BY ORDER OF THE COMMANDER
AIR MOBILITY COMMAND

AIR MOBILITY COMMAND
INSTRUCTION 16-1401

30 NOVEMBER 2020

Operations Support

INFORMATION PROTECTION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AMC/IP

Certified by: HQ AMC/IP
(Mr. Scott R. Wobbe)

Supersedes: AMCI16-1401, 23 August 2012

Pages: 7

This instruction applies to all Information Protection (IP) offices within AMC and provides guidance on roles and responsibilities to HQ AMC and installation IP offices. This instruction provides AMC policy for implementing the Air Force Information Protection program and protecting sensitive information (regardless of its classification, sensitivity, physical form, media or characteristics). It assigns specific responsibilities for program implementation, execution and oversight and supports all information centric instructions and processes in the Air Force and DoD community. It provides for the orderly transition of primary and additional duties of the IP office and a management structure to ensure the uninterrupted collection, processing and dissemination of information. This publication does not apply to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC) and their units. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule. See Attachment 1 for a glossary of references and supporting information. This instruction may be supplemented at the installation level, MAJCOM coordination is not required.

SUMMARY OF CHANGES

This document is a total rewrite with the elimination of several directorate functions. Updated terminology and addition of Security Program Executive Working Group.

1. POLICY AND PROGRAM MANAGEMENT

1.1. **Policy.** Information Protection (IP) is a key enabler to sustaining air, space and cyberspace dominance. Today's warfighter requires the capability to overcome 21st century irregular, catastrophic and disruptive IP challenges while sustaining the capability to address traditional ones. The warfighter depends on information to sustain military operations across the conflict spectrum.

1.2. **Philosophy.** IP is the collective policies, processes and implementation of risk management and mitigation actions instituted to prevent the compromise, loss, unauthorized access/disclosure, destruction, distortion or non-accessibility of information, regardless of physical form or characteristics, over the life cycle of the information. It includes actions to regulate access to sensitive information, controlled unclassified information and classified information produced by, entrusted to or under the control of the United States Government. IP employs a converged, collaborative and integrated framework to assure effective measures are employed to protect information and reduce risk.

1.3. **Program Management.**

1.3.1. Security Program Executive. The AMC Deputy Commander is designated as the Security Program Executive (SPE) to communicate and coordinate on security issues relative to the command.

1.3.2. AMC Program Manager. The Director, Information Protection (AMC/IP) is responsible for policy, resource advocacy, and oversight of the IP program. The Director reports to the AMC/CD and serves as the single focal point to converge and facilitate the command's enterprise information protection efforts. The Director, IP is the command

security specialist career field manager for the GS-008X series. The day-to-day operations and release of IP data/reports rests with the Director, IP.

1.3.3. AMC/IP Directorate. The AMC/IP Directorate develops information protection policy and procedures within AMC to better coordinate and focus on information centric core functions, as well as improve coordination at all levels.

1.3.4. AMC Installations. AMC host wing Vice Commanders (WG/CVs) are designated as the Installation's Security Program Executive. Installations will establish an Information Protection office (IPO). The Installation Chief, Information Protection (CIP) reports directly to and is supervised by the WG/CV. The IPO serves as the single focal point to converge and facilitate enterprise information protection efforts.

1.3.4.1. Exceptions. At Joint Base (JB) locations where the Air Force is lead service, the Vice Wing Commander is responsible for delivery of installation support services retains traditional IP authority. At JB Lewis-McChord, the Air Force is not the lead service, however, the 62 AW/CV will retain traditional IP authority. In cases where US Navy or US Army personnel function as the deputy joint base commander (DJBC), they will serve as the SPE.

1.3.4.2. AMC host IPOs are encouraged to establish MOUs with each tenant organization to integrate all IP activities and personnel into the host IPO.

2. IP CONSTRUCT. Commanders are responsible for establishing IP programs to provide a converged environment across all information domains. Installations will align IP program functions reporting directly to the CV. Because of the interrelationship between various functional elements of the information domain, IP is a major area of focus to be addressed by a multi-functional collaborative team approach. The goal is to seamlessly integrate the IP environment into the mission by focusing on the IP key pillars: Personnel Security, Information Security, and Industrial Security. At their respective levels, IP staffs provide daily functional management of IP issues.

3. RESPONSIBILITIES

3.1. **AMC/CD.**

3.1.1. Serves as the MAJCOM Security Program Executive (SPE).

3.1.2. Serves as the reporting official for the Director, Information Protection.

3.2. **AMC/IP.**

3.2.1. Reports directly to the AMC/CD.

3.2.2. Provides guidance and oversight on cross-functional information centric activities.

3.2.3. Provides policy and guidance to AMC Wing IP programs.

3.2.4. Augments Secretary of the Air Force Security, Special Program Oversight and Information Protection (SAF/AAZ) staff as outlined in Standard Core Personnel Documents.

3.2.5. Develops/executes an AMC/IP budget through the HQ AMC/CS Office.

3.2.6. Provides education, training and professional development program guidance.

3.2.7. Conducts teleconferences with Installation CIPs.

3.2.8. Provides IP briefing and related information to newly assigned AMC wing commanders.

3.2.9. Chairs the Security Program Executive (SPE) Working Group (SWG) a forum providing the SPE a coordinated variety of security organizations, infrastructure, and measures to safeguard Air Force personnel, information, operations, resources, technologies, facilities, and assets against harm, loss or hostile acts and influences. The SWG established a construct providing for improved oversight, execution and risk management of IP, SAP and SCI structures to support and enable AMC/CC's vision.

3.2.10. Provides support and coordinates activities with HQ AMC/A6 on cyber related issues, e.g., CCRI activities.

3.3. **AMC/CS.** Advocates for IP funding to meet mission needs., i.e., TDY, office supplies, etc.

3.4. **AMC (Installation) CV.**

3.4.1. Serves as the wing's Security Program Executive.

3.4.2. Serves as the supervisor and reporting official for the Chief, Information Protection.

3.5. **Installation Chief, Information Protection (CIP).**

3.5.1. Reports directly to the Wing CV.

3.5.2. Provides guidance and oversight for all enterprise information protection activities, functions and programs to assist the Installation Commander in maintaining a strong IP program.

3.5.3. Represents IP by attending senior-level meetings such as: wing staff meetings, Status of Discipline meetings, Integrated Defense Council meetings and commanders' call.

3.5.4. Ensures SIPRNET capability is readily available to the IP office.

3.5.5. Manages and provides oversight for all Information, Industrial and Personnel Security functions on the installation.

3.5.6. Annual Self-Inspections. Installation CIPs will conduct Annual Self-Inspections on major areas identified in DoDM 5200.01, Volume 1, Enclosure 2, *DoD Information Security Program: Overview, Classification, and Declassification*, and AFI 16-1404, *Air Force Information Security Program*, Chapter 10.

3.5.7. After review by the Wing CV, report IP metric data to AMC/IP.

4. ENTERPRISE PROTECTION RISK MANAGEMENT PROGRAM (EPRM).

4.1. General. The Enterprise Protection Risk Management Program provides a systematic approach to acquiring and analyzing information necessary for protecting assets and allocating security resources. To meet today's security challenges, AMC will follow national-level security policy initiatives that endorse a risk analysis methodology which examines three basic elements: threat, criticality, and vulnerability. The EPRM vision is to:

4.1.1. Effectively allocate scarce resources through informed and risk-based decision making.

4.1.2. Provide standardized, measured and enterprise-wide analysis to calculate and respond to risk.

4.1.3. Provide a converged environment for protecting the information needed for effective air, space, and cyberspace operations.

4.2. EPRM replaces Management Internal Control Toolset to capture non-compliance within the Air Force Inspection Program. Recommend IP Program Managers serve as Wing Inspection Team members to ensure non-compliance is entered into Inspector General Enterprise Management System (IGEMS) in order for the wing commander to make a risk management decision. In addition, recommend non-compliance discovered during Annual unit IP Self-Inspection be entered into IGEMS. This ensures all non-compliance is captured, recorded and acted upon by leadership during the Commander's Inspection Management Board.

5. OVERSIGHT.

5.1. AMC Staff Assistance Visits (SAV). AMC/IP will conduct SAVs on the installation-level IPOs when requested by the wing commander.

5.2. Command Cyber Readiness Inspections. Command Cyber Readiness Inspections (CCRIs) are conducted by the Defense Information Systems Agency (DISA). The Wing Communications Group/Squadron is the senior point of contact for this event in coordination with all host and tenant organizations.

6. ADMINISTRATION.

6.1. General. The Information Protection function conducts personnel security clearance activities, facilitates adverse information requests, stores privacy act data, conducts interviews, performs fingerprinting, performs classified information activities and maintains records.

6.2. Office Space. Wing IP offices require adequate office space to allow for privacy and security in ensuring classified information, discussions and personnel security interviews are protected. Separate offices which have the ability to be individually locked are required.

6.3. Equipment. Each IP office will have enough workstations to ensure connectivity to the NIPRNET and SIPRNET. If SIPRNET connectivity is unavailable in the local IP office, an accessible SIPRNET will be readily available.

7. IP METRICS

7.1. AMC/IP. The AMC/IP office will collect, collate and report metric data IAW SAF/AAZ requirements.

7.2. AMC/CD Review. AMC/IP will review metric data with the AMC/CD, prior to being released to SAF/AAZ.

7.3. Installation Reporting Requirement. The CIP will collect, collate and report metric data to AMC/IP IAW reporting requirements. CIPs will review metric data with their CV, prior to submitting to AMC/IP.

8. PROFESSIONAL DEVELOPMENT

8.1. Security Certification. To ensure IP professionals are maintaining current knowledge and job skills, DoD developed a Security Professional Education Development (SPeD) certification program. All IP personnel are required to become certified at the appropriate level. The SPeD Certification Credential certifies that a security practitioner satisfied standards approved by the Department of Defense Security Training Council, an advisory body for DoD on security training. Position descriptions are indexed for what certification levels are required. Continuing education is required to maintain certification.

8.2. Air Force Civilian Leadership Development. Job performance and development are key in maintaining expertise and competence for the IP professional. Personnel performing IP duties will be expected to attend Air Force civilian leadership programs as part of their development process. This is an individual responsibility for those personnel desiring promotions and new IP opportunities. In addition, completion of a Civilian Development Plan is required in order for the Development Team to properly vector an individual to meet their desired goals.

SCOTT R. WOBBE
Chief, Information Protection

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDM 5200.01 V 1-4, *DoD Information Security Program*, 24 Feb 2012

AFI 16-1404, *Air Force Information Security Program*, 29 May 2015

AFI 33-322, *Records Management and Information Governance*, 22 Mar 2020

Prescribed Forms

No Forms Prescribed

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acromyns