

**BY ORDER OF THE COMMANDER
OFFUTT AIR FORCE BASE**



AIR FORCE INSTRUCTION 31-401

**OFFUTT AIR FORCE BASE
Supplement**

28 JANUARY 2015

**Certified Current, 14 February 2019
Security**

INFORMATION SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: The official version of this publication is available electronically on the Offutt AFB Sharepoint site at:
<https://offutt.eim.acc.af.mil/55thWing/wingstaff/wgprograms/IP/default.aspx> and <http://www.e-Publishing.af.mil>

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 55 WG/IP

Certified by: 55 WG/CV
(Colonel Mark L. Williamson)

Supersedes: AFI 31-401_OFFUTTAFB
Sup1, 2 September 2008

Pages: 8

AFI 31-401, 1 November 2005, Information Security Program Management is supplemented as follows: This instruction establishes policies and procedures governing the information security program. This publication does not apply to Air Force Reserve Command (AFRC) or Air National Guard (ANG) Units. 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) located at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>. Contact supporting records managers as required. This publication requires collection and maintenance of information subject to the Privacy Act of 1974. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using Air Force (AF) Form 847, *Recommendation for Change of Publication*; submit recommendations for improvements and/or changes in writing to 55 WG/IP, 205 Looking Glass Ave, Offutt AFB NE 68113-3120.

SUMMARY OF CHANGES

Updated to show the realignment of the Information Security Program to 55 WG/IP. Deletes requirement for quarterly security manager's meetings. Adds guidance on where personal electronic devices (PEDs) are prohibited.

1.3.5.1.3. **(Added)** Wing Information Protection Office (IPO) staff members will not be appointed as primary or alternate security managers for any organization.

1.3.5.3.1. **(Added)** Provide a copy of the security manager appointment letters to 55 WG/IP.

1.3.8.1. **(Added)** For Offutt AFB, the Chief, Information Protection, is designated as the Foreign Disclosure Officer.

1.7.1.1.3. **(Added)** Ensure all classified SIPRNET transmissions are included during each sampling period.

5.8.1.1. Telecommunication facilities that process collateral Top Secret material must be established as a Top Secret Control Account (TSCA). NOTE: Automation of TSCAs will be approved on a case-by-case basis. Approval must be granted by 55 WG/IP (Wing ISPM).

5.8.1.3.1. An inventory is conducted upon change of the primary Top Secret Control Officer (TSCO). Changes of custody inventories are conducted as of the appointment date of the new TSCO. Annual inventories are conducted as of the anniversary date of the last inventory.

5.8.1.3.1.1. **(Added)** The TSCA appointing authority appoints disinterested personnel who have knowledge of Top Secret control procedures as inventory officials. More than one person may be appointed to conduct an inventory. During inventories, the official will evaluate the management of the TSCA. The TSCO and any alternates may not participate in the inventory, but may assist the inventory official. During a change of custody inventory, the new TSCO may evaluate the management of the TSCA by serving as the inventory official prior to assuming duties. For other than change of custody inventory, the senior inventory official must be senior in grade to the TSCO.

5.8.1.3.1.2. **(Added)** An inventory is conducted to audit inactive register page entries for proper disposition, to physically sight active material, and to ensure compliance with Top Secret control procedures.

5.8.1.3.1.3. **(Added)** When accomplishing the audit, the inventory official will determine that all pages of the register are available or accounted for. An entry marked as being audited will not be reaudited. The inventory official shall date item 11g, and sign item 13g of the AF Form 143, when review of the register page reflects a final disposition of:

5.8.1.3.1.3.1. **(Added)** A receipt covering permanent transfer of the document (item 13a or a separate receipt).

5.8.1.3.1.3.2. **(Added)** A recontrolled document (item 12f or item 16 and the presence of a new register page).

5.8.1.3.1.3.3. **(Added)** Downgrading or declassification (item 13f and supporting documentation).

5.8.1.3.1.3.4. **(Added)** Destruction (item 13d and 13e).

5.8.1.3.1.3.5. **(Added)** Incorporation into another document (item 13f and supporting documentation).

5.8.1.3.1.3.6. **(Added)** Other relief from accountability (item 13f and supporting documentation).

5.8.1.3.1.4. **(Added)** The sighting portion of the inventory is physically locating each document or material and comparing them to their respective register page entries reflecting accountability. Additionally, sighting ensures that all Top Secret material on hand has been entered into the register.

5.8.1.3.3.1. **(Added)** The inventory official will prepare a report and submit it to the appointing authority. The report must contain a specimen signature and initials of all inventory officials and will be of sufficient scope to explain compliance with all Top Secret control procedures. The report must list any material reflected in the register for which accountability could not be established, any material on hand but not entered in the register and any condition that could have resulted in the compromise or suspected compromise of material. The appointing authority will review the volume and need for retaining the Top Secret material, and will certify this review when endorsing the inventory report. A copy of the report is filed in the account for reference purposes during the next inventory.

5.8.1.7. **(Added)** Top Secret Control and Accountability:

5.8.1.7.1. **(Added)** The primary Top Secret Control Officer (TSCO) will prepare AF Form 143, Top Secret Register Page, for each Top Secret item received or derivatively created within the unit. Controlling action will be completed within one duty day of receipt or creation. All Top Secret material (non-SCI) maintained within any facility must be brought under control by the TSCO.

5.8.1.7.2. **(Added)** A Top Secret Register is a complete file of all AF Forms 143 and shall be kept on a calendar year basis. It will have an active and inactive section. AF Forms 143 in each section are filed numerically, based on the assigned register page number. The last page of each register will be marked "THIS PAGE (NUMBER) IS THE LAST PAGE OF THE TOP SECRET REGISTER FOR CALENDAR YEAR 20__". Maintain a Top Secret Register for the current year and four previous years.

5.8.1.7.3. **(Added)** Each Top Secret document or material will have a specific number assigned by the TSCO. This number is entered on the document and the register page. The format of the number will be the four-digit year, the alpha character of the unit and the sequential number of the document, e.g., 2013-XP-001. The alphabetical letters A, B, C and so on will be used when preparing continuation pages to the basic form. Previously assigned control numbers will not be removed from document(s). Line through (one-time) previously used control numbers.

5.8.1.7.4. **(Added)** All Top Secret material will be re-controlled annually. A register page that contains active and inactive entries is closed by transferring active entries to a new register page in the new year's register. Re-controlling remarks are entered in item 12f of the previous register page and item 15 of the new register page. Creating a new register page for the current year closes a register page that contains only active entries. Create a duplicate register page for active documents and renumber accordingly. Re-controlling remarks are placed in item 16 of the previous year's page, and item 15 of the new year's page.

5.8.1.7.5. **(Added)** TSCOs will attach AF Form 144, Top Secret Access Record and Cover Sheet, to the front of each non-SCI Top Secret document on file. The holder of the material is responsible for ensuring that all personnel who require access to the document have signed the AF Form 144. The AF Form 144 does not transfer with material when permanently removed from the account, and is maintained on file for two years after accountability terminated.

5.12.1.1. **(Added)** Designated temporary repositories for overnight storage of Top Secret, Secret and Confidential collateral material is the 55th Wing Command Post, commercial: 402-294-3725. 55 WG/IP will ensure operations dispatch, passenger service, base entry controllers and billeting personnel know where the overnight repository is located.

5.12.3.1. **(Added)** In-transit aircraft with large amounts of classified material will be parked in an aircraft parking ramp at Mike South. Vehicles/Trailers with large amounts of classified material will be parked at Mike North on the flightline. Owner/user personnel retain responsibility for their material/equipment.

5.14.2.2.1.1. **(Added)** Security Forces will not be designated to conduct these checks.

5.15.1.1. **(Added)** Copiers used for classified reproduction will not be connected to the unclassified network.

5.18.2.1. **(Added)** The Commander or Staff Agency Chief of the proposed area must submit a request for unattended open storage survey, in writing, to 55 WG/IP. NOTE: If the facility is operated 24 hours a day, no approval for unattended open storage is required, or granted.

5.18.2.2. **(Added)** The request must include complete justification, e.g., size, amount, reason security containers can't be used, etc., and type and level, of material or equipment to be openly stored.

5.18.2.3. **(Added)** See attachment 1 for guidance on prohibited items in classified open storage areas, classified discussion areas, restricted/controlled areas and transient/non-transient aircraft.

5.21.2.3. **(Added)** Refer to DODM 5200.01, Volume 3, Enclosure 5, paragraph 10a on how to protect the SF 700.

6.8. Use of the DD Form 2501, Courier Authorization Card, by 55th Wing units is not authorized for Offutt AFB. USSTRATCOM courier cards are not authorized for use by 55th Wing units outside of the STRATCOM complex.

6.8.1. **(Added)** Use a Courier Authorization Letter when classified material is hand-carried off base.

8.10.1.5.1. **(Added)** Refer to AFI 13-502, Offutt Supplement, for specific guidance on preparing and processing NC2-ESI approval packages.

8.11.5.1. **(Added)** Following e-Government Act and Government Paperwork Elimination Act guidance, the AF Form 2587 may be scanned and electronically filed once signed.

9.9.1.2. The inquiry/investigation official will contact 55 WG/IP for a briefing on the aspects of the security incident and 55 WG/JA for legal guidance on administering oaths and taking verbal testimonies and sworn statements. The inquiry/investigation official will provide a copy of the appointment letter to 55 WG/IP.

9.11.2.2.1. **(Added)** The inquiry/investigation official should not be the unit security manager as they manage the units security program and could be considered biased.

9.12.1.1. **(Added)** The inquiry report will be processed through 55 WG/IP for technical review, then the Appointing Authority (Commander) for closure. Provide a copy of the report to 55 WG/IP for filing. The original report is maintained by the affected unit security manager and used for recurring security education training.

9.12.1.2. **(Added)** The investigation report will be processed through 55 WG/JA to determine legal sufficiency and recommendations on any disciplinary actions that should be considered first; 55 WG/IP will then conduct a technical review to determine if all security standards were met for a compromise; and finally to the appointing authority (commander) for closure. If a security violation occurred, the report closure is not delayed awaiting a damage assessment from the OPR. The appointing authority must close the report and forward the damage assessment results upon receipt to 55 WG/IP.

9.12.4.1. **(Added)** Security managers must notify 55 WG/IP upon any granted extension, and provide a copy of the extension memorandum.

MARK L. WILLIAMSON, Colonel, USAF
Vice Commander, 55th Wing

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 31-401, Information Security Program Management, 1 November 2005

Abbreviations and acronyms

IPO—Information Protection Office

ISPM—Information Security Program Manager

NC2-ESI—Nuclear Command and Control – Extremely Sensitive Information

PDA—Personal Digital Assistance

PED—Personal Electronic Device

SCI—Sensitive Compartmented Information

TSCA—Top Secret Control Account

TSCO—Top Secret Control Officer

Attachment 2

PERSONAL ELECTRONIC DEVICE GUIDANCE

A2.1. (Added) Due to multiple security policies addressing personal electronic devices (PED), this consolidated guidance is provided for prohibited items in classified open storage areas, classified discussion areas, restricted/controlled areas and transient/non-transient aircraft as follows:

A2.1.1. **(Added)** The use of any device capable of capturing video and still images, to include cell phones with Integral Digital Camera Capability, pose an unacceptable security risk to the protection of vital USAF resources and information. Individuals will be denied access to restricted and controlled areas if in possession of these devices without a valid authorization letter IAW the 55th Wing Integrated Defense Plan.

A2.1.2. **(Added)** In the interest of protecting our classified material and equipment, the following items are prohibited from entry to our approved Classified Open Storage and Classified Discussion Areas:

A2.1.2.1. **(Added)** Personally owned photographic, video, and audio recording equipment.

A2.1.2.2. **(Added)** Personally owned computers and associated media.

A2.1.2.3. **(Added)** Personally owned CD-R, CD-RW, and any type of Magnetic Media.

A2.1.2.4. **(Added)** Government and personally owned Personal Digital Assistance (PDAs) and Palm Pilots.

A2.1.2.5. **(Added)** Cell phones or any hand-held two-way radios.

A2.1.2.6. **(Added)** Wrist watches with data ports or data diaries

A2.1.2.7. **(Added)** Thumb and flash drives.

A2.1.2.8. **(Added)** Two way pagers and/or beepers; receiving one way is acceptable.

A2.1.2.9. **(Added)** Any government or personally owned device with Wi-Fi, Blue Tooth or any other ability to transmit or record information.

A2.1.3. **(Added)** For 55 WG aircraft, use of PEDs is prohibited at all times except in the following circumstances:

A2.1.3.1. **(Added)** Aircrew may use cell phones on the ground prior to engine start. After engine start, cell phones will be powered down and properly stowed in an approved container and not used until aircraft shut down.

A2.1.3.2. **(Added)** Non-transient aircrews with PEDs are required to maintain a valid cellular telephone authorization letter when inside 55 MPA restricted or controlled areas signed by the Installation Commander or his designee.

A2.1.4. **(Added)** For Transient Aircraft, aircrews are authorized to maintain government and/or personal PEDs while inside the lower 55 MPA, Foxtrot Row on Upper Transient Aircraft Ramp and Bennie L. Davis Maintenance Facility (BLDMF) Aircraft Bays, Building 457. Transient aircrew in possession of such devices must turn off and stow the device in a cargo pocket, flight suit, luggage or flight-bag while transiting through the restricted area. These

aircrew members can be identified by their home station restricted area badge and are exempt from maintaining a valid cellular authorization letter.

A2.1.5. **(Added)** Campisi Alert Facility procedures. Transient and non-transient aircrews on alert and confined to the Campisi Alert Facility may use authorized electronic processing equipment in approved and designated electronic processing areas within the Campisi Alert Facility. SCW-1 must coordinate the designated electronic processing equipment areas with 55 SFS.

A2.1.6. **(Added)** The 55 CS/CC is the Collateral Designated Approving Authority for electronic devices and may waive this policy on a case by case basis for Classified Open Storage and Discussion Areas. Submit a request justifying the waiver to include 55 WG/IP and 55 CS/SCXS in the coordination process. Waiver authority for Sensitive Compartmented Information Facilities is the respective MAJCOM Special Security Officer. For other special access areas refer to JAFAN 6-0, Revision 1, Section 9 for additional guidance. Additionally, refer to 55th Wing Installation Defense Plan, Tab B/Appendix 3/Annex C for cellular phone use, airfield photography and videotaping approval authority within restricted and controlled areas. Security managers will include this topic in recurring security education efforts.