

**BY ORDER OF THE COMMANDER
14TH FLYING TRAINING WING (AETC)**

**AIR FORCE INSTRUCTION 31-401
1 NOVEMBER 2005**



**AIR EDUCATION AND TRAINING COMMAND
Supplement
5 JUNE 2007**

**COLUMBUS AIR FORCE BASE
Supplement
17 APRIL 2014**

Security

INFORMATION SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available on the e-Publishing website at www.e-publishing.af.mil for downloading.

RELEASIBILITY: There are no releasability restrictions on this publication.

OPR: 14 FTW/IP

Certified by: 14 FTW/CV
(Col Howard McArthur)

Supersedes: AFI 31-401 CAFBSUP, 25 September 2012

Pages: 17

This publication applies to all individuals assigned, attached or employed at Columbus AFB along with any servicing tenant units. This publication applies to Air Force Reserve Command (AFRC) Units. This supplement implements AFI 31-401, *Information Security Program Management*. It establishes procedures for properly safeguarding classified information on Columbus AFB. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. This revision reflects changes to the self-inspection program and deletion of items now incorporated into AFI

31-401_AFGM2. Additionally, Columbus Air Force base unit operating instructions have been consolidated into AFI 31-401_AETCSUP_COLUMBUSAFBSUP.

4.3.4. At Columbus AFB, the 14th Flying Training Wing Chief of Information Protection (CIP) is designated as the Information Security Program Manager (ISPM).

1.3.5.2. Ensure safe custodians receive training required by chapter 8.

1.3.6.2. Unique security requirements are annotated in Attachments 10 and 11.

1.3.6.4. The primary security manager must attend the CIP hosted unit security managers' meeting to maximize security awareness. It is optional but highly suggested for alternate security managers. A primary and one make-up meeting will be scheduled to allow for variances in schedules. A third meeting may be held for extenuating circumstances.

1.3.6.11.2. Includes Defense Security Service (DSS) Derivative Classification Training and JPAS/JCAVS Virtual Training for Security Professionals certificates for each security manager appointed. Training may be located at: <http://www.dss.mil/cdse/catalog/information-security.html>

1.3.6.11.6. Initial training for cleared personnel includes basic security training, unit specific training as required, NATO and derivative classification training. Un-cleared personnel may complete only general and unit specific portions of training. All appointed safe custodians shall accomplish initial safe custodian training. Recurring training consists of annual supervisor-to-subordinate training and annual completion of Information Protection Computer Based Training (CBT) located on the Advanced Distributed Learning Service (ADLS) website.

1.3.6.11.8. Additionally file safe custodian appointment letters along with the DSS derivative classification training certificates for each safe custodian appointed.

1.5.4. The Special Security Office (SSO) for Sensitive Compartmented Information (SCI) for Columbus AFB is AETC/A2OS. All personnel requiring SCI access will be processed through the Information Protection office. Individuals will need to provide their tasking letter or a copy of their orders.

1.6.1. Send waiver request through 14 FTW/IP.

2.1.3. There are no authorized OCAs at Columbus AFB.

5.2.1.2. The unit security manager is the presiding official and will sign the SF 312 in the Acceptance block.

5.3.1.1. The current office symbol to send active duty military NdAs to is AFPC/DPSOMI.

5.3.1.3. The current office symbol to send retired general officers NdAs to is AFPC/DPSOMR.

5.8.1.1. There are no Top Secret Control Accounts on Columbus AFB.

5.9.1.4. **(Added)** Use AF Form 614, *Charge Out Record*, to sign out/in classified documents temporarily removed from security containers, vaults or secure rooms to ensure accountability.

5.9.3.1. **(Added) Emergency protection.** The installation commander directs the implementation of emergency relocation/destruction of classified material based on civil disorder, terrorist threat/activities or enemy action. The protection of life and wellbeing of group/unit personnel will not be jeopardized to protect classified material.

5.9.3.1.1. **(Added)** Personnel protecting classified material must have a security clearance up to the highest level of the classified material being stored.

5.9.3.1.2. **(Added)** When it is safe to do so, post unarmed unit guards around a facility housing classified material when it is damaged to the extent it cannot be secured or when directed by the installation commander.

5.9.3.1.3. **(Added)** Ensure guards have sufficient knowledge to prevent unauthorized removal of classified material.

5.9.3.1.4. **(Added)** Individual in charge of group/unit guards must know storage container combination and be authorized to deviate from this plan.

5.9.3.2. **(Added) Fire.** If classified material can be safely removed from the facility, authorized personnel transport materials to the Command Post. If the command post is the facility in question and classified material can be safely removed from this facility, authorized personnel transport materials to the alternate command post. If classified material cannot be safely removed, leave it in the container and depart the facility.

5.9.3.3. **(Added) Bomb Threat.** In the event of a bomb threat the classified custodian should secure any classified material that is not in the locked container on their person. **DO NOT open classified containers.** The custodian or authorized person should transport any classified material that is not in the container to the command post or alternate command post if manned.

5.9.3.4. **(Added) Emergency Evacuation for Enemy Attack.** Relocation elsewhere on base is not feasible for activities possessing a large volume of classified material.

5.9.3.5. **(Added)** Relocation of classified material off base is not authorized.

5.11.2. Send request for removal of Secret or Confidential information from designated work areas during non-duty hours to 14 FTW/IP for technical review and approval.

5.11.3. Send contingency plans for residential storage of classified information to 14 FTW/IP for technical review and approval.

5.11.3.1. **(Added)** Inspections for unauthorized removal of classified are included in Random Installation Entry/Exit Vehicle Checks (RIEVC). Procedures are outlined in the Security Forces AFI 31-201, *Installation Entry Control*.

5.12.1. The Columbus AFB Command Post is designated as the overnight repository for classified information for Columbus AFB. The Command Post is also designated for temporary storage of classified material (Confidential, Secret) in the possession of transient and other personnel.

5.12.2. Secret and Confidential material will not be stored on the flightline during in-processing for deployment purposes unless specifically approved by the installation commander.

5.13.1.1. **(Added)** At a minimum, activities hosting local classified meetings or briefings will conduct meetings IAW DoDM 5200.01-V3, section 16, *Classified Meetings and Conferences*.

5.13.1.1.1. **(Added)** Post guards (unit hosting) as needed on exit/entry doors or adjacent rooms to prevent unauthorized monitoring, eaves dropping and/or protection of portable devices for attendees.

5.13.1.1.2. **(Added)** Announce meeting on a need-to-know basis, preserving Operations Security (OPSEC) IAW AFI 10-701, *Operations Security*. For OPSEC questions, contact the Wing OPSEC manager.

5.13.1.1.3. **(Added) Verify Attendees.**

5.13.1.1.3.1. **(Added)** Verify attendees' clearances by using Joint Personnel Adjudication System (JPAS). JPAS checks shall not be conducted earlier than one week prior to the meeting or briefing.

5.13.1.1.3.2. **(Added)** For the Crisis Action Team members, verification of members' clearances through JPAS will be conducted every 30 days by wing staff agency security managers. A roster will be populated and maintained in the command post identifying cleared members.

5.13.1.1.4. **(Added) Conducting the Classified Meeting.**

5.13.1.1.4.1. **(Added)** The meeting shall brief, IAW AFI 31-401, Para 4.8.2., personally owned information systems storage media are prohibited in areas where classified is processed. Additionally, IAW AFSSI 7702, Para 5.4.12., All other wireless Portable/Personal Electronic Devices (PED) not specifically addressed, that are used for storing, processing, and/or transmitting information must be turned off in areas where classified information is electronically stored, processed, or transmitted. Any items falling within these criteria shall be placed outside of the briefing room door.

5.13.1.1.4.2. **(Added)** Any meeting slides must be marked with a classification level and any special warning or control notices. Information on the slide area must be portion marked to differentiate classified from unclassified.

5.13.1.1.4.3. **(Added)** Secure the entry door at the start of the classified session. Do not allow subsequent entry without halting the meeting/briefing, safeguarding classified materials and verifying the identity and security clearance of personnel seeking entry.

5.13.1.1.4.4. **(Added)** The meeting should begin with an administrative announcement reminding attendees that classified material will be discussed during the meeting, that all clearances have been verified and the highest level of classified information that may be discussed during the meeting (commensurate with the level of attendees access/eligibility). Also cover any special warning or control notices that may be applicable to the material such as “Formerly Restricted Data”, Not Releasable to Foreign Nationals - “NOFORN”, etc.

5.13.1.1.4.5. **(Added)** Generally, note taking is prohibited. If notes are authorized, personnel should mark their notes as classified “Working Papers” with the classification markings annotated as directed in AFI 31-401, AETC Sup, Para 4.3.1.

5.13.1.1.4.5.1. **(Added)** The host should be prepared to wrap, transport, and temporarily store any working papers created in the host unit’s approved GSA safe. Additionally, the host will brief attendees on how to properly transport classified materials. Attendees will coordinate with their unit’s safe custodian an approximate date and time to transfer the classified materials from the host’s safe to their unit’s safe. Transfer must take place within 10 working days or the materials will be properly destroyed.

5.13.1.1.4.6. **(Added)** Any classified documents, notes, disks, or briefing slides must be properly marked, collected and accounted for at the end of the meeting/briefing.

5.15.1.3.1. **(Added) Secure Fax Machine Procedures.**

5.15.1.3.1.1. **(Added)** Only those government official(s) appointed or positions designated by the group/unit commander may transmit classified documents via fax machine. This designation may be incorporated with the appointment memorandum annotated in Para.

5.24.4.1. Maintain appointment memorandum in group/unit security manager binder. **Note:** No appointment letter on file reflects the transmission of classified documents via secure fax machine is not authorized within the group/unit.

5.15.1.3.1.2. **(Added)** The secure fax machine is located within the Command Post (Bldg. 724, Room 149) and will be operated IAW AFI 10-207 and any supplements.

5.18.3.1.1. Procedures for protection and positive entry into Columbus Air Force Base’s secure rooms are annotated in Attachments 10 and 11.

5.18.3.1.3. Submit a draft written security plan outlining compensatory measures that will be implemented for the level of certification required (Secret) via email to 14 FTW/IP for technical review. Send the final security plan to 14 FTW/IP for approval utilizing an AF IMT 1768 or

ESSS. Once approved by the 14 FTW/IP, the written security plan becomes part of the 14 FTW/CC certification package for the open storage of classified information.

5.22.1. Columbus AFB's certified GSA safe inspector is located in the Civil Engineering (CE) squadron. Contact the CE service desk at 434-2857 and submit a work request. The GSA inspector does not have an ANACI/NACLC and must be escorted when servicing security containers.

5.23. At a minimum, combinations to security containers, vaults, and secure rooms will be changed whenever an individual knowing the combination no longer requires access to it or when a possible or actual compromise has occurred. A preventative maintenance inspection will be conducted with each combination change. Results will be annotated on an AFTO Form 36, *Maintenance Record for Security Type Equipment* and Standard Form 700, *Security Container Information*. **Note:** Safe custodians are the only unit personnel knowledgeable of the combination to the unit's GSA safe. Some units may have many safe custodians due to the number of personnel that require the combination.

5.24.4. (Added) Procedures for Reproduction of Classified Materials.

5.24.4.1. (Added) Only those government official(s) appointed or positions designated by the group/unit commander may approve the reproduction of **SECRET** and below classified documents. Maintain appointment memorandum in group/unit security manager binder. **Note:** No appointment letter on file reflects reproduction of classified is not authorized within the group/unit.

5.24.4.2. (Added) The location of the only approved classified reproduction equipment (copier) is the Command Post located at Bldg. 724, Room 149. Approved reproduction equipment will be placed in an area where command post individuals can maintain constant surveillance and enforce rules against unauthorized use.

5.24.4.3. (Added) The reproduction of classified material will be strictly controlled and any reproduction limitations enforced. If the reproduction of classified material is required, two appropriately cleared persons must accomplish the reproduction process. The reproduction approval official appointed by the group/unit commander will indicate the number of authorized copies on the original document, include distribution/recipients and initial. Additionally, "Copy ___ of ___ total copies" will be annotated on each copy along with initials of reproduction official. The requester will appropriately file annotated documents.

5.24.4.4. (Added) Ensure approved classified reproduction equipment is cleared after classified reproduction in accordance with instructions as outlined on AETCVA 31-5, *Classified Reproduction Authorized*. If applicable, erase volatile memory after each use.

5.24.4.5. (Added) Review DoDM 5200.01 and AFI 31-401 for additional requirements or limitations.

5.27.2.1. **(Added)** Classified material stored in storage containers will be reviewed annually, not later than the 10th working day in January to determine the disposition of unneeded classified material. Classified material will not be retained longer than necessary.

8.3.4. Group/unit security managers may provide supervisors security education training material to assist them in training their personnel.

8.3.4.1. **(Added)** Supervisors will evaluate and rate Air Force employees on the performance of security responsibilities and provide training annually.

8.6. There are no authorized OCAs on Columbus Air Force Base.

8.7.1. **(Added)** Initial safe custodian training and derivative classification training is required for all appointed safe custodians. Initial safe custodian training will be administered by the unit security manager and documented via sign-in sheet. Derivative classification training must be re-accomplished every two years. Initial safe training materials are located at <https://columbus.eis.aetc.af.mil/14ftw/IP/Information>. Derivative classification training is located at: <http://www.dss.mil/cdse/catalog/information-security.html>

JAMES R. SEARS, JR., Colonel, USAF
Commander, 14th Flying Training Wing

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

DODM 5200.01, *Information Security Program*
AFI 10-207, *Command Post*
AFI 10-701, *Operations Security*
AFI 31-101, *Integrated Defense (FOUO)*
AFI 31-113, *Installation Perimeter Access Control*
AFI 31-201, *Installation Entry Control*
AETCVA 31-5, *Classified Reproduction Authorized*
AETCVA 31-10 *Classified Work In Progress*

Adopted Forms

AF Form 1109, *Visitor Register Log*
AF Form 1199, *USAF Restricted Area Badge*
AF Form 614, *Charge Out Record*
AFTO Form 36, *Maintenance Record for Security Type Equipment*
SF 312, *Classified Information Nondisclosure Agreement*
SF 701, *Activity Security Checklist*
SF 703, *Top Secret Cover Sheet*
SF 704, *Secret Cover Sheet*
SF 705, *Confidential Cover Sheet*
SF 706, *Top Secret (Label)*
SF 707, *Secret (Label)*
SF 708, *Confidential (Label)*

Abbreviations and Acronyms

14 CS—14th Communication Squadron
ADLS—Advanced Distributed Learning Service
CAT—Crisis Action Team
CBRNE—Chemical, Biological, Radiological, Nuclear and Explosive
CBT—Computer Based Training
CIP—Chief, Information Protection
CP—Command Post
DSS—Defense Security Service
EA—Emergency Action
EAL—Entry Authority List
EAM—Emergency Action Message
ECC—Emergency Control Center
E-QIP--Electronic Questionnaire for Investigations Processing
FPCON—Force Protection Condition
ISPM—Information Security Program Manager
JPAS--Joint Personnel Adjudication System
NCC—Network Control Center

OPSEC—Operations Security

RAB—Restricted Area Badge

RIEVC—Random Installation Entry/Exit Vehicle Checks

SCI—Sensitive Compartmented Information

SFS—Security Forces Squadron

SSO—Special Security Office

Attachment 9 (Added)**A9. (Added) PROCESSING CLASSIFIED MATERIALS:**

A9.1. **(Added) Internal Control of Secret Material.** Personnel who possess a valid personnel security clearance equal to or greater than the information being disclosed (verify via **Joint Personnel Adjudication System** (JPAS)), have a need to know information in the performance of their duties and have a signed Standard Form (SF) 312, *Classified Information Nondisclosure Agreement* recorded in JPAS will handle Columbus Air Force Base's classified materials in the following manner:

A9.1.1. **(Added)** Ensure all classified material is properly marked when it is placed into or removed from vaults/storage containers. SF 706, *Top Secret (Label)*, SF 707, *Secret (Label)*, and SF 708 *Confidential (Label)*, will be used to indicate Top Secret, Secret, and Confidential CDs, diskettes, laptop computers. SF 703, *Top Secret Cover Sheet*, SF 704, *Secret Cover Sheet*, and SF 705, *Confidential Cover Sheet*, will be utilized whenever classified documents are removed from the storage container.

A9.1.2. **(Added)** Classified material/information, which has been removed from the storage container, will not be left unattended at any time. If the custodian of the material is called away from the working area, he/she will secure the information in the storage container. Security containers, vaults, secure rooms and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

A9.1.3. **(Added)** The exterior door to the working area will be closed when classified material is taken out of the security container and an AETC VA 31-10 *Classified Work In Progress*, is posted on exterior door.

A9.1.4. **(Added)** Classified material or information will not be intermixed with non-classified material in the working area.

A9.1.5. **(Added)** Conspicuously mark notebooks, binders, and similar holders with the highest classification of the material it contains. Affix the appropriate classified cover sheet to front and back and mark the spine with the overall classification. All classified materials must annotate the classification, whom the material is classified by or derived from along with declassification instructions.

A9.2. **(Added) Compromise.** In the event of an actual or suspected compromise of classified material, notify the group/unit security manager immediately!

A9.3. **(Added) Transmission.** The telephone is considered an unsecured voice system and as such may not be used for transmissions of classified information. A STE is the only phone that can be used for classified telephone transmissions.

A9.4. **(Added) Transportation.** In the event classified information needs to be transported via commercial carrier, procedures outlined in IAW DoDM 5200.01-V3, Enclosure 4, will be followed.

A9.5. (Added) Handling Registered, Certified, First Class and Express Mail

A9.5.1. **(Added)** Group/unit personnel will be notified by the Base Information Transfer Center (BITC) when registered, certified, first class or express mail has been received. Classified custodians who have been designated in writing will pick up and sign for the potentially classified parcels.

A9.5.2. **(Added)** All incoming mail will be safeguarded until its classification is determined. Incoming mail will be opened on the day it is received. If classified material is received by a group/unit via means other than through BITC, the group/unit security manager must be notified immediately.

A9.5.3. **(Added)** Items delivered by civilian carriers (UPS/FedEx/Messenger/etc.) will be safeguarded until classification is known. Any mail labeled "return service requested" has the potential to be classified documents and will be protected as same. Notify the group/unit security manager immediately if mail meeting these criteria is delivered to the unit. If the mail parcel cannot be delivered to the direct recipient, the parcel MUST be stored in A GSA approved document safe until direct delivery to the recipient can be made.

A9.6. (Added) Escort or Hand-carrying of Classified Material

A9.6.1. **(Added)** The unit commander, staff agency chief, or security manager authorizes appropriately cleared couriers to hand-carry classified material on commercial flights or by means other than commercial flights IAW DoDM 5200.01-V3, Enclosure 4.

A9.6.2. **(Added)** Group/unit security managers or supervisors brief each authorized member hand-carrying classified material of their duties and responsibilities.

A9.6.3. **(Added)** Each group/unit that releases classified material to personnel for hand-carrying:

A9.6.3.1. **(Added)** Main a list of all classified material released and document IAW AFI 31-401, AETC Supplement.

A9.6.3.2. **(Added)** Keep the list until conformation of the material reaching the recipient.

A9.7. **(Added) Documentation.** Officials shall provide a written statement to each individual who is authorized to escort, courier, or hand-carry classified material. The authorization statement may be contained in a letter, a courier card, or other written document, including travel orders. Procedures will be accomplished IAW DoDM 5200.01-V3, Enclosure 4, Para.

12 and AFI 31-401, AETC Supplement. **EXCEPTION:** documentation is not necessary when hand-carrying classified information to activities within an installation.

Attachment 10 (Added)**A10. (Added) NETWORK CONTROL CENTER (NCC) SECURITY AND ENTRY CONTROL REQUIREMENTS**

A10.1. **(Added)** 14th Communication Squadron (14 CS) personnel will comply with all entry and circulation control procedures as outlined in AFI 31-101, *Integrated Defense (FOUO)* and all applicable supplements.

A10.1.1. **(Added)** NCC Personnel will follow all FPCON procedures in effect as directed by the commander.

A10.1.2. **(Added)** NCC Personnel will ensure all non NCC personnel at the NCC follow all FPCON procedures in effect as directed by the commander.

A10.2. **(Added)** NCC will maintain an Entry Authority List (EAL) of escort personnel. Security clearances for personnel annotated on the EAL will be verified by the unit security manager using JPAS; the unit commander will endorse the EAL. The EAL will then be sent to Security Forces (SFS) for authentication. Whenever changes occur, NCC will update, route for signature and authentication, and post the EAL at the secure area barrier door.

A10.2.1. **(Added) Verification of Unescorted Entry Authorization.** Columbus AFB does not utilize the AF Form 1199, *USAF Restricted Area Badge*; therefore NCC personnel will verify individual's credentials through a combination of personal recognition, and Entry Authority List (EAL).

A10.3. **(Added) NCC Escort Official.** NCC personnel with escort authority are designated on the NCC EAL. Extended visitors requiring more than a one-time entry will have a visit request submitted through JPAS for clearance verification. Authorized personnel may grant entry into the NCC by following these guidelines:

A10.3.1. **(Added)** Only personnel designated by the NCC EAL are authorized to sign personnel into the NCC using the AF Form 1109, *Visitor Register Log*.

A10.3.2. **(Added)** Escort officials must be trained IAW AFI 31-101. Escort officials will brief the visitors on evacuation and safety procedures prior to entry. Escort officials will maintain visual contact and ensure visitors follow evacuation and safety procedures, maintain accountability, and assist as needed when evacuating.

A10.3.3. **(Added)** Visual contact will be maintained by escort. Only visitors with a cleared JPAS visit request will be allowed in the classified processing area.

A10.3.4. **(Added)** Unapproved devices (USB storage, cellular devices or any camera equipped device) will remain outside the secure room.

A10.3.5. **(Added)** Un-cleared visitor warning indicators (red flashing overhead lights) will be activated when personnel are being escorted.

A10.3.6. **(Added)** All personnel granted entry into the NCC will be signed in utilizing the posted AF Form 1109 unless otherwise annotated on an EAL. First responders will be signed into the NCC using the posted AF Form 1109 AFTER the responding situation has been called "ALL CLEAR".

A10.4. (Added) Entry and Exit Procedures. Strict entry procedures are required to provide adequate protection for personnel working inside the restricted area and to eliminate unnecessary traffic. NCC entry is controlled by the on-duty personnel during normal day-to-day operations. No other individuals will admit or allow entry of any persons desiring access without the specific approval of duty personnel. Unit procedures must comply with the following, if applicable:

A10.4.1. **(Added)** During working hours, the back door of the secure room will be armed and secured with the metal arm bar IAW DoDM 5200.01 unless actively being used and observed by NCC personnel.

A10.4.2. **(Added)** During actual and exercise Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) conditions, actual or exercise active shooter conditions, or actual or exercise FPCON Delta conditions, only first responders and key personnel will be granted access; procedures in Para. A10.3.6. still apply.

A10.5. (Added) Facility Alarm Activation Procedures. The NCC is equipped with a facility alarm monitored by SF. In the event the facility alarm is activated, all personnel will follow the procedures below.

A10.5.1. **(Added)** Do not leave the facility unless there is an immediate danger. Personnel at facility will immediately make contact with the Emergency Control Center (ECC) via 434-7128. Follow the instructions from ECC personnel for identification and confrontation from first responders. First responders will secure the building.

A10.6. (Added) Evacuation Procedures. If the NCC is ordered to evacuate for any reason, all classified items will be secured unless there is immediate danger. If there are open storage items present, the vault door will be secured after all personnel are evacuated. If classified items are not able to be secured, an immediate inventory will be performed upon return. Notify the SF first responders that all personnel present must be logged until all items are accounted for.

Attachment 11 (Added)**A11. (Added) COMMAND POST (CP) SECURITY AND ENTRY CONTROL REQUIREMENTS**

A11.1. **(Added)** 14 FTW CP personnel will comply with all entry and circulation control procedures as outlined in AFI 10-207, *Command Post*, Chapter 11, AFI 31-101, *Integrated Defense (FOUO)*, and all applicable supplements.

A11.2. **(Added) Verification of Unescorted Entry Authorization.** Columbus AFB does not utilize the AF Form 1199 series, US Air Force Restricted Area Badge (RAB); therefore entry controllers will verify individuals' credentials through a combination of personal recognition, signature and credential check, and Entry Authority List (EAL); telephone or radio verification.

A11.2.1. **(Added)** Controllers do not need to annotate the following individuals on the AF Form 1109: IG or MAJCOM SAV members authorized unescorted entry into the CP/Command Center. Such inspectors and evaluators will use their own RAB from their home unit for entry if a Joint Personnel Adjudication System (JPAS) visit request or valid authenticated EAL is in place.

A11.3. **(Added) CP Escort Official.** CP personnel may be designated to escort visitors. Following notification and permission of the on-duty controller team, controllers may grant entry to the CP by following procedures outlined below.

A11.3.1. **(Added)** Only personnel designated by CP managers are authorized to sign personnel into the CP using the AF Form 1109.

A11.3.2. **(Added)** Escort officials for the CP restricted area will be limited to CP personnel, wing commander, and vice wing commander as applicable.

A11.3.3. **(Added)** Escort officials must be trained IAW AFI 31-101.

A11.4. **(Added) Entry and Exit Procedures.** Strict entry procedures are required to provide adequate protection for personnel working inside the restricted area and to eliminate unnecessary traffic. CP entry is controlled by the on-duty controller(s) during normal day-to-day operations. Augmenters control entry during Crisis Action Team (CAT) activation, contingencies, increased FPCONs, or as determined by the commander. No other individuals will admit or allow entry of any persons desiring access without the specific approval of an on-duty controller. Unit procedures must comply with the following, if applicable:

A11.4.1. **(Added)** Only one door of an entrapment/standoff area may be open at a time during routine operations. An entry controller must be present and all classified materials stored in the locked GSA security container if both doors are opened for operational or maintenance reasons.

A11.4.2. **(Added)** Escort officials will visually confirm personnel inside the entrapment/standoff area prior to opening the inner door to verify only the expected personnel are present, no apparent duress exists and the individual is in possession of a restricted area badge or other applicable identification credentials. Escort officials will check the contents of bags or packages before allowing access to visitors. Personal recognition is a valid technique and can be used after initial verification of the individual's authorization to enter. All visitors to the CP must be initially identified and processed. Visitors authorized unescorted access to the CP may be permitted re-entry upon examination of their restricted area badge or a controlled picture identification badge and personal recognition and search of any hand carried items.

A11.4.3. **(Added)** When personal recognition cannot be made, escort officials will direct personnel requesting entry to display restricted area badge or other identification credentials in front of close circuit camera for verification. The inner door shall remain secured until the process is complete.

A11.4.4. **(Added)** During actual and exercise CBRNE conditions, Command Personnel entering a restricted area will use a local entry code.

A11.4.5. **(Added)** During routine operations, personnel exiting the CP must ensure the entrapment/standoff area is clear (no one in entrapment/standoff area) before opening the inside door.

A11.5. **(Added) Circulation Control.** Emergency Action (EA) cell/console area direct access will be restricted to essential CP personnel and key personnel designated by the CP managers. The duty controllers will control access to the EA cell/console area.

A11.5.1. **(Added) Routine Operations.** During routine operations, only those CP personnel authorized direct access (i.e. controllers, CP administrative personnel) into the CP will be given the cipher lock combinations to the external doors. Only certified EA controllers will have the cipher lock combination to EA cell door, if the CP is so equipped.

A11.5.2. **(Added) CAT Operations.** During CAT or high-density operations, when an augments has been posted, the augments may be given the cipher lock combinations to CP outer door and CAT inner doors to control entry (not the EA cell door). The cipher lock combinations will be changed immediately upon completion of the exercise/operation or resolution of the crisis situation.

A11.5.2.1. **(Added)** Verification of CAT members' clearances through JPAS will be conducted IAW Para., 5.13.1.1.3.3. CAT members substituted on short notice will have the new attendee present a memorandum endorsed by their unit security manager stating the status of new attendee's security clearance or security clearances will be verified in JPAS.

A11.5.3. **(Added)** During CAT or high density operations when an augments is not available, the commander may authorize the outer door cipher lock combination be given

to CAT members, as required, who have unescorted access authority to the CP. Cipher lock combinations will be changed immediately upon completion of the exercise/operation or resolution of the crisis situation.

A11.5.4. **(Added)** Once visitors requiring escort have been processed into the CP by an escort official, the escort official may designate another individual authorized unescorted entry to control visitors. The escort official must ensure the escort is aware of the safety and security requirements pertinent to the visit. Procedures must be in-place to ensure personnel without both a need to know and the proper security clearance are cleared from the EA area and restricted from hearing conversations when the unit missions dictate classified discussion between controllers.

A11.5.5. **(Added)** Collocated CPs occupied by personnel with differing levels of clearances must ensure provisions are made to ensure protection of the classified material or equipment. For example, administrative personnel could not be left alone with access to Emergency Action Message (EAM) formats.