defense Trade Control, PM/DTC Room 200, SA-6, Washington DC 20522.

**A7.4.** Classification and Declassification Information:

| Element of Information | Classification of Element | Reason for Classification | Declassification or Downgrading Instructions |
|---|---|---|---|

| INFORMATION REVEALING | CLASS/ REASON | DECLAS DATE OR EVENT | REMARKS |
|---|---|---|---|
| m. LOS pointing accuracy | U | | |
| n. Tracker capability when minimum trackable target characteristics are revealed | S/1.4g | 31 Jan 2030 | UNCLASSIFIED when characteristics are not revealed. |
| o. Reliability | U | | |
| p. Vulnerability to countermeasures and counter-countermeasures | S/1.4g | 31 Jan 2030 | |
| q. Counter-countermeasure capability | S/1.4g | 31 Jan 2030 | |
| r. Hardware | U | | |
| s. Software | U | | |
| t. Number of active detectors comprising the AN/AAQ-26 IDS detector assembly | U | | |

Element of Information | Classification of Element | Reason for Classification | Declassification or Downgrading Instructions

Include remarks as required

| INFORMATION REVEALING | CLAS/ REASON | DECLAS | REMARKS |
|---|---|---|---|
| 2. Multispectral/Multiband passive sensors - polarimetric and non-polarimetric | | | |
| a. Program Objective | U | | |
| b. Detector characteristics and figures of merit (size, D, D*, D**, QE, spectral response, frequency response, noise etc) | See Remarks | | Unclassified, Distribution D: Critical Technology applies. |
| c. Measured system-level figures of merit (area coverage, spatial resolution, spectral coverage, spectral resolution, noise level, polarimetric extinction ratio, FOR, FOS, FOV) | | | |
| (1) Laboratory sensor | U | | |
| (2) Flight-qualified sensor | S 1.4g | 1 Dec 2014 | |
| d. Predicted and measured operational performance (Pd, Pr, Pc, Pid, Pfa, ROC, Pt) vs range, atmospheric conditions, target type/signature, background and clutter level | S 1.4g | 1 Dec 2014 | |

TOPIC—Information revealing:

CLS DCL REASON

S 25X1 1.4(c) 1.4(e)

If any 25X markings are going to be used, they must be annotated in the Security Classification/Declassification Guide before they can be used on derivatively classified documents. AF/XOS-FI will process the guides through ISCAP for approval.

**A7.5.** DD Form 2024, DOD Security Classification Guide Data Elements:

**DOD SECURITY CLASSIFICATION GUIDE DATA ELEMENTS** | **REPORT CONTROL SYMBOL**

*See reverse side for purpose and additional completion instructions*

**1. REASON FOR SUBMISSION** *(X as applicable)*

| | a. NEW GUIDE | | b. REVISION | | c. REISSUANCE | | d. BIENNIAL REVIEW | | e. CANCELLATION | | f. CORRECTION |
|---|---|---|---|---|---|---|---|---|---|---|---|

**2. PROMULGATING DOCUMENT** *(Include type of document, activity, symbol or serial number and date. Do not include the subject of the document. If no promulgating document, state "None." Do not exceed 46 characters.)*

**3. CLASSIFICATION GUIDE TITLE** *(Include the full title (if unclassified) and any short title. Do not exceed 134 characters.)*

**4. CLASSIFICATION GUIDE DATE** *(YYMMDD) (Do not exceed 6 characters)*

**5. CLASSIFICATION GUIDE ORIGINATOR** *(Activity which issued guide. Do not exceed 25 characters.)*

Include office symbol and MAJCOM

**6. AVAILABLE THRU DTIC** *(X one)* *(See paragraph G of Instructions on reverse.)* Distribution Statement, Ref: AFI 61-204, Atch 2

| | B | | C | | D | | E | | F | | X | | NO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

**7. BIENNIAL REVIEW DATE** *(YYMMDD) (Do not exceed 6 characters)*

**8. NUMBER OF REVISIONS AND DATE OF LATEST** *(Show number of revisions first, then the date of latest revision (YYMMDD). If none, so state. A reissued guide would have no revisions. Do not exceed 8 characters.)*

**9. SUBJECT MATTER INDEX TERMS** *(Selection of these terms is critical to proper indexing of the classification guide. They should concisely describe what the classification guide pertains to. Each term may consist of one or more words. Each term may not exceed 34 characters. A total of three Subject Matter Index terms may be listed, each on its own line. The classification guide will appear in the index under each listed Subject Matter Index Term.)*

a. Examples: Aircraft, Weapons, Communications, Space, Nuclear, etc.

b.

c.

**10. CLASSIFICATION OF GUIDE** *(X as applicable to indicate classification status of the classification guide, that is, X the classification of the guide document. Write Special Access Required block if the guide itself requires such access, or X the fact that the guide document is unclassified.)*

| | TS | | S | | C | | U | | SPECIAL ACCESS REQUIRED |
|---|---|---|---|---|---|---|---|---|---|

**11. INDEX SOURCE NUMBER** *(Enter existing number if guide is listed in index.)*

**12. The highest classification prescribed by the guide is** *(X as applicable, that is, X the highest classification that the guide states is to be applied to information by users of the guide.)*

| | TS | | S | | C |
|---|---|---|---|---|---|

**13. The guide prescribes classification of information controlled within a Special Access Program** *(X one, that is, X YES if the guide states that information classified pursuant to it requires Special Access Program protection or X NO if this is not the case.)*

| | a. YES | | b. NO |
|---|---|---|---|

**14. REMARKS**

As required

**15. ORIGINATOR**

| a. TYPED NAME | b. TITLE | e. DATE SIGNED |
|---|---|---|
| | | |

| c. OFFICE/AGENCY/DEPARTMENT | d. SIGNATURE |
|---|---|
| | |

**16. ACTION OFFICER**

| a. NAME | b. TELEPHONE NO. *(AUTOVON if outside DC Metropolitan area.)* |
|---|---|
| | |

DD Form 2024, JUL 86 (EG) *Previous editions are obsolete.* Designed using Perform Pro, WHS/DIOR, Mar 95

**All circled items are required to be filled in.**