

31 July 1999



Information Security

**MANAGING THE INFORMATION SECURITY
PROGRAM**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFRC WWW site at <http://www.afrc.af.mil>. and the AFRCEPL (CD-ROM), published monthly.

OPR: 913 SFS/SFAI (Ms. Pearl Jonasz)
Supersedes 913 AGR 205-1, 1 April 1992

Certified by: 913 SPTG/CC (Col Dana S. Marsh)
Pages: 5
Distribution: F

This instruction implements Air Force Policy Directive 31-4. It provides guidance and designates responsibilities for the 913th Airlift Wing's Information Security Program (ISP) management. It applies to all base personnel at Willow Grove Air Reserve Station, Pennsylvania.

SUMMARY OF REVISIONS

This instruction aligns with AFI 31-401, AFI 31-501, AFI 31-601, and AFI 31-101. It clarifies many areas within the 913th AW relating to personnel security, information security, Sentinel Key Program (SK), Clearance Access Verification System (CAVs), responsibilities of Security Managers (SM)/Alternates (ASM), Military Personnel Office (DPM), Civilian Personnel Office (DPC) Reserve Recruitment Office and Security Force Information Office (SFI). A (I) indicates revisions from the previous edition.

1. References. All personnel with designated responsibilities will become familiar with the following applicable references to ensure compliance of the base Information Security Program (ISP):

- 1.1. Information Security Program, AFI 31-401.
- 1.2. Personnel Security Program, AFI 31-501.
- 1.3. Industrial Security Program, AFI 31-601.
- 1.4. Security Education & Training Guide.

2. Information Security . To ensure the proper protection of DoD classified and sensitive information the following responsibilities are established:

- 2.1. The 913 SPTG Security Specialist is OPR for implementation and administration of the Information Security Program through the designated assistants and the unit/agency security managers and alternates. The SFI will:

2.1.1. Conduct Security Manager (SM) meetings twice and year to discuss and resolve security problems, and afford guidance and training.

2.1.2. Monitor unit/agency Semi-annual Security Self-Inspections.

2.1.3. Conduct an Annual Program Review.

2.2. Unit Commanders/Agency Chiefs will appoint in writing a full-time employee (Civilian/ART) as Security Manager and one or more alternate Security Managers. Alternate Security Managers may also be full-time employees or members of the USAFR as required, to ensure an aggressive and continuing ISP is implemented in their activity. Alternate Security Managers will function as the SM in the absence of the primary SM. Primary and alternate Security Managers must have a security clearance according to AFI 31-401.

2.3. Security Managers will follow the guidance of AFI 31-401 and:

2.3.1. Provide advice and assistance in security matters to their Unit Commanders/ Agency Chiefs and all personnel assigned to their activity.

2.3.2. Become familiar with AFI 31-401 and maintain their unit/agency Security Managers Handbook.

2.3.3. Ensure internal Security Operating Instructions (OI) are developed and implemented at their organization.

2.3.4. Ensure compliance with the security education requirements of AFI 31-401, Chapter 10, and Security Education and Training Guide.

2.3.5. Monitor their unit/agency Semiannual Security Inspections for scope, quality and accuracy.

3. Personnel Security - To ensure personnel are properly cleared for access to classified information, the following procedures for requesting and monitoring security clearances are established.

3.1. The 913 SPTG Security Specialist is designated the single authorized requester for security clearances AFI 31-501 and will:

3.1.1. Maintain a file copy of all security clearance requests and monitor their progress, maintaining appropriate inquiries as necessary.

3.1.2. Submit tracer actions as appropriate and monitor their progress, making additional follow-up inquiries as necessary.

3.1.3. Monitor the military and civilian Clearance Access Verification System (CAVS) Roster, coordinating with DPM/DPC to correct erroneous data.

3.2. The Reserve Recruitment Office, as the first point of contact with newly assigned military personnel, is designated to initiate security clearance request forms and documentation, and will:

3.2.1. For non-prior military personnel, accomplish an ENTNAC; for prior military personnel with more than a 24 month break in service, accomplish a NAC; and for Top Secret Access accomplish an SSBI. An appropriate security clearance form must be accomplished through the Defense Investigative Service, EPSQ Program IAW DoD 5200.1-R and AFI 31-501, Chapter 3, Sec 3.2. Forward an original SF86, appropriate finger print card, and EPSQ disk for review and dispatch to SFAI.

3.2.2. For prior military personnel with less than 24 months break in service, accomplish a form letter (tracer) completed with the necessary data as required by AFI 31-501, for recertification of security clearance and forward to AFI to initiate appropriate tracer action on Sentinel Key Program, (CAVS).

3.3. The Civilian Personnel Office (DPC) is designated, in accordance with AFI 31-501, Chapter 4, to initiate requests forms and documentation for security clearances on newly assigned civilian employees. DPC will:

3.3.1. During the initial processing period, determine the individual's need for a security clearance based upon their position sensitivity as reflected in AFI 31-501, Chapter 3 and official position description.

3.3.2. Submit appropriate documents, requesting the necessary level of security clearance and provide the SFAI a copy for monitoring progress.

3.3.3. Make inquiries in accordance with AFI 31-501, Chapter 4, for prior service civilian personnel, send tracer action, and forward transmittal copy of tracer action to SFAI for monitoring of clearance progress.

3.3.4. Coordinate all tracer actions and comeback copies between SFAI and DPC.

3.4. Unit/Agency Security managers (SM) will ensure Unit Commander/Agency Chiefs are aware of all ongoing security clearance actions within their activity. SM will:

3.4.1. Ensure that all supervisory personnel are aware of their responsibility to report derogatory information concerning personnel, in accordance with AFI 31-501, Chapter 7, Paragraph 7.7.

3.4.2. Upon the receipt of any derogatory information concerning personnel with security clearances, establish a Special Information Folder (SIF) and forward information to the ISPM in accordance with AFI 31-501, Chapter 8.

3.4.3. Deny access to classified information to any persons who do not have a valid security clearance, do not have a need-to-know, do not have appropriate level of clearance, have not signed the NDA Form (SF 312-Check the CAVS roster), or upon which an SIF has been established.

3.4.4. SM will monitor the progress of unit personnel security clearance actions utilizing the Sentinel Key Program (CAVS) Roster. Additionally, the Unit/Agency SM will notify SFAI of any incorrect personnel clearance access, regarding line badge information. Additional information pertaining to line badges is covered in AFI 31-101.

3.4.5. Assist their assigned personnel in the completion of forms and any documentation required for security clearances when:

3.4.5.1. An individual requires an upgraded level of security clearance.

3.4.5.2. An individual requires a Periodic Re-investigation.

3.4.5.3. Addition information is required to complete a pending or open security investigation.

3.4.6. Ensure incoming personnel accomplish SF 312, Classified Information Nondisclosure agreement, and forward document to SFAI. The initial security briefing will be given, by the security manager, at this time.

4. CAVS . The CAVS Roster is the primary tool of the Security Manager to monitor the progress of security clearance actions. The CAVS Roster is generated by the Sentinel Key Program, which resides at Bolling Air Force Base, in Washington DC, and is maintained by the 497th Intelligence Group.

4.1. Security Managers will produce their unit CAVS Roster on a monthly basis (Currently the SFAI will forward a copy to each unit until this product is available to all SMs upon request).

4.2. DPC will forward the ART/Civilian personnel CAVS Roster to the SFAI.

4.3. A Line Badge Information Roster will be forwarded to each unit, upon request, by the Security Clerk, in Pass & ID Office. SM must pay particular attention to individuals' clearance information to ensure only authorized personnel are granted access to controlled or restricted areas and that the requirement for the access exists.

4.4. Once a year the SM will be responsible for a Line Badge Inventory, this will assist in ensuring information is current, i.e. office symbol, name, rate/rank etc.

4.5. The CAVS Roster is the only official source of verification of security clearances unless a Personnel Notification Record Printout, has been received between monthly updates of the CAVs Roster. Should the Printout Information not show up within three months (3) on the new CAVs Roster notify the SFAI.

5. Classified Information Nondisclosure Agreement (NDA) . The requirement to sign the NDA is to ensure Air Force members are fully aware of the duties imposed on them by law and to obtain from each member a personal commitment to protect classified information in accordance with the law. DoD 5200.1-R/AFI 31-401, Chapter 7 explains general policies governing the NDA.

5.1. The new member will obtain the SF 312 from his/her SM. In the event the SM or alternate is not available, the member will be referred to SFAI.

5.2. The SM will review and explain the SF 312 to the member.

5.3. After members have reviewed the SF 312, a signature is required to indicate concurrence. The SM will witness the signature and, in turn complete the SF 312; both the witness and acceptance blocks will be completed and signed by the Security Manager. Ensure the members' name, title or rate/rank is also on the front of the SF 312. The completed SF 312 will then be forwarded to the SFAI for maintenance and distribution.

5.4. If any member refuses to sign the SF 312, the SM will notify the SFAI immediately. Security, immediate supervisor, Civilian Personnel (if applicable), and HQ AFRC will review the case for possible removal or other adverse action.

5.5. Individuals who decline to sign the NDA are denied access to classified information, and appropriate action is taken to revoke the security clearance of declining individuals.

6. Security Termination Briefings/Debriefings . Upon termination of employment, administrative withdrawal of security clearance, or contemplated absence from duty or employment of 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement, AF Form 2587. All Termination Briefings will be made IAW DoD 5200.1-R/AFI 31-401, Chapter 10. This is the responsibility of the unit SM.

6.1. AF Form 2587 will be maintained for two years after the execution of the statement. For civilians, AF Form 2587's must be maintained at the unit of assignment. For military personnel accomplish two (2) forms, forward the original to the servicing DPM for inclusion in the UPRG and file the copy in the unit of assignment for two (2) years.

6.2. If an individual fails to complete an AF Form 2587 or relinquish the unit Line Badge upon termination or resignation, then the unit SM must mail the form and memo to return the Line Badge to the individual's home. The individual will then sign the completed form and return the Line Badge to the SM, where the AF Form 2587 will be maintained for two years and the Line Badge will be forwarded to the SFAR. You may coordinate with DPM, as they may have other forms to be sent to the individual.

CHARLES D. ETHREDGE, Col, USAFR
Commander