

**BY ORDER OF THE COMMANDER  
94TH AIRLIFT WING**

**94TH AIRLIFT WING INSTRUCTION 31-401**

**11 MARCH 2014**



**Security**

**INFORMATION SECURITY PROGRAM  
MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available at [www.e-publishing.af.mil](http://www.e-publishing.af.mil) for downloading or ordering.

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

---

OPR: 94 AW/IP

Certified by: 94 AW/CC  
(Col Timothy E. Tarchick)

Supersedes: 94AWI31-401, 1 February 2008

Pages: 21

---

This instruction implements Air Force Instructions (AFI) 31-401, *Information Security Program Management*; AFI 31-501, *Personnel Security Program Management*; and AFI 31-601, *Industrial Security Program Management*. Use this instruction with Executive Orders (EO) 12829, *National Industrial Security Program*; 12968, *Access to Classified Information*; 13526, *Classified National Security Information* and Department of Defense (DOD) 5200.1-R, *Information Security Program*; 5200.2-R, *Personnel Security Program*; and 5220.22-M, *National Industrial Security Program Operating Manual*. This instruction will assist in better understanding roles in managing and safeguarding classified information and sensitive unclassified programs. This is accomplished by encompassing the tenets of the various security programs into a comprehensive but manageable program that meets both mobility and national security requirements. This instruction applies to all members assigned at Dobbins Air Reserve Base. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change for Publication*; route AF Form 847 from the field through major command (MAJCOM) publications/forms manager. 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 the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afirms/afirms/afirms/rims/cfm>.

**SUMMARY OF CHANGES**

**This document is substantially revised and must be completely reviewed.**

1.1.	Role of the ISPM. ....	4
1.2.	ISPM Responsibilities. ....	4
1.3.	ISPM Support Staff. ....	5
<b>Chapter 2—INFORMATION SECURITY PROGRAM</b>		<b>6</b>
2.1.	Security Manager Appointments. ....	6
2.2.	Security Manager Training. ....	6
2.3.	Security Manager Meetings. ....	6
2.4.	Security Manager Responsibilities. ....	7
2.5.	Information Security Program Reviews (ISPR). ....	8
2.6.	Preliminary Inquiries and Formal Investigations. ....	8
2.7.	Additional ISPM Responsibilities. ....	9
2.8.	ISPM Responsibilities for DOD Unclassified Controlled Nuclear Information (DOD UCNI). ....	9
2.9.	Protecting Classified Material on Aircraft. ....	9
2.10.	Equipment to Process or Destroy Classified Material. ....	10
<b>Chapter 3—PERSONNEL SECURITY PROGRAM</b>		<b>11</b>
3.1.	Program Management. ....	11
3.2.	Personnel Security Investigations (PSIs). ....	11
3.3.	Security Information Files (SIF's). ....	12
3.4.	Central Adjudication Security Personnel Repository (CASPR). ....	13
3.5.	Joint Personnel Adjudication System (JPAS). ....	13
3.6.	ISPRs. ....	13
3.7.	Position Coding. ....	14
3.8.	Denied or Revoked Clearance Eligibility. ....	15
<b>Chapter 4—INDUSTRIAL SECURITY PROGRAM</b>		<b>16</b>
4.1.	Overview. ....	16
4.2.	Program Management. ....	16
<b>Chapter 5—SECURITY EDUCATION AND TRAINING</b>		<b>17</b>
5.1.	Overview. ....	17
5.2.	Formal Training for Information Security Specialists. ....	17
5.3.	Training Cycles and Requirements. ....	17
<b>Chapter 6—SPECIAL INSTRUCTIONS</b>		<b>19</b>

6.1. Classified Messages. .... 19

6.2. Classified material must be under the control of the individual that meets the requirements IAW DOD 5200. .... 19

6.3. Classified material will not be reproduced without the approval of the originating authority and/or the commander depending on the circumstances. .... 19

6.4. Personnel will annotate the master copy of documents with special dissemination and reproduction limitations indicating the distribution and the amount of copies reproduced. .... 19

6.5. All accountable mail will be handled as classified information until the classification is determined. .... 19

6.6. Include emergency protection/removal procedures in operating instructions and practice them. .... 19

6.7. Each unit will designate one day each year for the review and destruction of classified material in their custody. .... 19

6.8. Each unit will assess the need to establish and keep secure conference and classified training facilities. .... 19

**Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 20**

## Chapter 1

### INFORMATION SECURITY PROGRAM MANAGER (ISPM)

#### 1.1. Role of the ISPM.

1.1.1. The installation Chief of Information Protection (IP) is designated as the Information Security Program Manager (ISPM). The day-to-day program management responsibilities are delegated through the Chief of Information Protection to subordinate staff members.

1.1.2. The information security program outlines methods for transmitting classified information, safekeeping and storage criteria, specific marking requirements, disposal and destruction, access, dissemination, accountability and control, reproduction of classified, classification and declassification procedures, and preliminary inquiries or formal investigations of information security incidents. Also covered is the requirement and procedures for identifying, marking and protection of DOD UCNI. Management of the information security program encompasses two other closely related programs—the Personnel and Industrial Security Programs.

1.1.3. The purpose of the personnel security program is to ensure security clearances and access authorizations are only granted in the best interest of national security. This program addresses all personnel security investigations, clearances, access authorizations, investigations for granting unescorted entry to restricted areas, and security information files (SIFs). This program is our internal defense in the fight against terrorism as it provides the initial and continuing suitability screening for all Air Force personnel.

1.1.4. Perhaps the least understood of these programs is the Industrial Security Program. The objective is to assure Department of Defense classified information entrusted to government affiliated contractors is protected against unauthorized disclosure. It involves security supervision of contractors, inspection and oversight responsibilities, classified contracts, visitor controls, facility security clearances and classification guidance. Most AF contractors are integrated into the sponsoring unit and receive security inspections and oversight as part of the unit.

**1.2. ISPM Responsibilities.** Each program is very involved and requires continuous guidance and support. Personnel assigned to the Information Security function of 94 AW/IP assist in fulfilling the following ISPM responsibilities.

1.2.1. Managing the overall installation Information, Personnel, and Industrial Security Programs.

1.2.2. Ensuring appointed security managers for units or staff agencies are quickly and completely trained to perform their duties.

1.2.3. Managing the information security training program and providing technical guidance to unit or staff agency security managers.

1.2.4. Conducting security manager meetings. Preparing and distributing minutes of each meeting to all security managers and their commander, equivalent or staff agency chief for use in their security programs.

1.2.5. Providing indoctrination training to Original Classification Authorities (OCAs) and designated activity personnel involved in the preparation of security classification guides or guidance.

1.2.6. Conducting information security program reviews (ISPR).

**1.3. ISPM Support Staff.** Manpower is allocated to support the Information, Personnel and Industrial Security Programs.

## Chapter 2

### INFORMATION SECURITY PROGRAM

#### 2.1. Security Manager Appointments.

2.1.1. Each unit commander or equivalent or staff agency chief, will appoint a full-time and an alternate security manager. The appointing official provides a copy of the appointment letter to the information security section for their files. Units having fewer than 25 personnel may have only one full-time security manager. Security managers must have a SSBI, NACLIC or ANACI personnel security investigation or reinvestigation completed or in process. If in process, the security manager must have had previous clearance eligibility to access the Joint Personnel Adjudication System (JPAS).

2.1.2. Small organizations may have joint or mutual security managers when they fall under the jurisdiction of a single commander. Examples include such organizations as the Safety Office, Historian or Chaplain who are often grouped together under the Wing Commander's program.

2.1.3. Tenant USAF units may normally participate in the programs. Usually there is only one operational ISPM per installation. If someone else is claiming ISPM responsibilities, contact the ISPM for guidance and coordinate their participation through Wing Plans and Logistics Readiness.

2.1.4. The 94 AW/IP retains records of appointments and tenant participation and support.

#### 2.2. Security Manager Training.

2.2.1. The ISPM is responsible to provide formal training to security managers as soon as possible after their appointment or within 90 days, whichever is sooner. Every day of delay has adverse impact on their unit, and ultimately the program.

2.2.2. Training is based on the requirements of, DOD 5200.1-R, DOD 5200.2-R, AFI31-401, AFI 31-406, *Applying North Atlantic Treaty Organization (NATO) Protection Standards*; and AFI 31-501. Additional training will be based on need and capability.

2.2.3. Although the information security program interfaces with other security-related programs, such as COMSEC, COMPUSEC, EMSEC, OPSEC, etc., 94 AW/IP is not normally responsible for providing related training.

2.2.4. The 94 AW/IP documents and records security manager training.

#### 2.3. Security Manager Meetings.

2.3.1. The 94 AW Chief of Information Protection serves as Chairperson and approves the agenda for these meetings.

2.3.2. Attendance by all primary security managers is mandatory. Alternates attend in the absence of the primary. If neither the primary nor alternate is available, a representative attends.

2.3.3. The meetings provide a forum for interaction between security managers and resolution of common problems.

2.3.4. Meeting minutes are published, recorded and distributed to all agencies by the information security section.

## **2.4. Security Manager Responsibilities.**

2.4.1. Provides advice and assistance to the unit commander or equivalent, or staff agency chief and personnel assigned to the activity.

2.4.2. Develops and implements internal security operating instructions.

2.4.3. Ensures assigned personnel fulfill security education training requirements outlined in DOD 5200.1-R and AFI 31-401.

2.4.4. Monitors internal information security self-inspections. Ensures self-inspections are conducted semi-annually. Reviews reports and ensures timely corrective actions are taken. (Security managers do not inspect their own functions.)

2.4.5. Participates in security managers' meetings and training. Addresses problem areas and assists other security managers in resolving similar situations.

2.4.6. Reviews and processes challenges to classification decisions.

2.4.7. Manages JPAS within the unit, to include a frequent check for notifications and changes.

2.4.8. Notifies unit personnel when their Periodic Reinvestigation (PR) is due.

2.4.9. Monitors the Information, Personnel, and Industrial security programs. Specific responsibilities are outlined in the Security Manager's Handbook.

2.4.10. Debriefs personnel of their continued responsibility to safeguard classified after access to the information has been terminated. Debriefings are documented using AF Form 2587, *Security Termination Statement*, which is maintained on file for two years. Military members and civilian employees are debriefed under the following conditions:

2.4.10.1. When discharged, retired, or employment is terminated.

2.4.10.2. When access to a Special Access Program is terminated, i.e., SCI, NATO, CNWDI, or SIOP.

2.4.10.3. When a Security Information File (SIF) is established, only if access to classified information is withdrawn.

2.4.11. Maintains a current Security Manager Book with the following contents:

2.4.11.1. Security Manager Appointment Letter

2.4.11.2. Unit Security Operating Instruction

2.4.11.3. Last 2 semi-annual security self-inspection reports

2.4.11.4. Security Manager meeting minutes

2.4.11.5. Information letters

2.4.11.6. List of security containers (make, model, type of lock) and locations

2.4.11.7. Program review reports

2.4.11.8. Signed annual information security training plan

2.4.11.9. For units with security containers, TO 00-20F-2.

2.4.11.10. Copy of the annual review of the Unit Manning Document.

2.4.12. Informs 94 AW/IP of all classified contractors working within their area. Once the contract has been completed they will notify 94 AW/IP.

## **2.5. Information Security Program Reviews (ISPR).**

2.5.1. The ISPM ensures the Information Security section conducts ISPRs of all serviced activities. If the activity stores or processes classified information, the program review is conducted annually. If the activity doesn't store or process classified information the program review is every two years.

2.5.2. Reviews are "staff assistance" oriented to identify noteworthy and problem areas.

2.5.3. The ISPR examines elements of the Information, Personnel and Industrial programs. Reviews may be based on a random sampling, but must be extensive enough to determine overall status of programs run by the security managers. They are not compliance inspections and are not assigned ratings.

2.5.4. The Chief of Information Protection signs the report before it is forwarded to the visited activity for their review and corrective action, but may delegate the responsibility. There is no mandate that the visited activity respond to the report, unless requested by 94 AW/IP. The 94 AW/IP retains the last 2 copies of the ISPRs.

## **2.6. Preliminary Inquiries and Formal Investigations.** The 94 AW/IP has a detailed handbook for inquiry officials if they desire to learn more.

2.6.1. Initial notification of security incidents is made to 94 AW/IP representative by the end of the first duty day after discovery.

2.6.2. When an incident occurs, a preliminary inquiry must be conducted to determine whether a compromise of classified material has occurred and to properly categorize the incident. A preliminary inquiry official (commissioned officer, senior noncommissioned officer, or DOD civilian, usually GS-9 or above) is appointed by the commander, equivalent, or staff agency chief. The ISPM is responsible to brief the inquiry or investigation official and assist as needed.

2.6.3. Security incidents are categorized as follows:

2.6.3.1. Compromise

2.6.3.2. Probable Compromise

2.6.3.3. Security Deviation

2.6.4. The ISPM or his or her staff monitors the inquiry's progress to ensure it is completed in a timely manner (normally 10 workdays, but some may take as long as 30 days).

2.6.5. If the inquiry determines a compromise occurred and the probability of damage cannot be ruled out, a formal investigation is initiated by the appointing authority unless the appointing authority believes no further information will be developed and uses the

preliminary inquiry to close the incident. The originating agency of the classified material must be notified if compromise or probable compromise occurred.

2.6.6. The 94 AW/IP will retain records and forms as required.

## **2.7. Additional ISPM Responsibilities.**

2.7.1. Provides technical guidance to Original Classification Authorities (OCAs).

2.7.1.1. Within the Air Force, OCAs are identified by the Secretary of the Air Force or the Administrative Assistant to the Secretary by position, not individual name. The incumbent of the position (identified on an OCA list at the AFSFC web site) may exercise the authority only after completing OCA training.

2.7.1.2. The only current OCA on Dobbins ARB, GA is 22 AF/CC. If 22 AF/CCV will have to perform OCA duties in the absence of 22 AF/CC, training must be conducted. The list of OCAs is available at the AFSFC web site.

2.7.2. The ISPM or his or her staff provides advice on preparation of classification guides. The ISPM is in a position to oversee many of the original decisions or derivative determinations. The information security section should maintain copies of the latest classification guidance available which may impact the wing's mission. Base agencies will often seek technical guidance in helping make accurate derivative classification decisions. The information security section should be well versed in this area and know where to obtain the applicable classification guidance. The information security section should also keep DOD 5200.1-I, *Index of Security Classification Guides*, available for review.

**2.8. ISPM Responsibilities for DOD Unclassified Controlled Nuclear Information (DOD UCNI).** The installation commander and 94 AW/IP Chief are designated by AFI 31-401 as UCNI Officials. For the greater part, ISPM responsibilities are generally to educate the base populace on protection measures for DOD UCNI and reviewing DOD UCNI safeguarding measures during information security program reviews. Each unit/staff agency should, in turn, include a review of DOD UCNI safeguarding procedures during their semiannual security inspections.

2.8.1. Specific responsibilities are:

2.8.1.1. Identify information meeting definition of UCNI.

2.8.1.2. Determine criteria for access to UCNI and approve special access requests.

2.8.1.3. Approve or deny the release of UCNI information.

2.8.1.4. Ensure all UCNI information is properly marked, safeguarded, transmitted, and destroyed.

2.8.1.5. Document decisions and report them through command ISPM channels to HQ USAF/XOS-FI. RCS Number DD-C3I (AR)1810 applies to this data collection.

## **2.9. Protecting Classified Material on Aircraft.**

2.9.1. Aircraft commanders (owners/users) are responsible for the protection of classified material and components aboard their aircraft whether on a DOD facility, at a civilian airfield, or when stopping in foreign countries IAW DOD 5200.1-R, paragraph C6.3.9.

Aircraft commanders should consult with the 94 AW/IP Chief for assistance in complying with these requirements.

2.9.1.1. To provide security-in-depth for classified components and material on aircraft, park the aircraft in an established restricted area.

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

2.9.1.3. If the aircraft cannot be locked, place all removable classified material (e.g., paper documents, floppy disks, videotapes) in a storage container secured with a GSA-approved lock. The storage container must be a seamless metal (or similar construction) box or one with welded seams and a lockable hinged top secured to the aircraft. Hinges must be either internally mounted or welded. Containers installed for storage of weapons may also be used to store classified material even if weapons/ammunition are present, provided the criteria listed above have been met. Check the container every 12 hours for tampering.

2.9.1.4. If the aircraft cannot be locked and is not equipped with a storage container, place the removable classified in an approved security container. Contact 94 OG/OGA for proper courtesy storage of classified material. Classified components attached to the aircraft, do not have to be removed.

**2.10. Equipment to Process or Destroy Classified Material.** All units possessing shredders, facsimile machines, and copiers or other equipment approved for processing or destroying classified information and materials will report this equipment to 94 AW/IP as part of the classified container list. This equipment will be used jointly by all organizations in the information security program to reduce expense. The 94 AW/IP will provide a list of this equipment annually to all unit security managers. Units will inform 94 AW/IP of the need to purchase such equipment so the need to develop a central destruction facility may be continually assessed.

## Chapter 3

### PERSONNEL SECURITY PROGRAM

**3.1. Program Management.** The personnel security program is administered by the personnel security specialist. Requests for personnel security investigations, clearances, special access authorizations, and administrative withdrawal of personnel security clearances are monitored and processed through 94 AW/IP. The following is an overview of other major functions of the personnel security section.

3.1.1. **Technical Guidance.** Provides technical guidance and assistance to the installation commander, squadron commanders or equivalents, staff agency chiefs, security managers, and all other base personnel on matters involving personnel security.

3.1.2. **Joint Personnel Adjudication System (JPAS).** Manages the installation-wide application of user levels 5, 6, 7, 8, 9, and 10.

**3.2. Personnel Security Investigations (PSIs).** All requests for personnel security investigations go through the 94 AW/IP office. PSIs are conducted by the Office of Personnel Management (OPM) as a means of determining employment suitability as well as eligibility for access to classified information or unescorted entry into restricted areas.

3.2.1. As the point of contact for submitting PSI's, the personnel security section ensures all investigative forms are accurately completed. Once investigations are submitted they are monitored until closed. Investigations are tracked in JPAS and Central Adjudication Security Personnel Repository (CASPR).

3.2.2. When an investigation is completed, the AFCAF reviews the results to determine whether it is favorable or contains derogatory information. The AFCAF grants security clearance eligibility to the highest level possible based on the type of favorable investigation conducted. The following are the personnel security specialists' responsibilities relative to PSIs:

3.2.2.1. Process investigation requests to Office of Personnel Management (OPM). Assist unit/staff agency personnel with e-QIP and process their requests for personnel security investigations.

3.2.2.2. Provide guidance to the servicing CPF concerning investigation requests submitted to OPM.

3.2.2.3. Monitor opening transactions.

3.2.2.4. Maintain a wing tracking spreadsheet for activated investigations, security manager listing, required security manager training, SIF/SOR status.

3.2.2.5. Manage the JPAS program for all non-Sensitive Compartmented Information activities.

3.2.2.6. Monitors CASPR for security clearance status.

3.2.3. Periodic personnel security investigations (PSIs) and periodic reinvestigations (PRs) for access to classified information will be conducted as follows:

3.2.3.1. For secret access, initiate a periodic investigation 6 months before the last investigation is out of scope, i.e. 9.5 years from the close date.

3.2.3.2. For top secret, SCI-DCID 6/4 access, initiate a periodic investigation 6 months before the last investigation is out of scope, i.e. 4.5 years from the close date.

3.2.3.3. All investigations will be submitted through e-QIP.

3.2.3.4. The 94 AW/IP will initiate a SIF on any employee who fails to comply and submit their PSIs through e-QIP after the 3rd missed activation. The commander, equivalent, or staff agency chief will initiate progressive disciplinary action (i.e. LOC, LOA, LOR, Article 15, dismissal) on any employee who fails to comply and complete successive PSIs through e-QIP in the specified time.

**3.3. Security Information Files (SIF's).** A SIF is a temporary file used as a repository to maintain pertinent documents related to a case in which a person's trustworthiness, judgment, or reliability has been questioned. Investigations are initiated to support or resolve unfavorable information. The decision to establish a file is made either by the individual's commander, equivalent or staff agency chief due to behaviors identified in DOD 5200.1-R or by the Air Force Central Adjudication Facility (AFCAF) based on derogatory information uncovered during an investigation.

3.3.1. If the ISPM disagrees with a commander, equivalent or staff agency chief as to the appropriateness of establishing a file, the case is forwarded to the installation commander for resolution. Access to classified information and unescorted entry into restricted areas are normally suspended whenever a SIF is established; however, it is the unit commander, equivalent or staff agency chief's decision. If the adverse information involves a civilian employee, notify the civilian personnel flight. If the individual has access to SCI information, the Special Security Officer (SSO) is responsible for the SIF.

3.3.2. The personnel security section advises the ISPM on matters relating to the SIF establishment. SIF custodial responsibilities include:

3.3.2.1. Advising the installation commander and subject's commander, equivalent or staff agency chief of the contents of the file, including significant information placed in the file after it is established.

3.3.2.2. Safeguarding the file.

3.3.2.3. Recording all notifications, reviews, and other transactions occurring to the file during the entire life of the file.

3.3.2.4. Ensuring completeness of a SIF before sending it to the AFCAF for final adjudication. Information in the files includes, but is not limited to, the following:

3.3.2.4.1. AFOSI reports.

3.3.2.4.2. Local police reports.

3.3.2.4.3. Documents of administrative action.

3.3.2.4.4. Evaluation by base agencies. i.e., Security Forces, Social Actions, Staff Judge Advocate, Mental Health, etc.

3.3.2.4.5. Any other pertinent information relating to the case.

3.3.2.5. The ISPM, through the personnel security specialist, must take the following actions when establishing a SIF:

3.3.2.5.1. Notify the AFCAF and the installation commander of SIF establishment.

3.3.2.5.2. Ensure access to classified information and unescorted entry to restricted areas are suspended, if considered necessary by the subject's unit commander, equivalent or staff agency chief.

3.3.2.5.3. Provide the AFCAF timely status reports on open SIFs.

3.3.2.5.4. Maintain the SIF as outlined in AFI 31-501.

3.3.2.5.5. Destroy the file once the AFCAF completes the adjudication process.

3.3.3. Once a SIF/SOR is received from the AFCAF to suspend a security clearance notify 94 CF for termination of Local Area Network (LAN) and information technology systems. If a member needs continued access, the unit security manager must accomplish a network waiver.

**3.4. Central Adjudication Security Personnel Repository (CASPR).** CASPR is used by the AFCAF to notify our office of security clearance changes to personnel statuses, i.e., clearance granted, sent to due process, SIF, SOR, Denials and Revocations.

3.4.1. AFCAF generated Suitability's, SIF, SORs, Denials and Revocations will be sent through CASPR.

3.4.2. All responses/intents from the members will be processed through CASPR.

**3.5. Joint Personnel Adjudication System (JPAS).** JPAS is an on-line system that reflects current clearance eligibility and other pertinent data.

3.5.1. Information entered into JPAS by the AFCAF is immediately available to system users. JPAS provides a periodic update to the personnel data systems operated by AFPC, however JPAS is the only source for confirming clearance eligibility. Security managers and information and personnel security personnel are required to check JPAS for updates frequently and to update information in JPAS including in- and out-processing, PSI submission information, Non-disclosure agreements, US and NATO accesses.

3.5.2. JPAS use is restricted to the security community and security managers. JPAS accounts may be established for entry controllers also. Military members need a minimum of a current NACLC before the system will allow access. Civilian employees require a minimum of a current ANACI. The personnel security specialist maintains a list of all non-SCI installation authorized users. All JPAS users will accomplish Personal Identifiable Information (PII) training and will send their certificate to 94 AW/IP office to maintain. This is a one time requirement.

3.5.3. JPAS provides access to position access requirements, investigative and clearance eligibility data as well as records of select briefings/accesses such as Personnel Reliability Program, Critical Nuclear Design Information, and North Atlantic Treaty Organization access briefings.

**3.6. ISPRs.** While the personnel security section isn't normally manned to visit every agency during the information security program review, they should get out as often as possible, discuss

special interest items and changes with security managers, coordinate findings, and assist in making recommendations for improvement.

### 3.7. Position Coding.

3.7.1. Commanders are responsible for determining the appropriate code for the organization's manpower positions IAW AFI 31-501, *Personnel Security Management*, **Chapter 7**, para **7.2**

3.7.2. Position codes are assigned by the type of investigation required for mission purposes versus security clearance requirements. Positions must be coded with the appropriate investigative level. Investigation types and definitions follow:

3.7.2.1. Single Scope Background Investigation (SSBI) (**Code 5**): Initial investigation to access up to Top Secret, certain AFSCs and sensitive programs.

3.7.2.2. National Agency Check, Local Agency Checks and Credit (NACLIC) (**Code 6**): Initial investigation for access up to Secret for military and contractors. Required for military entry and retention.

3.7.2.3. Access National Agency Check and Inquiries (ANACI) (**Code 7**): Initial investigation for access to Secret for civilians.

3.7.2.4. National Agency Check Plus Inquiries (NACI) (**Code 8**): Required for entry to government service for civilians and federal employees in positions not requiring access to classified.

3.7.3. A corresponding code is assigned to the investigation type and reflected in both the Headquarters Air Force Manpower Data System and Unit Manpower Documents.

3.7.4. A select group of AFSCs have been designated with a mandatory SSBI requirement, e.g., Intelligence (14N); Pilots (11B/11F); Navigator (12B/12F), etc. There are also several sensitive programs that have been designated as a mandatory SSBI requirement, e.g., Presidential Support, PRP, SCI. Please refer to the mandatory AFSC list.

3.7.5. The 3-Star/Civilian Equivalent approval is required for additional SSBI requirements that fall outside the mandatory AFSC or program lists.

3.7.6. Positions designated for military deployments will be coded as a NACLIC, unless the position requires an SSBI based on day-to-day mission requirements. Commanders have authority to grant interim TS access for deployment purposes for 180 days, and can renew this access for extended deployments. An SSBI is not required in these instances.

3.7.7. Unit commanders, staff agency chiefs and section heads are required to conduct an annual review of their position codes in May and maintain a copy of the review in the security managers handbook.

3.7.8. Prior to allowing access to classified information, custodians of classified information must ensure military, civilians and contractors have the following:

3.7.8.1. Current eligibility as identified in JPAS. Current eligibility is defined as eligibility at the level required (top secret, secret, confidential) and the investigation is in scope. In scope means that the investigation is no more than 5 years old for top secret

and no more than 10 years old for secret and confidential. Document US Access levels in JPAS after NdA indoctrination.

3.7.8.2. Attestation for top secret is annotated on the NdA, block 11. The signed NdA and the indoctrination are documented in JPAS.

3.7.8.3. Need to know for official government business.

3.7.8.4. Current and required training to include initial or recurring information security training and unit/duty specific training.

3.7.9. Those granting access to classified information must gain the originator's approval before releasing the information outside the Executive Branch or as specified by the originator of the classified material.

**3.8. Denied or Revoked Clearance Eligibility.** When the AFCAF makes the final decision to deny or revoke a security clearance, commanders, staff agency chiefs and section heads will immediately evaluate the retention and employment policies for that member. Render a decision to retain, retrain, or release the member within 90 days. Ensure coordination with 94 FSS/DPC and or 94 FSS/DMP.

## Chapter 4

### INDUSTRIAL SECURITY PROGRAM

**4.1. Overview.** Classified contracts may involve research and development; installation, modification, and maintenance of weapons systems or communications systems; or installation and maintenance of systems that handle classified information. Whatever the involvement and whatever the type of contract, it is the 94 AW/IP Chief who represents the installation commander in the security supervision of the contractor operations for all except Special Access Programs (SAP) or Sensitive Compartmented Information (SCI) efforts.

**4.2. Program Management.** The initial steps are to review the DD Form 254, *Contract Security Classification Specification*, and discuss with the contractor, contracting officer, and program manager to determine the degree of involvement with classified information and degree of oversight required.

4.2.1. In some cases, contractor operations will only involve intermittent visits to the installation. The contractor is then told of the installation's policies regarding entry and exit, vehicle registration, alerts, personal identification, firearms and explosives, and procedures for entry into controlled and restricted areas.

4.2.2. In other cases, the contractor operations will occupy space on the installation. In these cases, 94 AW/IP must use knowledge of the contractor operations to determine the extent of security support required. Within the Air Force, we establish the contractor activity as a Visitor Group (VG). VGs are always under the security cognizance of the installation commander and are usually integrated into the security program of the unit that requires their services. This allows control and flexibility in dealing with the contractor. It also recognizes the way we do business with most contractors, i.e., their operations are merged with Air Force operations and it's not feasible to establish them as a separate operating entity.

4.2.3. The 94 AW/IP takes the following actions:

4.2.3.1. Performs initial visit to discuss the security agreement with the contractor.

4.2.3.2. Ensures the contractor knows what the security requirements are and what security support will be made available by the 94 AW/IP office.

4.2.3.3. Completes the security agreement and advises the contractor that they will be included in the host unit information security program review schedule. The 94 AW/IP staff do not conduct a separate ISPR for contractors integrated into a unit.

4.2.3.4. The ISPM and the information security section will be responsible to forward, retain and review all relevant contracts, forms, agreements, and inspections.

## Chapter 5

### SECURITY EDUCATION AND TRAINING

**5.1. Overview.** Security education is essential to prevent security violations. Make the training as interesting as possible. Periodicals and newsletters will help to fill the gap between training sessions.

5.1.1. The 94 AW/IP will ensure the base security education program is comprehensive and effective. Specific responsibilities include:

5.1.1.1. Developing local policy and providing guidance to base units/staff agencies pertaining to the security education program.

5.1.1.2. Developing security education products and disseminating them to base units/staff agencies.

5.1.1.3. Reviewing unit/staff agency security education programs during Information Security Program Reviews.

5.1.1.4. Ensuring security education receives appropriate emphasis in unit metrics and self-inspections.

5.1.2. Security education is directed in DOD 5200.1-R and AFI 31-401.

### **5.2. Formal Training for Information Security Specialists.**

5.2.1. Each year the service receives a limited number of formal training allocations for courses sponsored by DSSA. Courses offered are in-residence and web-based and designed to train security specialists. Some courses are funded by HQ AETC and others are unit funded. Available courses are listed on the DSSA web site. Correspondence courses are also available.

5.2.2. Air Force military, civilians, and contractors who perform security manager duties are strongly encouraged to participate in the DSSA courses.

### **5.3. Training Cycles and Requirements.**

5.3.1. Initial Training: All personnel will receive initial information security education at their initial assignment. If proof/documentation of training is not provided, the USM will ensure training is conducted and documented within 90 days of arrival on station or before accessing classified information, whichever is sooner. 94 AW/IP can assist USMs and supervisors and provides training materials specified below.

5.3.1.1. Personnel assigned in non-sensitive positions, i.e. no clearance required, will receive non-sensitive (unclassified) and NATO classified training.

5.3.1.2. Personnel assigned in critical-sensitive or non-critical sensitive positions, i.e. security clearance required and all military, will receive sensitive (classified) and NATO classified training.

5.3.2. Annual Training: All personnel will receive annual Information Protection training. Access this training through the Advanced Distributed Learning Service (ADLS) at <https://Golearn.csd.disa.mil>. This site can also be reached from within the Air Force Portal

Home Page/Top Viewed: Training section. Any member who does not currently have an ADLS account can establish one by visiting the web site.

5.3.3. Recurring Training: All personnel will receive recurring Information Protection training. The 94 AW/IP office has created a training power point which can be used for recurring training.

5.3.4. Specialized Training: All personnel who originally classify, derivatively classify, handle or store classified material as part of their duties must be appropriately trained. The 94 AW/IP can assist USMs and supervisors and provides appropriate training materials.

## Chapter 6

### SPECIAL INSTRUCTIONS

**6.1. Classified Messages.** Commander designated personnel are responsible for picking up incoming squadron classified messages, up to the Secret level, from the message center. Notify the 94 AW Command Post, the 94 AW Intelligence Officers or 94 AW/IP before picking up **Top Secret** messages. Classified messages received during non-duty hours will be delivered directly to 94 Command Post or 94 SFS. Authorized personnel will implement Chain of Custody for the classified message until the material is relinquished to the appropriate destination. All questions pertaining to the protection of classified material should be directed to 94 AW/IP, or refer to the directions given in DOD 5200.1-R and AFI 31-401.

**6.2. Classified material must be under the control of the individual that meets the requirements IAW DOD 5200.1-R and AFI 31-401 or material must be locked in the GSA approved security container with an XO-7 lock or higher if not in approved open storage.**

**6.3. Classified material will not be reproduced without the approval of the originating authority and/or the commander depending on the circumstances.**

**6.4. Personnel will annotate the master copy of documents with special dissemination and reproduction limitations indicating the distribution and the amount of copies reproduced.** Apply copy marking IAW DOD 5200.1-R and AFI 31-401.

**6.5. All accountable mail will be handled as classified information until the classification is determined.** The appropriate receipts and package IAW DOD 5200.1-R and AFI 31-401 will accompany classified material dispatched through Base Information Transfer System (BITS). The 94 AW members without proper authorization **will not** transport classified material off base. The member must be designated and trained as the official courier by the unit commander.

**6.6. Include emergency protection/removal procedures in operating instructions and practice them.**

**6.7. Each unit will designate one day each year for the review and destruction of classified material in their custody.**

**6.8. Each unit will assess the need to establish and keep secure conference and classified training facilities.** Coordinate through the 94 AW/IP office before beginning such projects.

TIMOTHY E. TARCHICK, Colonel, USAFR  
Commander

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

AFI 31-401, *Information Security Program Management*  
AFI 31-406, *Applying North Atlantic Treaty Organization (NATO) Protection Standards*  
AFI 31-501, *Personnel Security Program Management*  
AFI 31-601, *Industrial Security Program Management*  
DOD 5200.1-I, *Index of Security Classification Guides*  
DOD 5200.1-R, *Information Security Program*  
DOD 5200.2-R, *Personnel Security Program*  
DOD 5220.22-M, *National Industrial Security Program Operating Manual*  
DODD 5210.83, *Unclassified Controlled Nuclear Information (UCNI)*  
EO 12829, *National Industrial Security Program (NISP)*  
EO 12968, *Access to Classified Information*  
EO 13526, *Classified National Security Information*  
ISOO Directive Number 1, *Classified National Security Information*  
AFMAN 33-363, *Management of Records*

***Adopted Forms***

AF Form 847, *Recommendation for Change for Publication*  
DD Form 254, *Contract Security Classification Specification*

***Abbreviations and Acronyms***

**AFCAF**—Air Force Central Adjudication Facility  
**AFI**—Air Force Instruction  
**AFMAN**—Air Force Manual  
**AFOSI**—Air Force Office of Special Investigation  
**CASPR**—Central Adjudication Security Personnel Repository  
**COMSEC**—Communications Security  
**COMPUSEC**—Computer Security  
**EMSEC**—Emission Security  
**DOD**—Department of Defense  
**IP**—Information Protection  
**ISPM**—Information Security Program Manager

**JPAS**—Joint Personnel Adjudication System

**NATO**—Applying North Atlantic Treaty Organization

**OCA**—Original Classification Authorities

**OG/OGA**—Operations Group/Airfield Operations

**OPM**—Office of Personnel Management

**OPSEC**—Operations Security

**PSI**—Personnel Security Investigation

**SIF**—Security Information File

**SSO**—Special Security Officer

**UCNI**—Unclassified Controlled Nuclear Information