

**BY ORDER OF THE COMMANDER  
AIR FORCE MATERIEL COMMAND**

**AIR FORCE MATERIEL COMMAND  
INSTRUCTION 31-400**



**24 AUGUST 2009**

**Certified Current 26 October 2012  
Security**

**INFORMATION PROTECTION (IP)**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the e-publishing website 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: HQ AFMC/IP

Certified by: HQ AFMC/IP (Larry D. Huyett)  
Pages: 7

---

This instruction implements AFD 31-4, *Information Security*. This is a new instruction and should be reviewed in its entirety. This AFMC instruction supports AFI 31-401, *Information Security Program Management*; AFI 31-501, *Personnel Security Program Management*; AFI 31-601, *Industrial Security Program Management*; AFI 10-701, *Operations Security (OPSEC)*; and AFI 10-704, *Military Deception Program* by defining roles and responsibilities of the HQ AFMC IP Office and the AFMC Installation IP Offices. This publication does not apply to either the Air Force Reserve Command (AFRC) or the Air National Guard (ANG) units. Send comments and suggestions about this publication for improvements on AF Form 847, *Recommendation for Change of Publication*, to the Office of Primary Responsibility (OPR). 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 the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afirms/afirms/rims.cfm>.

**1. BACKGROUND:**

1.1. Security is a key enabler to sustaining air, space and cyberspace dominance. To address the diverse security issues across the Air Force, Headquarters United States Air Force (HAF) formed the Air Force Security Policy and Oversight Board (AFSPOB) to align the multiple functional activities having responsibility for the varied aspects of security. The Secretary of the Air Force (SECAF) appointed SAF/AA as the Air Force Senior Administrative Security Official to chair this board.

1.2. The AFSPOB recommended to the Chief of Staff of the Air Force (CSAF) that each MAJCOM mirror the efforts of HAF by creating a structure to implement information

protection policy and procedures within the MAJCOMs to better coordinate and focus on security as well as improve coordination at all levels.

1.3. The Vice Commanders at the MAJCOMs serve the role of the Command's senior security official. The HQ AFMC Information Protection office (HQ AFMC/IP) serves as the single focal point to converge multifunctional security issues and lead the Command's information protection efforts. HQ AFMC/IP office unifies the restructured Information, Personnel, Industrial and Operations Security (OPSEC)/Military Deception staff.

1.4. The Chief of Information Protection chairs the AFMC MAJCOM Security Advisory Group (MSAG) comprised of functionally designated subject matter experts/representatives. The MSAG membership includes, but is not limited to, information security, personnel security, industrial security, physical security, OPSEC, information assurance, information management, public affairs, program protection, special access, Sensitive Compartmented Information (SCI), international affairs and foreign disclosure.

1.5. The Vice Commanders at each air base wing serve the role of the Installation's senior security official. The installations will establish an ABW/Information Protection office (ABW/IP). The ABW/IP office serves as the single focal point to converge multifunctional security issues and lead the Installation's information protection efforts. The ABW/IP offices will report directly to the ABW/CV.

2. **SCOPE:** This AFMCI applies to all AFMC IP Offices. It specifies primary roles and responsibilities of the HQ AFMC/IP and ABW/IP offices. This AFMCI provides for the orderly transition of all aspects of the IP offices and a management structure to ensure the uninterrupted collection, processing and dissemination of information. ABW/CCs may augment this instruction to detail their specific implementation needs.

### 3. **OPERATIONAL CAPABILITIES:**

#### 3.1. Initial Operational Capability (IOC):

3.1.1. HQ AFMC created an Information Protection office (HQ AFMC/IP) reporting to the AFMC Vice Commander. Installations must create an ABW/Information Protection office (ABW/IP) reporting directly to the ABW/CV. The manpower positions for the HQ AFMC/IP and ABW/IP offices were resourced from existing information, personnel and industrial security billets.

3.1.2. HQ USAF identified the billets/position numbers.

3.1.3. While the new IP offices must include Information, Personnel and Industrial Security Programs as a minimum for IOC, there is no prohibition against including other related security programs such as Operations Security, Military Deception, Program Protection, Foreign Disclosure, Special Access Programs, Antiterrorism or Scientific and Technical Information under the IP umbrella. However, these programs will not transfer or fall under the Installation IP offices without submitting an approval request from the wing installation commander to HQ AFMC/IP. HQ AFMC/IP will coordinate with the MSAG and the appropriate HQ functionals prior to submitting to AFMC/CV for approval. For example, security of special access programs may be included as part of IP as long as it has been approved by the AFMC Special Access Program Management

Office, HQ AFMC/A5J. IP offices that had other disciplines under their umbrella prior to 10 Nov 08 are exempt from this requirement to send a request for transfer approval.

3.1.4. HQ AFMC/IP and ABW/IP will ensure all publications/forms are transferred/updated, as appropriate, in accordance with AFI 33-360, *Publications and Forms Management*.

3.2. Full Operational Capability (FOC) is defined by AFMC as:

3.2.1. Creation of MAJCOM and Installation IP Offices.

3.2.2. Realignment of manpower positions from SF to IP.

3.2.3. Realignment of military positions to civilian positions. Note: for military billets performing IP duties, installations will realign vacant civilian Security Forces authorizations in lieu of military to the installation IP offices and retain military authorizations for deployment taskings. Military authorizations that initially cannot be exchanged with vacant civilian authorizations will remain in Security Forces units and the personnel detailed to installation IP offices. HQ AFMC/IP will work with SAF/AAP and AF/A7S to develop a plan to identify tradeoffs and return detailed military personnel back to Security Forces units.

3.2.4. Implementation of this AFMCI.

3.2.5. Establishment of the MAJCOM and base Security Advisory Groups.

3.2.6. Publications/forms are transferred/updated in accordance with AFI 33-360.

3.3. **Paragraphs 3.1.** and **3.2** will be completed by 30 Jun 09.

#### 4. **RESPONSIBILITIES:**

4.1. While AFMC/CV has overall command responsibility for the following Information Protection programs, the day-to-day operations and release of Information Protection data/reports will be the responsibility of HQ AFMC/IP: Information, Industrial, Personnel, and Operational security and Military Deception program.

4.2. The above programs in **paragraph 4.1** provide guidance for the following subject areas: Security Classification Guides; Information Safeguarding; Original Classification Authorities; Security, Education, and Training; Classification Management; Declassification Management; Unclassified Controlled Information; For Official Use Only; Formerly Restricted Data; NATO Security Policy; and Unclassified Controlled Nuclear Information.

4.3. HQ AFMC/IP will specifically: provide policy and guidance for the Information Protection Program; attend HQ AFMC weekly staff meetings; attend HQ AFMC/CS staff meetings; coordinate HQ AFMC/IP office space relocation with HQ AFMC/CS; designate a single HQ AFMC/IP FM point of contact for all financial-related matters; annually, develop an AFMC IP budget through the HQ AFMC/CS Office.

4.4. HQ AFMC/IP will interface and update AFMC/CV on IP activities through: reports on all Information Security Program Reviews; Annual Top Secret position status report; AFMC MAJCOM Security Advisory Group (MSAG) meeting minutes; Executive summaries of Air Force Security Advisory Council meetings and Executive summaries of Security Developmental Team results, or as required.

4.5. HQ AFMC/IP will prepare the following annual reports: SF 311, Agency Security Classification Program Data Report; Operations Security Report and Military Deception Report.

4.6. ABW/IP offices will specifically:

4.6.1. Provide policy and guidance for the Installation Information Protection Program.

4.6.2. Provide HQ AFMC/IP Office with a monthly status on progress of Full Operational Capability (FOC).

4.6.3. Attend installation staff meetings.

4.6.4. Provide HQ AFMC/IP with the Installation Annual Top Secret Position Status Report no later than 30 June.

4.6.5. Establish an Installation SAG (ISAG). The ISAG membership includes, but is not limited to, information security, personnel security, industrial security, physical security, OPSEC, information assurance, information management, public affairs, program protection, special access, Sensitive Compartmented Information (SCI), international affairs and foreign disclosure.

4.6.6. Conduct ISAG meeting at least quarterly.

4.6.7. Provide HQ AFMC/IP with the minutes of the ISAG meetings no later than 30 days after the meeting.

4.6.8. Provide HQ AFMC/IP with the installation's Annual SF 311, Agency Security Classification Program Data Report no later than 1 October.

4.6.9. Provide HQ AFMC/IP with the installation's Annual OPSEC Assessment Report no later than 1 October.

## 5. GOVERNANCE PROCESS:

5.1. To implement a governance structure, the SECAF and CSAF chartered the AFSOB to provide a focused and unified AF perspective on security issues across the Service as well as to DoD, executive agencies and other external organizations. Additionally, the AFSPOB created the Air Force Security Advisory Group (AFSAG) to deliberate and prepare issues for AFSPOB consideration.

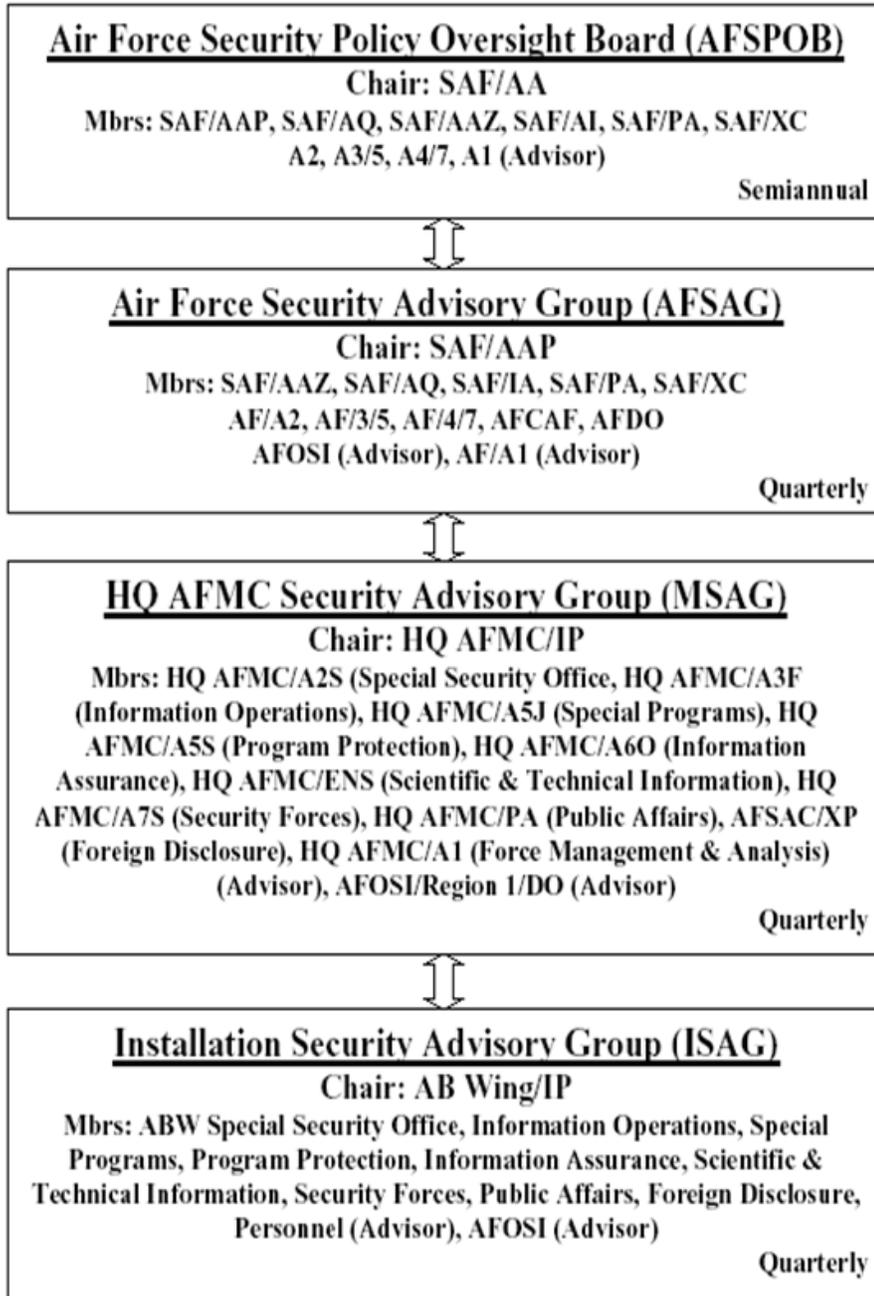
5.2. The AFSAG works issues that cut across the security environment as well as coordinating and networking security issues with the MAJCOMs and installations through their respective SAGs.

5.3. The AFMC MSAG works issues that cut across security functional lines. The MSAG takes a Command approach to solve security issues as well as deliberate and prepare any issues that may have an AF impact and forward to the AFSAG.

5.4. ISAGs work issues that cut across security functional lines. The ISAG takes an installation approach to solve security issues as well as deliberate and prepare any issues that may have an AFMC impact and forward to the MSAG.

**Figure 1. Governance Process.**

Figure 1. Governance Process.



**6. Adopted Forms:** AF Form 847, *Recommendation for Change of Publication*

TERRY L. GABRESKI  
Lieutenant General, USAF  
Vice Commander

**Attachment 1**

**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION**

***References***

AFI 10-701, *Operations Security (OPSEC)*, 18 October 2007

AFI 10-704, *Military Deception*, 30 August 2005

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

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFI 31-601, *Industrial Security Program Management*, 29 June 2005

AFI 33-360, *Publications and Forms Management*, 18 May 2006

AFMAN 33-363, *Management of Records*, 1 March 2008

AFPD 31-4, *Information Security*, 1 September 1998