

**BY ORDER OF THE COMMANDER
440TH AIRLIFT WING**

440th AIRLIFT WING INSTRUCTION 31-401

19 JUNE 2012



Information Security

**INFORMATION PROTECTION PROGRAM
MANAGEMENT**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 440 AW/IP

Certified by: 440 AW/IP
(Mr Ernest Davis)

Pages: 19

This instruction implements Air Force Policy Directive (AFPD) 31-4, AFI 31-401, *Information Security*, AFI 31-501, *Personnel Security*, AFI 31-601, *Industrial Security*, Department of Defense Manual 5200.01 Vol 1-4, *Air Force Guidance Memorandum (AFGM) 1*, DoD *Information Security Program*, Department of Defense Regulation 5200.2-R, *Personnel Security Regulation*, Department of Defense Regulation 5220.22-R, *Industrial Security Regulation and the Air Force Information Protection CONOPs dtd 1 July 2008*. It establishes policies and procedures for Information Protection within the 440 Airlift Wing (AW) and all Air Force tenant units on Ft Bragg. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with 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/gess-af61a/afirms/afirms/>. 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, directly to 440 AW/IP, 374 Maynard Street, Bldg 306 Room 105, Ft Bragg, NC 28308-2409.

| | | |
|----|--|---|
| 1. | Information Security Policy and Program Management. | 2 |
| 2. | Marking. | 4 |
| 3. | Safeguarding. | 4 |

| | | |
|---|---|-----------|
| 4. | Storage of Classified Materials (Reference DoDM 5200. | 6 |
| 5. | Transmitting/Transporting/Destruction of Classified Information. | 7 |
| 6. | Training. | 8 |
| 7. | Security Incidents. | 8 |
| 8. | Personnel Security. | 11 |
| 9. | Security Clearance. | 11 |
| 10. | Requesting Personnel Security Investigations. | 12 |
| 11. | Air Reserve Technicians. | 13 |
| 12. | The Joint Personnel Adjudication System (JPAS). | 13 |
| 13. | Security Information Files (SIFs). | 13 |
| 14. | Security Clearance Reinstatement. | 13 |
| 15. | Industrial Security. | 13 |
| Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION | | 15 |

1. Information Security Policy and Program Management.

1.1. The Chief of Information Protection (CIP) and the Information Protection Office (IPO) has oversight for the 440 AW Information Protection (IP) program. The CIP implements the IP program on behalf of 440 AW/CC. The CIP is the Air Force Security Program Manager for all Air Force units on Ft Bragg who participate in the 440 AW/IP Information Security Program and is the single point of contact for all USAF information, personnel, and industrial security issues on Ft Bragg. The CIP is the designated authority to perform industrial security program oversight for Air Force contractor operations. Letters accepting or declining participation in the AFRC Information Security Program will be maintained in appropriate unit activity folders/binders. The IPO will provide the following services:

1.1.1. Conduct semi-annual security manager meetings. The CIP will sign meeting minutes and post them to the 440 AW/IP Information Protection SharePoint Site at: https://eim.amc.af.mil/org/440aw/440_WSA/Information%20Protection/default.aspx

1.1.2. Conduct training for newly appointed Unit Security Managers (USM). Initial USM training is conducted quarterly by IPO or as required, one-on-one USM training can be accomplished. Upon completion of training, security managers receive a Certificate of Training.

1.1.3. Assist USMs in developing unit security operating instructions.

1.1.4. Process and monitor inquiries and investigations.

1.1.5. Provide oversight for Visitor Group Security Agreements (VGSA) for all Air Force tenant units on Ft Bragg in accordance with AFI 31-601, *Industrial Security Program Management*. Security reviews may be conducted more often than once every 12 months for VGSA contractors who possess classified material.

1.1.6. Conduct a Wing Security Advisory Group (WSAG) semi-annually or more frequently as required and provide meeting minutes to all group members. Meeting minutes will also be posted to the 440 AW/IP Information Protection SharePoint Site.

1.1.7. The 440 AW/IP will conduct Local Information Protection Management Evaluations (LIPMEs), formally known as program reviews (PRs), on an annual basis. *EXCEPTION:* An extension to 18 months may be granted by the CIP for units that have demonstrated highly effective; discrepancy free programs during the previous PR. LIPMEs/SAVs may be conducted every two years for activities or units that do not store classified information.

1.1.8. All participating agencies will receive a LIPME. These evaluations will incorporate information, personnel, and industrial (if applicable) security programs and will either be conducted annually or semi-annually. The CIP will provide the commander or equivalent (hereafter referred to as unit commanders) the PR results in writing.

1.1.9. Air Force contractor visitor groups will be integrated into the 440 AW'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 (NISPOM).

1.2. Commander Responsibilities:

1.2.1. Commanders are responsible for implementation of the Information Security Program within their area of responsibility.

1.2.2. To ensure program success and continuity, Commanders are recommended to appoint full-time USMs as primary and alternates with at least one-year retainability. The primary USM will be a full-time employee/member of the unit. Appointment of security monitors is encouraged to assist USMs. Commanders forward USM appointment letters to 440 AW/IP within 15 days of appointment.

1.2.3. Ensure the USM receives training within 90 days of appointment. This training will be conducted by 440 AW/IP.

1.2.4. Security self-inspections: Unit commanders and staff agency chiefs involved with processing or holding classified information ensure personnel conduct semi-annual security self-inspections to evaluate information security program effectiveness.

1.2.4.1. Unit commanders and staff agency chiefs will appoint an individual, in writing, other than the unit security manager to conduct a semi-annual security inspection. These two self-inspections will be conducted 1) between 1 January and 30 July, and 2) between 1 August and 31 December utilizing the Management Internal Control Toolset (MICT) if available to the unit. The unit inspector must have access to MICT if it is to be used. Self-inspections should be completed by a person knowledgeable of the Information Security Program (other than the SM). USMs should monitor the inspection, review the observations (if any) and follow up to ensure discrepancies are corrected. The security manager will forward the semi-annual self-inspection report to 440 AW/IP upon completion if not using MICT. The

CIP may count the annual LIPME as one of the unit semi-annual self-inspections if the last self-inspection program review was conducted within the last six months.

1.3. Security Manager Responsibilities:

1.3.1. The USM manages the Information Security Program for the unit and maintains a security manager's continuity book. The USM continuity book will be tabbed as follows:

1.3.1.1. TAB 1: Current Security Managers appointment letter (copy to IP), Security container location/custodians (copy to IP), Classified Account Custodian (copy to IP), Semi-annual inspector appointment letter, Top Secret Control Officer letter (if applicable) (copy to IP), Security Managers Training Certificates.

1.3.1.2. TAB 2: Unit operating instructions.

1.3.1.3. TAB 3: Semi-annual inspections (last two reports).

1.3.1.4. TAB 4: Local Information Protection Management Evaluation (LIPME) (last two reports).

1.3.1.5. TAB 5: Inspection Checklist (MICT).

1.3.1.6. TAB 6: Unit INFOSEC Training Plan.

1.3.1.7. TAB 7: Vault/Secure Room certifications/SIPRnet surveys.

1.3.1.8. TAB 8: Industrial Security Program (If Applicable).

1.3.1.9. TAB 9: Misc.

1.3.2. Mandatory attendance is required by primary or alternate security manager at the semi-annual hosted security manager meetings.

1.3.3. Security Container Listing: Develop a master security container listing and provide a copy to 440 AW/IP. This list should contain the following: manufacturer of the container, unique ID number, lock type (X-08/09), physical location of the container, custodian information and date of last initial inspection or Preventive Maintenance Inspection conducted by the 440 AW/IP. If there is a secure room or vault in the unit, enter the location, type of lock and custodian information.

1.3.4. Ensure a visual aid identifying the USM and alternate is posted conspicuously throughout the Unit to ensure assigned personnel are aware of USM appointments.

2. Marking.

2.1. Classified holders must notify originator of improperly marked documents in writing.

2.2. All binders that contain classified information will be marked top and bottom, front and back with the highest level of classified stored therein. Exceptions would be binders that are too small to have an adequate spine.

3. Safeguarding.

3.1. Access.

3.1.1. Joint Personnel Adjudication System (JPAS) will be utilized to verify an individual's access level.

3.1.2. Nondisclosure Agreement (NdA). Provide a copy of the completed SF 312 to the individual upon request. Once you enter the data into JPAS send SF 312 to the appropriate agency, addresses are located in AFI 31-401 para 5.3.

3.1.3. Refusal to sign. When a person refuses to sign an NdA, the commander or staff agency chief:

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

3.1.5. Denies the individual access to classified information.

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

3.1.7. In absence of verification of a signed SF 312, Nondisclosure Agreement (NDA), complete a new form and forward to 440 AW/IP.

3.1.8. 440 AW/IP may forward visit requests in the absence of security managers.

3.2. Use AF Form 614, Charge Out Record, or similar form, when a document is removed from a security container.

3.3. The unit operating instruction (OI) must address procedures for the protection, removal or destruction of classified material in case of natural disaster, fire, civil disturbance, terrorist activities or enemy action. (DoDM 5200.01, Vol 3, Enclosure 2, para 10). An OI template is located on the 440 AW Information Protection EIM page.

3.4. In units and staff agencies in which classified material is stored or handled and the facility is manned on a 24-hour, 7-day-a-week basis by cleared personnel may have the option to use SF 701, Activity Security Checklist on security containers, vaults or secure storage rooms. This action is at the discretion of the owner. At no time will classified material be left unattended when opened. Include on your SF 701 (if applicable): Check all classified computers to ensure that the hard drive has been removed and locked in a GSA approved container. Check all Global Command and Control System (GCCS)/SIPRNET connections to ensure they have been properly secured IAW local guidance.

3.5. The Pope Combined Command Post is designated as the overnight classified repository for AFRC and AMC transient aircraft on Pope Field. Storage space is very limited, however the Command Post may assist other AF units requiring classified storage in locating/procuring storage on Ft. Bragg as appropriate.

3.6. Classified Meetings and Conferences.

3.6.1. The 440 AW/CC delegates the authority to certify classified conference areas to 440 AW/IP. Notify the IP office of any classified meetings and schedule a site survey one week prior to the meeting. The following procedures must also be accomplished when hosting classified meetings:

3.6.1.1. Verify security clearances on attendees prior to any classified briefings or discussions.

3.6.1.2. Ensure the door to the discussion area is closed and someone is posted outside the door if sound attenuation and unauthorized entry is not adequate and cannot be controlled.

- 3.6.1.3. Ensure the briefing is kept to need-to-know for those in attendance.
- 3.6.1.4. Ensure classified is kept under constant surveillance. Use of classified cover sheets is required when material is removed from secure storage.
- 3.6.1.5. Return all classified material/information to secure storage when not under personal observation and control.
- 3.6.1.6. Note taking or electronic recording during classified sessions shall be permitted only when it is determined by the host that such action is necessary to fulfill the U.S. Government purpose for the meeting.
- 3.6.1.7. Classified waste must be destroyed using approved methods (burning, melting, pulping, pulverizing and cross-cut shredding).
- 3.6.1.8. Ensure that classified documents, recordings, audiovisual material, notes and other materials created, distributed or used during the meeting are controlled, safeguarded and transported as required by this instruction and DoDM 5200.01 Vol 1-4, *Information Security Program*.
- 3.6.1.9. Cellular phones, two-way radios, two-way beepers, and other electronic equipment that can receive and transmit a signal are prohibited in all offices and areas where classified and sensitive information may be discussed. 440 AW/CF will determine which work areas are affected and implement this requirement accordingly. Owners of designated areas should make every effort to inform personnel of the prohibited (unless otherwise approved) use of electronic equipment, to include but not limited to posting signs and visual aids and including the information in briefings/training, etc.

3.7. Post visual aids at all machines (to include fax machines) approved for classified reproduction. At a minimum, post visual aids at all copy machines not authorized for classified reproduction.

4. Storage of Classified Materials (Reference DoDM 5200.01 Vol 3, Enclosure 3).

4.1. Secure storage rooms containing open stored classified material, equipment or hardware built after 1 October 1995 must have two levels of detection alarm operating when appropriately cleared attendants are not present. 440 AW/IP will determine whether open or unattended storage areas provide adequate protection for classified material.

4.1.1. 440 AW/IP must send requests to waive any provisions of DoDM 5200.01 Vol 1-4 and AFI 31-401 to HQ AFRC/IP for concurrence. Post the storage facility approval notices/letters inside the approved area.

4.2. Prior to storing classified information in a vault or secure room, 440 AW/IP will coordinate a survey of the facility with the Fort Bragg, Directorate of Emergency Services (DES) (Physical Security), Directorate of Public Works (DPW) or Army Corps of Engineers (engineer support), and 440th Communications Flight to determine if the vault or secure room meets the construction and communication requirements outlined in DoDM 5200.01 Vol 3, Appendix to Enclosure 3 and all other requirements of DoDM 5200.01 Vol 3 and AFI 31-401 for the storage of classified information. If the facility meets requirements, 440 AW/IP, may approve the facility for storage of classified information. If the facility does not meet requirements, consider alternate or compensatory security controls in accordance with

DoDM 5200.01 Vol 3 and Mil Handbook 1013/1A. Re-evaluate all secure storage rooms and vaults every 5 years and accomplish new approval letter and/or waiver requests. Once 440 AW/IP certifies the room meets DoDM 5200.01 Vol 3 requirements the owning commander or Staff Agency Chief must approve it for open storage of classified.

4.3. Equipment Designations and Combinations. Personnel having the combination will be recorded on SF 700, Security Container Information. An additional SF 700 may be necessary for containers with more than five users.

4.4. Retention of Classified Records. Annual cleanout day will be accomplished in the month of January.

4.5. Methods and Standards.

4.5.1. For a listing of National Security Agency (NSA) evaluated and approved destruction devices see Annex B to NTISSI No.4004.

4.5.2. Post visual aids at shredders approved and not approved for destruction of classified.

5. Transmitting/Transporting/Destruction of Classified Information.

5.1. Personnel who are sending/receiving classified materials through a contract carrier (example: FEDEX, UPS etc) mail are cautioned that these carriers deliver directly to the addressee. Sender must ensure the material is delivered to personnel with the appropriate clearance and who have the ability to protect the material.

5.2. The USM will ensure procedures are established in their unit operating instruction on how to properly process and secure accountable first class mail received through 440th Communication Flight (CF).

5.3. The USM must ensure a courier briefing and acknowledgement statement are accomplished prior to issuing DD 2501, *Courier Card*, or letters. A copy of the courier briefing must be maintained in the Security Manager's Book, Tab 9. A copy of the briefing can be obtained from the 440 AW/IP EIM site.

5.3.1. DD 2501 can be obtained from the 440 AW/IP. The USM will annotate the card number and expiration date "Not to exceed (1) one year" in paragraph 4 of the Courier Briefing and Acknowledgement Statement. DD Form 2501 is accountable and must be maintained by the USM when individuals are not hand carrying classified information. When expired or no longer required, the USM will destroy the Card and email IPO with the date the card was destroyed.

5.3.2. Supervisor verbal authorization is required prior to hand carrying classified information to and from activities on Ft. Bragg. A DD Form 2501 or courier authorization designation memorandum is not required.

5.3.2.1. When classified material is hand carried on Ft Bragg (outside the unit or activity), a briefcase may serve as the outer wrapper. The inner envelope will be marked with the classification of the information, to include the unit address.

5.3.2.2. When hand carrying classified materials while traveling aboard commercial aircraft, use the procedures as outlined DoDM 5200.01 Vol 3.

5.3.2.3. Incorporate into the internal operating instruction to ensure only properly cleared individuals sign for incoming FedEx, UPS etc (or any contract carrier), registered mail, first class mail with caveat "Return Service Requested", and Postal Service Express mail shipments. An AF Form 12, Accountable Container Receipt or AF Form 310, Document Receipt and Destruction Certificate, must be completed anytime the material is transferred to a recipient not shown on the material's distribution. In addition, when using FedEx (or other contract carrier), registered mail, first class mail with caveat "Postmaster Do Not Forward," and Postal Service Express mail to send outgoing mail, personnel must verbally indicate whether the mail piece contains classified material to allow the Official Mail Center (OMC) to verify delivery. (Reference AFI 24-201, 7.8.1).

5.3.2.4. Bulk classified material destruction. Ft Bragg facilities for the destruction of classified and controlled sensitive information are at Bldg C-1629 on Ardennes Street. Hours of operation are Tuesday, Wednesday and Thursday by appointment only. Call 910-432-2488 and leave a message. Your call will be returned with a date and time to meet the classified destruction request.

5.3.2.5. In case of fire, natural disaster or civil disturbance (if time permits before evacuation of an area). Secure classified material in a vault or security container within the immediate area. Personnel will not risk injury or loss of life to secure classified material. If classified material cannot be properly stored, personnel will evacuate the area to the limits established by emergency response forces. Immediately after the emergency, personnel will return to their area and check for unsecure classified material. If material is missing, inadvertent access or compromise is suspected, the custodian will comply with AFI 31-401 Chapter nine.

5.4. Annual classified "Clean-out" for Air Force tenant units serviced by the 440 AW/IP office will be in the month of January of each year.

6. Training.

6.1. As a minimum, training documentation must include the trainee's name and grade, type of training (initial, refresher, or specialized), date of training, and a specific list of completed training subjects and tasks.

6.2. 440 AW/IP ensures primary and alternate security managers are trained within 90 days of appointment. Security Managers receive documentation of training. Security Managers are responsible for providing information security program training to their units.

6.3. Continuing and Refresher Training. USMs ensure this training is accomplished and documented.

7. Security Incidents.

7.1. 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. The commander or staff agency chief of the activity responsible for the security incident will appoint an inquiry official to conduct a preliminary inquiry.

7.1.1. The preliminary inquiry official will be appointed within three working days of the incident's discovery and report to 440 AW/IP with a copy of the appointment memorandum.

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

7.1.3. Inquiry officials will coordinate their actions with 440 AW/IP and the servicing staff judge advocate's office.

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

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

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

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

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

7.1.6. 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.

7.1.7. If the inquiry reveals suspected unauthorized disclosure to the public notify HQ AFRC/IP through CIP channels. Classify security incident notices, memorandums, and reports according to the classified source from which they are derived. Refer to DoDM 5200.01 Vol 3, Enclosure 6. Specifically address:

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

7.1.7.2. Was classified information compromised?

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

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

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

7.1.7.6. To what extent was the compromised information disseminated?

7.1.7.7. Was the information properly classified?

7.1.7.8. Was the information officially released?

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

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

7.1.8. Damage Assessment.

7.1.8.1. 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.

7.1.8.2. The OCA must:

7.1.8.2.1. 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.

7.1.8.2.2. Set-up damage assessment controls and procedures.

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

7.1.9. Formal Investigation.

7.1.9.1. 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.

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

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

7.1.9.2.2. 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.

7.1.9.2.3. The investigative official must be a commissioned officer, senior NCO (E-7 and above), or a civil service employee equivalent (GS-9 and above) processing the appropriate security clearance.

7.1.9.2.4. Appointing Authorities will not appoint an investigative official who is retiring, separating, or being reassigned within 120 days.

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

7.1.10. Management and Oversight.

7.1.10.1. The inquiry/investigative official will route the completed report through 440 AW/IP for review before forwarding it to the appointing authority.

7.1.10.2. The appointing authority will:

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

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

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

7.1.10.2.4. Forward a copy of the completed report to the IPO identifying corrective actions taken.

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

7.1.11. The 440 AW/IP will:

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

7.1.11.2. Monitor the status of security incidents.

7.1.12. Inquiry/investigative officials must complete inquiry/investigations within 30 duty days from appointment. 440 AW/IP will retain a copy of the investigation.

8. Personnel Security.

8.1. Types and Scope of Personnel Security Investigations. The scope of each type of personnel security investigation is listed in AFI 31-501.

8.1.1. National Agency Check plus Inquiries (NACI). NACIs are required on all civilian employees entering government employment and assigned to nonsensitive positions. NACIs are also conducted on contractors requiring access to the Air Force Unclassified but Sensitive Internet Protocol (IP) Router Network (NiPRNET).

8.1.2. National Agency Check, Local Agency Checks and Credit Check (NACLIC). NACLICs are required for military access to Secret information.

8.1.3. Access National Agency Check with Written Inquiries and Credit Check (ANACI). ANACIs are required for civilian employees' initial secret security clearances or assignment to non-critical sensitive positions.

8.1.4. Single Scope Background Investigation (SSBI). SSBIs are required for access to TOP SECRET, Sensitive Compartmented Information (SCI), special sensitive positions and for critical sensitive positions. This investigation is for civilians and service members.

8.1.5. Periodic Reinvestigation (PR). PRs are investigations conducted for the purpose of updating a previously completed background investigation. A PR for a SSBI is considered a SBPR and is required every 5 years from the date of the last investigation. A PR for a NACLIC is considered a PRS and is required every 10 years from the date of the last investigation. There is no PR requirement for NACIs.

9. Security Clearance.

9.1. Interim Security Clearance. Commanders may grant interim security clearance for access to Top Secret and Secret information IAW AFI 31-501.

9.2. Interim Top Secret security clearances:

9.2.1. Favorable NACI, NACLIC or ANACI completed.

9.2.2. Consult the Joint Personnel Adjudication System (JPAS) to determine the existence of a favorable NACI, NACLIC or ANACI. The investigation is acceptable if there is no break in service over two years.

9.2.3. Favorable review of personnel security questionnaire.

9.2.4. Favorable review of local personnel records, installation and/or military police records, medical records, and other security records, as appropriate.

9.2.5. SSBI package has been submitted to OPM for scheduling by an authorized requestor.

9.3. Interim Secret security clearances:

9.3.1. Favorable review of personnel security questionnaire.

9.3.2. Favorable review of local personnel records, installation and/or military police records, medical records, and other security records, as appropriate.

9.3.3. NACLIC or ANACI has been submitted to OPM for scheduling by an authorized requestor.

9.4. Interim access for individuals requiring NACIs. Since there is no clearance granted off the NACI investigation, there is no interim granted for this investigation. However, JPAS will reflect IT-III access after the following:

9.4.1. Favorable review of personnel security questionnaire.

9.4.2. Favorable review of local personnel records, installation and/or military police records, medical records and other security records, as appropriate.

9.4.3. NACI has been submitted to OPM for scheduling by an authorized requestor.

10. Requesting Personnel Security Investigations.

10.1. The AF Form 2583, Requester for Personnel Security Action will be the only form required in requesting a Personnel Security investigation.

10.1.1. Once the local files check is completed, the USM will deliver the request to the 440 AW/IP.

10.1.2. The Personnel Security Specialist will create an application in the Electronic Questionnaire for Investigations Processing (e-Qip) and email the instructions to the service member and the USM.

10.1.3. Once the subject completes the application and sends it back to the 440 AW/IP, it will be validated. If there are corrections to be made, it will be set back to the subject to make the required adjustments.

10.1.4. Once all corrections are made, signature pages will be forwarded to 440 AW/IP at which time the completed package will be sent electronically to OPM for scheduling.

10.2. For ANACIs, subjects must also turn in a copy of their resume and an OF 306. At that time, their fingerprints will be electronically taken and also sent to OPM to marry up with their investigative package.

10.3. For NACIs, subjects must also turn in a copy of their resume and an OF 306. At that time, their fingerprints will be electronically taken and also sent to OPM to marry up with their investigative package.

10.4. There are no additional requirements for SBPRs or PRs.

11. Air Reserve Technicians. Personnel designated as Air Reserve Technicians (ARTs) are required to maintain an ANACI.

12. The Joint Personnel Adjudication System (JPAS). JPAS is the Department of Defense (DoD) personnel security clearance and access database. It facilitates personnel security management for the DoD Central Adjudication Facilities (CAF), Air Force Central Adjudication Facilities (AFCAF), security managers and offers both non-SCI and SCI functions. JPAS is the primary source for determining investigative data/status of investigations on individuals in the DoD.

13. Security Information Files (SIFs). A SIF is a collection of documents generated as a result of the discovery or development of unfavorable information, which brings into questions a person's continuing eligibility for a security clearance or access to SCI. It may be established by a commander, civilian equivalent, or by AFCAF.

13.1. If the Commander is generating the SIF, it will normally happen within 20 days of receipt of unfavorable information. However, if the commander has sufficient reason to doubt the validity of unfavorable information, the decision to establish a SIF and notification to the AFCAF may be extended up to 45 days. A SIF will be established immediately if SCI access is involved.

13.2. The commander must notify the individual with the establishment of the SIF annotating whether the access to classified information has been suspended. See template letter located on the 440 AW/IP EIM site.

13.3. If the SIF is an AFCAF generated SIF, the commander will be notified of such action and subject will have 60 days to reply to the SIF.

14. Security Clearance Reinstatement. An individual's commander may request reinstatement of their security clearance 12 months after the effective date of revocation or denial or decision of the PSAB, whichever is later. Requests should be sent to the AFCAF with the commander's recommendation for approval. The commander recommends reinstatement and includes an explanation on how the individual's behavior has improved and the appropriate documentation corresponding to the reason(s) for the denial or revocation. The documentation required depends on the reason(s) involved, such as, evaluation for mental health issues, evaluation for drug or alcohol abuse; or current financial statement(s).

15. Industrial Security.

15.1. The 440 AW/IP is designated to perform industrial security oversight for contractor operations.

- 15.2. 440 AW/IP conduct security reviews for cleared facilities and visitor groups at least once every 12 months or as determined by the CIP providing frequency is not less than stipulated in DOD 5220.22-M or 5220.22-R.
- 15.3. Contractor home office facilities will appoint a contractor security representative(s) in writing and a copy is kept in the USM handbook for all contracts involving classified.
- 15.4. DD Form 254, Block 13, Security Guidance, include and show coordination of the system program director or project manager.
- 15.5. Integrated and National Industrial Security Program Operating Manual (NISPOM) Visitor Group personnel attend initial, refresher and annual training provided by contractor security representative(s). Contractor security representative(s) will document contractor visitor group personnel who have completed training.
- 15.6. Contractor management officials for NISPOM Visitor Groups are responsible for ensuring contract personnel satisfy NISPOM training requirements.
- 15.7. 440 AW/IP will determine the designation of Air Force contract visitors.
- 15.8. For Air Force tenant units on Ft Bragg, the program manager, project manager, Air Force Activity, or unit security manager will notify the 440 AW/IP in writing upon contract completion or termination.
- 15.9. A signed copy of the Visitor Group Security Agreement (VGSA) will be maintained by the 440 AW/IP.
- 15.10. NISPOM Visitor Groups will conduct self-inspections of their security programs IAW Air Force Activity checklist and document the self-inspection.

NORMAN R. HAM, JR., Brig Gen, USAFR
Commander

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

AFI 31-401, *Information Security Program Management*, 1 November 2005
AFI 31-401, *Personnel Security*, 28 March 2006
AFI 31-601, *Industrial Security*, 8 August 2003
AFI 33-129, *Web Management and Internet Use*, 3 February 2005
AFI 33-322, *Records Management Program*, 7 October 2003
AFI 33-332, *Privacy Act Program*, 29 January 2004
AFI 33-364, *Records Disposition—Procedures and Responsibilities*, 22 December 2006
AFMAN 33-363, *Management of Records*, 1 March 2008
T.O. 00-20F-2, *Air Force Technical Order System*, 15 October 2006
DOD 5200.01, *Air Force Guidance Memorandum (AFMG)*, DOD Information Security Program Volumes 1-4
DOD 5200.2-R, *Personnel Security Program*, 1998
DOD 5200.22-R, *Industrial Security*, January 1995

Abbreviations and Acronyms

AFI—Air Force Instruction
AFMAN—Air Force Manual
AFPD—Air Force Policy Directive
AFSC—Air Force Specialty Code
AFRC—Air Force Reserve Command
CIP—Chief Information Protection
DoD—Department of Defense
DoDD—Department of Defense Directive
DoDI—Department of Defense Instruction
DoDM—Department of Defense Manual
FOIA—Freedom of Information Act
FOUO—For Official Use Only
HQ USAF or HAF—Headquarters Air Force, includes the Secretariat and the Air Staff
IA—Information Assurance
IP—Information Protection

LIPME—Local Information Protection Management Evaluation

MAJCOM—Major Command

MICT—Management Internal Control Toolset

NISPOM—National Industrial Program Operating Manual

OI—Operating Instruction

OPR—Office of Primary Responsibility

SAV—Staff Assistance Visits

USAF—United States Air Force

USM—Unit Security Manager

VGSA—Visitor Group Support 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 **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. Controll 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.

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.