*BY ORDER OF THE COMMANDER*
*AVIANO AIR BASE (USAFE)*

*AIR FORCE INSTRUCTION*

*16-1404*

*AVIANO AIR BASE*
*Supplement*

*16 NOVEMBER 2021*

*Operations Support*

# *AIR FORCE INFORMATION SECURITY PROGRAM*

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

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

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

---

OPR: 31 FW/IP

Certified by: 31 FW/CV
(Col Vincent J. O'Connor)

Pages: 12

---

This Aviano Air Base supplement implements and extends the guidance of AFI 16-1404, *Air Force Information Security Program*, 29 May 2015, as follows: This supplement outlines specific procedures to accomplish in order to protect classified information and controlled unclassified information (CUI) developed by or in the possession of the Air Force. It applies to all personnel on Aviano Air Base, including tenant units and geographically separated units who require 31 FW information security oversight. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, Publications and Forms Management, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

1.3.3. **(Added)** Oversight of Information Protection for Aviano AB is delegated to 31 FW/CV.

1.6. **(Added) Air Force Information Security.** Is a core security discipline within Information Protection that is designed to identify and protect classified national security information and CUI in accordance with DoD policy issuances. DoDM 5200.01, Volumes 1-3, DoDI 5210.02, DoDD 5210.50, DoDI 5210.83, and DoDM 5200.45 provide the foundational guidance and this AFI clarifies responsibilities within these DoD governances where needed.

1.6.1. **(Added)** The Air Force standard guidance for marking collateral classified information is DoDM 5200.01, Volume 2, *Marking of Classified Information*. Personnel assigned to Special Access Program (SAP) and Sensitive Compartment Information (SCI) will follow additional guidance as mandated by their security officials. The standard for marking CUI (e.g., For Official Use Only (FOUO)) is DoDM 5200.48.

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

2.4.2.1. **(Added)** 31 MSG/CC will appoint a primary and least one alternate as NATO Sub-Registry officials. (T-3)

2.4.2.2. **(Added)** Unit Commanders will appoint a NATO Control Point Officer and at least one alternate based upon NATO Sub-registry recommendations to meet NATO requirements. (T-0)

2.4.4. **(Added)** The second week in February is annual clean-out week. (T-0) Review all classified records and holdings for retention or destruction. Before destroying any classified records, check with the Wing History Office for possible retention of records of historical value. Use a Memorandum for Record (MFR) to document the review and destruction of the organization's materiel. File a copy of the annual clean-out memorandum in the unit folder on the 31 FW Information Protection SharePoint site or other approved location. (T-3)

2.4.7. **(Added)** The authority to approve/recertify open storage rooms/areas is delegated to the Chief, Information Protection (CIP). (T-3)

2.5.5.1. **(Added)** Emergency protection, storage, destruction, or relocation of classified material will be done by personnel IAW the unit's Emergency Protection Plans (EAP) for the vaults, security containers, or secure rooms, which hold the classified material. The emergency action plan as a minimum will consist of actions taken during non-hostile (fire, bomb threat, etc.) and hostile emergencies (refer to Wing Contingency Plans). (T-0)

2.5.5.1.1. **(Added)** The EAPs will be clearly identified and posted inside each security container, secure room or vault door containing classified material.

2.5.5.2.1. **(Added)** Unit Commanders shall identify and publish specific security measures and train personnel based on the assets and facilities under their control. (T-0) Authorized personnel who permit another individual to access classified information or enter the area are responsible for confirming their need to know and access eligibility. (T-0)

2.5.5.2.2. **(Added)** Persons requiring facility access without the appropriate level of clearance and/or need to know shall be escorted at all times within the facility by a cleared person who is familiar with the security procedures of the facility. (T-0)

2.5.5.3. **(Added)** The 31st FW, Command Post, will provide temporary classified storage up to "Secret and NATO Secret" and issue a receipt using the AF Form 1297, Temporary Issue Receipt,

for classified material received from personnel arriving unexpectedly or in-transit. (T-3) Personnel who require temporary classified storage should request it in advance of arrival if possible.

2.5.8.4. **(Added)** 31 FW/IP will conduct a security survey, with assistance from 31 CES and 31 SFS if needed, to ensure all security requirements are met. (T-1) Once the room or area security survey is complete and meets the requirements, CIP will endorse the request and attach the survey to the request.

2.5.8.5. **(Added)** Once CIP approves the request, 31 FW/IP will retain a copy of the package and forward the approval package to the commander and security manager (SM) for record. The approval letter will be placed on the inside of the door to the area or immediately adjacent if necessary inside the room. (T-3)

2.7.1. **(Added)** Appoint (in writing) a primary and at least one alternate SM. To ensure program success and continuity, it is recommended that personnel appointed have one year of retainability. (T-3)

2.7.2. **(Added)** Grant personnel access to classified information and continually evaluate their trustworthiness in accordance with DoDM 5200.01, Volume 1, Enclosure 2, and DoDM 5200.02_AFMAN16-1405, 1 August 2018. (T-0) This may not be delegated. (T-0) Ensure all collateral access is reflected in the security access requirement (SAR) level shown on the unit manning document. Consider suspension of an individual's access whenever their trustworthiness, loyalty, or honesty becomes questionable in accordance with AFI 31-501 (CHANGING TO AFI 16-1405). (T-1)

2.7.4. **(Added)** Identify unit personnel whose duties require derivative classification and provide 31 FW/IP an electronic master listing. Maintain a current copy in the unit folder on the 31 FW Information Protection SharePoint site or other approved location designated by 31 FW/IP. (T-3)

2.7.7. **(Added)** Unit security plan/instruction will be reviewed by 31 FW/IP. (T-3)

2.7.10. **(Added)** The unit commander will sign a memorandum approving all equipment used for reproducing classified material. Place the original memorandum on or near the equipment. The SM will ensure reproduction rules and locally produced visual aids "*Approved for Classified Reproduction"* are posted in close proximity of the approved equipment. Include procedures in unit OI. File a copy of the approval memorandum in the unit folder on the 31 FW Information Protection SharePoint site or other approved location designated by 31 FW/IP.

2.7.12. **(Added)** Unit commanders will submit written requests to include justification for open storage rooms/areas/vault to the CIP. (T-3)

2.7.13.3. **(Added)** Units hosting classified meetings are responsible for ensuring appropriate security measures are in place to properly control access and protect national security information. For classified meetings, conferences and symposiums, the host unit submits a security plan to 31 FW/IP a minimum of ten (10) days prior.

2.7.13.4. **(Added)** Activities hosting classified meetings or forums will coordinate their security procedures with 31 FW/IP. As a minimum, procedures should contain the meeting title, its location, purpose, classification level (if permitted), identity of the responsible point of contact and a statement of who (organization or title) approved the meeting. Also, the plan must address clearance verification procedures prior to attendee arrival, an assessment of security controls required during the meeting (e.g. perimeter guards), access controls at the meeting entry point,

policy on introducing and utilization of electronic or photographic devices in the meeting room, storage of classified materials (exhibits/documents) before, during and after the meeting, policy/procedures for note-taking during classified portions of the meeting and communications/ destruction/transmission procedures for those requiring these services during or after the meeting. The plan is not limited to these areas alone; additional requirements are determined locally. The plan is not necessary for meetings held in a conference facility/room approved by the units or IP, nor does it apply to routine or ad-hoc discussions between individuals. (T-2)

2.7.13.5. **(Added)** Foreign participation in classified or unclassified meetings and conferences can take place only after approval from the servicing Foreign Disclosure Office (FDO).

2.7.16. **(Added)** Identify the location of all security containers within the unit by memorandum and provide 31 FW/IP an electronic master listing of all unit security containers, secure rooms/vaults. File a copy of the memorandum in the unit folder on the 31 FW Information Protection SharePoint site or other approved location designated by 31 FW/IP. (T-3)

2.7.17. **(Added)** Commanders will notify the CIP when a room or area is no longer required for open storage. The CIP will accomplish a decertification letter and forward it to the unit commander. Once decertified, the CIP will notify the SM and 31 SFS.

2.7.18. **(Added)** Commanders will notify 31 FW/IP prior to any modifications or construction to existing open storage areas to assess any impacts to security requirements. (T-3)

2.8.1. **(Added)** SM will complete all required training NLT 90 days after they are appointed by the commander. (T-3)

2.8.2. **(Added)** Assistant SM will complete all required training NLT 90 days after they are appointed by the commander. (T-3)

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

2.8.7. **(Added)** SM will file all memorandums and documents required by 31 FW/IP on the 31 FW Information Protection SharePoint site or other approved location designated by 31 FW/IP. (T-3)

4.2. **(Added) Controlled Unclassified Information (CUI).** Certain types of unclassified information require markings. Such information is referred to as CUI. DoDM 5200.48 provides guidance on the various types of CUI and their associated markings. Any person having questions as to whether a marking is CUI should contact their Security Manager or Wing Information Protection Office for additional guidance.

4.2.1. **(Added)** The originator of a document is responsible for determining at origination whether the information may qualify for one of the CUI statuses identified in DoDM 5200.48. (T-0)

4.2.2. **(Added)** It is the responsibility of the originator when marking FOUO to determine which FOIA exemptions applies. (T-0) It is recommended the exemption number(s) be annotated at the end of the sentence or paragraph it applies to facilitate review and requests for public release in the future. Refer to DoDI 5200.48 for specific definitions of the exemptions

4.2.3. **(Added)**

4.2.3. All CUI documents, information technology, other electronic media, blueprints, engineering drawing, charts, maps, photographic media, sound recordings, microfilm, microfiche, and similar microform media, **not** contained in a classified document, will be marked in accordance with DoDI 5200.48. (T-0)

5.1. **(Added)** Safeguarding. All Air Force personnel who work with classified information or CUI are personally responsible for taking proper precautions to ensure unauthorized persons do not gain access to classified information and CUI. (T-1) Only methods identified in DoDM 5200.01, Volumes 3 and DoDI 5200.48 may be used to store classified information and CUI when it is not under the personal observation and control of an authorized individual.

5.1.1.1.2. **(Added)** A signed Standard Form (SF) 312, "*Classified Information Non-Disclosure Agreement*" (NDA). (T-0) If the individual refuses to sign an NDA deny access to classified information (T-0) and initiate a Security Information File in accordance with DoDM 5200.02_AFMAN 16-1405, 1 August 2018. (T-1) Contact the local civilian human resources office or military personnel office for instructions on how to process the form for retention in personnel records.

5.1.1.2. **(Added)** IAW DoDM 5200.02_AFMAN 16-1405, 1 August 2018, The commander may utilize (optional) Air Force Form 2583, Request for Personnel Security Action, to document and identify investigation, security clearance and special access program authorization. If used, sign the AF Form 2583 Block 26. (T-1) Once access is granted the security manager will:

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

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

5.1.1.3.2. **(Added)** Establish an Incident Report IAW DoDM 5200.02_AFMAN 16-1405, 1 August 2018 if necessary. (T-1)

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

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

5.2.5. **(Added)** Commander will identify by memorandum all approved classified shredders within the unit. The memorandum will indicate make, model, serial number and location of the shredder. Post a locally produced visual aid "Authorized for Destruction of Classified Information" or Standard Form 707, Secret (label) on the shredder. A copy of the memorandum will be posted on the outside or inside of the shredder door and file a copy in the unit folder on the 31 FW Information Protection SharePoint site or other approved location designated by 31 FW/IP. (T-3)

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

5.3.2.2. **(Added)** Documentation. Use a courier authorization letter or DD Form 2501, Courier Authorization, when hand-carrying classified within the local area (on base and off base) when the courier is required to pass through an installation or facility checkpoint. A courier must carry an authorization letter when traveling outside the local area or aboard commercial passenger aircraft. Refer to specific guidance in DoDM 5200.01, Volume 3, Enclosure 4.

5.3.2.2.1. **(Added)** Each individual hand carrying classified material will receive a briefing and training from the SM. The individual will read and sign the Classified Material Courier Briefing. The SM will maintain a copy of the signed briefing memo until no longer needed. (T-3)

6.2.1.1. **(Added)** Unit security managers are responsible for developing organizational specific security training, as necessary. 31 FW/IP will approve all organizational specific IP security training. (T-3)

6.2.2.1. **(Added)** Individual must provide SM copies of training record showing completion of derivative classification training. (T-3)

6.2.2.2. **(Added)** Derivative classification training will be documented locally by the security manager for all approved unit derivative classifiers. (T-3)

6.4. **(Added)** Recommend quarterly or semi-annual sessions for maximum motivational and retentive effect. Documentation methodology must allow tracking of the training to determine date of training, subject areas covered, identity of attendees and percentage of assigned personnel trained. Procedures must be in place to identify and provide timely make-up for those missing regularly scheduled training. SMs will document training for all unit personnel (Contractors, DOD Civ, Mil) and maintain (on file) a consolidated list. (T-2)

6.7.2. **(Added)** SM will complete all required training NLT 90 days after they are appointed by the commander. (T-3)

6.7.3. **(Added)** Assistant SM will complete all required training NLT 90 days after they are appointed by the commander. (T-3)

7.3.1. **(Added)** Inquiry Officials. Commanders and Directors shall appoint an inquiry official, in writing within two duty days from the discovery of the security incident. (T-1) These individuals will not be less in rank or grade than the person(s) involved with the incident, the security manager, persons assigned to the Information Protection Office, or Director or Chief, Information Protection. (T-1) The individual must be cleared to the highest level of information involved or be given one-time access IAW DoDM 5200.02_AFMAN 16-1405, 1 August 2018. (T-1) The inquiry official shall:

7.3.1.1. **(Added)** CIP will conduct a technical review and attach it to the inquiry/investigation report prior to submitting the report to the appointing authority.

7.3.2.4. Consider establishing an Incident Report IAW DoDM 5200.02_AFMAN 16-1405, 1 August 2018, when it is determined the violation was a willful or negligent unauthorized disclosure involving information systems. (T-1) Contact the Wing Information Protection Office for guidance

before authorizing entries in JPAS/DISS to ensure accurate reporting. (T-1) Some entries are permanent and cannot be removed without DoD Central Adjudication Facility approval.

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

8.1.2. **(Added)** Additional requirements for DoD UCNI can be found in DoDI 5210.83, *DoD Unclassified Controlled Nuclear Information (UCNI)* and DoDI 5200.48. Mark UCNI material in accordance with DoDI 5200.48.

8.7. **(Added)** Access to RD. Commanders and Directors grant personnel access to RD information based on verification of final security eligibility, need-to-know, ensuring the individual receives an RD indoctrination briefing, has a signed SF 312. The Commander may also have the individual sign the AF Form 2583, if utilized. (T-1) Security Managers update the access in JPAS/DISS. (T-1)

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

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

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

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

8.8.5. **(Added)** Verify the CNWDI access is updated in JPAS/DISS. (T-1)

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

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

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

9.2.3. **(Added)** If utilized, ensure the AF Form 2583 is completed:

9.2.4. **(Added)** Ensure the NATO access is updated in the JPAS/DISS. (T-1)

9.4. **(Added)** Security managers may debrief personnel to NATO information when the individual no longer needs access or leaves the organization, e.g., permanent change of station or assignment, separation or retirement when delegated by their commander.

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

9.5.1. **(Added)** Foreign national/host nation employees of the U.S. Government from NATO member nations who require access to NATO classified information in the performance of their duties will apply to their government for NATO certification for access to NATO classified information and provide that certification to the Unit Commander, program manager, unit security manager, and Wing IPO as appropriate. (T-3)

9.6. **(Added)** Access to NATO Information for non-U.S. and non-NATO Nation citizens**.** Non-U.S. and non-NATO nation citizens may be granted access to NATO information if an approved Limited Access Authority (LAA) with a NATO mission essential need-to-know exists. Refer to DoDM 5200.02_AFMAN 16-1405, 1 August 2018 for more information on LAAs. Refer to the current USSAN for instruction on granting access to non-NATO personnel.

10.1. **(Added)** General . The Senior Agency Official (SAF/AA) is required to establish a self-inspection program and report annually on a Fiscal Year (FY) basis to the Information Security Oversight Office (ISOO) and Office of Under Secretary of Defense, Intelligence (OUSD(I)) on the program's adherence to the principles and requirements of EO 13526, *Classified National Security Information*, DoDM 5200.01, Volumes 1-3, DoDI 5200.48. The SPE and Wing Commander's assist the Senior Agency Official with the development of the reports as part of the program oversight hierarchy.

10.1.3.1. **(Added)** 31 FW/IP will focus on areas of interest identified in AFI 16-1404, para. 10.3. using IG unit self-inspections, SAVs, IGEMS, and MICT. (T-3)

10.1.3.2. **(Added)** 31 FW/IP will be member of Wing Inspection Team (WIT) and conduct unit self-inspections IAW AFI 90-201 under the direction of the Wing IG. Findings will be utilized to complete the Wing's annual self-inspection.

10.1.3.3. **(Added)** Tenant units and GSUs that store or handle classified material and receive oversight and support from 31 FW/IP as specified in a support agreement, MOU, or MOA, will be inspected as part of the Wing IG's inspection program or biennially by 31 FW/IP. Tenant organizations may receive an information security inspection from their higher headquarters. In such cases, the tenant shall notify 31 FW/IP and provide a copy of the report. (T-3)

10.3. The Wing Chief, Information Protection and AFDO will complete the self-inspection using this AFI and DoDM 5200.01, Volumes 1-3, DoDI 5200.48. (T-1) The Wing Chief, Information Protection has responsibility for developing the report for areas in paragraph **10.3.1** – **10.3.6** (T-1) AFDO has responsibility for developing the report for **paragraph 10.3.5** as it relates to training of declassification authorities and **paragraph 10.3.7**.

10.3.1.4. **(Added)** Any other areas required by this AFI or DoDM 5200.01, Volumes 1-3, DoDI 5200.48

10.3.2.6. **(Added)** Any other areas required by this AFI or DoDM 5200.01, Volumes 1-3, DoDI 5200.48

10.3.3. **(Added)** Safeguarding. Identify discrepancies based upon the level of information each unit is required to protect IAW with standards of this AFI and DoDM 5200.01, Volume 3, DoDI 5200.48 (T-0)

10.6. **(Added)** Collateral classified material and CUI kept within a Sensitive Compartmented Information Facility (SCIF) or Special Access Program (SAP) Facility do not fall within the

purview of 31 FW/IP. Responsibility for inspections rests with the applicable SSO or Program Security Officer (PSO).

BARRE R. SEGUIN, Brigadier General, USAF
Commander, 31st Fighter Wing

**Attachment 1**

**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

***References***

Executive Order 13556, *Controlled Unclassified Information*, 4 November 2010

DoD Manual 5200.01 (Volumes 1-3), *Information Security Program,* 24 February 2012

AFI 31-101, *Integrated Defense (FOUO)*, 8 October 2009

AFI 16-1404*, Information Security Program Management,* 29 May 2015

AFI 16-1406, *Industrial Security Program Management*,

DoDM 5200.02_AFMAN *16-1405, 1 August 2018,*

AFI 90-201, *The Air Force Inspection System*, August 2, 2013

AFMAN 33-363*, Management of Records,* 1 March 2008

***Adopted Forms***

AF Form 2583, *Request For Personnel Security Action*

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

DD Form 2501, *Courier Authorization*

SF 312, *Classified Information Nondisclosure Agreement*

SF 700, *Security Container Sheet*

SF 701, *Activity Security Checklist*

SF 702, *Security Container Check sheet*

***Abbreviations and Acronyms***

**CC**—Commander

**CDSE**—Center for Development of Security Excellence

**CIP**—Chief, Information Protection

**COMSEC**—Communications Security

**CMI**—Classified Message Incident

**DISS**—Defense Information System for Security

**EMSEC**—Emission Security

**FDO**—Foreign Disclosure Office

**GSA**—General Services Administration

**HTSA**—Host Tenant Support Agreement

**IP**—Information Protection

**IPO**—Information Protection Office

**IT**—Information Technology

**JPAS**—Joint Personnel Adjudication System

**MICT**—Management Internal Control Toolset

**NATO**—North Atlantic Treaty Organization

**OI**—Operating Instruction

**OPSEC**—Operations Security

**PED**—Portable Electronic Device

**SCG**—Security Classification Guide

**SCI**—Sensitive Compartmented Information

**SCIF**—Sensitive Compartmented Information Facility

**SM**—Security Manager

**SME**—Subject Matter Expert

**SSO**—Special Security Officer

**TS**—Top Secret

**TSCA**—Top Secret Control Account

**TSCO**—Top Secret Control Officer

**USB**—Universal Serial Bus

**VGSA**—Visitor Group Security Agreement

**WIT**—Wing Inspection Team

***Terms***

**Collateral Classified Information**—Classified information which is not Sensitive Compartmented Information.

**Controlled Unclassified Information**—Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

**Sensitive Compartmented Information (SCI)**—A type of intelligence requiring more restricted dissemination and more protection to ensure that intelligence sources and analytical methods are protected.

## Attachment 2

## AIR FORCE SECURITY CLASSIFICATION GUIDE TEMPLATE

**Figure A2.1. SCG Template Cover Page.**

**[CLASSIFICATION] - center classification designation here IAW DoDM 5200.01, Volume 2 for classified guides. If unclassified see bottom of this page for marking guides FOUO.**

**[UNCLASSIFIED NAME OF THE SYSTEM, PLAN, PROGRAM, OR PROJECT]**
**SECURITY CLASSIFICATION AND DECLASSIFICATION GUIDE**

**[Program Logo (Optional)]**

**[Date (if revision, this date is the date of the original SCG)]**
**[When applicable, revision date]**
**ISSUED BY: [Name and address of issuing office]**
**APPROVED BY: [OCA name and title, or personal identifier]**
**[Statement of supersession of previous guides, if any]**
**[Distribution statement IAW DoDI 5230.24 and AFI 16-204]**

****NOTE: When the SCG or declassification guide is classified, all markings required by DoDM 5200.01, Volume 2 shall be included.**

**[CLASSIFICATION] – center classification here IAW DoD 5200.01, Volume 2 if guide is classified. If guide is unclassified, place FOUO designation here IAW DoDM 5200.48.**