

**BY ORDER OF THE SECRETARY
OF THE AIR FORCE**

AIR FORCE INSTRUCTION 16-1402

5 AUGUST 2014

Operations Support

**INSIDER THREAT PROGRAM
MANAGEMENT**



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: SAF/AAZE

Certified by: SAF/AAZ
(Michael J. Janosov)

Pages: 8

This instruction implements the DoD Insider Threat Program (InTP) required by AFPD 16-14, *Security Enterprise Governance* and Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and *National Insider Threat Policy and Minimum Standards for the Executive Branch Insider Threat Programs*. It assigns responsibilities for the oversight and management of the Air Force Insider Threat Program. The disclosure provisions in this instruction are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive Orders and statutory provisions are incorporated into this instruction and are controlling. This instruction is mandatory for all Air Force military and civilian personnel members to include the Air Force Reserve and Air National Guard, contractors, and consultants (when contract performance supports the Air Force), and non-DoD U.S. Government Agencies whose personnel, by mutual agreement, require support from or conduct operational activity with the Air Force. This publication may be supplemented at any level, but all direct supplements must be routed to the Office of Primary Responsibility (OPR) of this publication for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. In accordance with AFI 33-360, submit requests for waivers through the chain of command to the appropriate tier waiver approval authority, or alternately, to the Publication OPR

for non-tiered compliance items. Ensure 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 AF Records Disposition Schedule (RDS) maintained in the Air Force Records Information Management System (AFRIMS).

1. Purpose. This Instruction assigns responsibilities for the Air Force Insider Threat Program (InTP) in accordance with AFPD 16-14.

1.1. The purpose of this AFI is to establish a framework to integrate policies and procedures to detect, deter, and mitigate insider threats to national security and Air Force assets. Implementing guidance will be established to:

1.1.1. Ensure existing and emerging insider threat training and awareness programs are developed, implemented and managed accordingly.

1.1.2. Continuously evaluate personnel by enhancing technical capabilities to monitor and audit user activity on information systems.

1.1.3. Leverage antiterrorism (AT), counterintelligence (CI), human resources (HR), law enforcement (LE), security (e.g. cyber (formerly information assurance), information, industrial, personnel, physical, and operations), medical, and other authorities to improve existing insider threat detection and mitigation efforts.

1.1.4. Detect, mitigate and respond to insider threats through integrated and standardized processes and procedures while ensuring civil liberties and privacy rights are safeguarded.

2. Governance. In accordance with AFPD 16-14, the Air Force Security Enterprise and Mission Assurance Working Group (AF SEMAWG) directed the Air Force Insider Threat Working Group (InTWG) be established. The AF InTWG will identify strategic goals, approve program implementation, integrate policy and procedures, and develop prioritized resource recommendations. The InTWG will coordinate with DoD and Intelligence Community (IC) insider threat leads to represent Air Force interests. The need for the AF InTWG will be reviewed annually and will be disestablished when the AF SEMAWG no longer deems its services/functions necessary.

3. Objectives.

3.1. The Air Force Insider Threat Program will consist of the following focus areas:

3.1.1. Network monitoring and auditing. Available monitoring and auditing capabilities shall support insider threat detection and mitigation efforts to the extent possible. Monitoring and auditing capabilities shall be integrated into the overall insider threat mitigation process. Capabilities should constantly be improved in order to meet current and future Air Force mission requirements as well as Federal and Department of Defense standards, and to proactively incorporate best practices to prevent and detect anomalous activity.

3.1.2. Information Sharing. An effective Insider Threat program relies upon timely sharing of information. Counterintelligence, security, LE, and HR policies must ensure that pertinent information reaches insider threat program personnel so they can take

appropriate action. Information sharing policies and procedures must comply with privacy, whistleblower, and records retention requirements.

3.1.3. Security. Procedures must be in place that support continuous evaluation of personnel to assess their reliability and trustworthiness. Access control methods and physical safeguards are essential for ensuring authorized personnel do not breach the boundaries of authorized access. Security (e.g. cyber, information, industrial, personnel, physical, and operations security) policies and procedures must account for the continuous evaluation of personnel, access controls, and safeguards in place to protect National security assets.

3.1.4. Training and Awareness. Insider threat program personnel will receive training to ensure adherence to privacy, whistleblower, records retention, civil liberties, and information sharing requirements. Insider threat program personnel will provide training to commanders and supervisors on identifying, reporting, and mitigating insider threats. Additionally, commanders and supervisors will ensure insider threat training is provided to assigned personnel within 30 days of hire, and annually thereafter. **(Tier 2)**.

3.1.5. Insider Threat Reporting and Response. Insider threat actors typically exhibit concerning behavior. Reporting and sharing behaviors of concern among stakeholders is necessary to determine the severity of the threat and appropriate response options. Procedures must be in place to enable trained insider threat personnel to integrate necessary and relevant information, analyze and appropriately respond to mitigate the threat. These procedures must be consistent with privacy, civil liberties, records retention, and whistleblower protection guidance.

Table 1. Insider Threat Program Focus Areas, Objectives, and Stakeholders.

Network Audit	Information Sharing	Security	Training/Awareness	Insider Threat Reporting/Response
<i>Establish a capability to monitor & audit users across all domains</i>	<i>Facilitate the sharing of CI, Security, cyber, LE, HR, and other related information (medical)</i>	<i>Evaluate security controls in place to protect assets (information, people, equipment)</i>	<i>Provide workforce with training on insider threat awareness & reporting responsibilities</i>	<i>Establish an integrated reporting and response capability</i>
SAF/AA; SAF/CIO A6; AF/A2; AF/A3/5	SAF/AA; SAF/CIO A6; SAF/IG; AF/SG; AF/A1; AF/A2; AF/A4/7	SAF/AA; SAF/CIO A6; AF/A1; AF/A2; AF/A4/7	SAF/IG; AF/A1	SAF/AA; SAF/IG; SAF/CIO A6; AF/SG; AF/A1; AF/A2; AF/A4/7

4. Responsibilities.

4.1. Administrative Assistant to the Secretary of the Air Force (SAF/AA), as the security Senior Agency Official and the Security Program Executive, will provide oversight and policy authority for the Air Force InTP.

4.1.1. Director, Security, Special Program Oversight and Information Protection (SAF/AAZ) will serve as the designated representative to SAF/AA for InTP management and accountability and will:

4.1.1.1. Provide oversight for the InTP and coordinate with stakeholders to promulgate policy.

4.1.1.2. Coordinate with representatives of the InTWG to identify and make resource recommendations to SAF/AA.

4.1.1.3. Integrate future insider threat detection and mitigation procedures as they are developed into applicable security policies where appropriate.

4.1.1.4. For Special Access Programs (SAP), promulgate policies and procedures that support monitoring and auditing of SAP networks and assets for insider threat detection and mitigation in accordance with Air Force and IC policies.

4.1.1.5. Ensure procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters.

4.1.1.6. Develop guidelines and procedures for documenting insider threat matters reported and response action(s) taken that will enable timely resolution.

4.1.1.7. Appoint a co-chair for the InTWG, which will be under the oversight of the Security Enterprise and Mission Assurance Working Group.

4.1.1.8. Develop an InTP implementation plan and annually report to the Secretary of the Air Force, program accomplishments, resource requirements, insider threat risks, program impediments or challenges, and recommendations for program improvements.

4.1.1.9. Coordinate InTP issues through the Air Force Security Enterprise Executive Board Secretariat.

4.1.1.10. Provide a representative to departmental and interagency forums engaged in countering insider threats.

4.2. Assistant Secretary of the Air Force for Acquisition (SAF/AQ) will:

4.2.1. Ensure policies and procedures are in place to implement applicable requirements of the InTP.

4.2.2. Provide a representative to the InTWG.

4.3. Chief of Information Dominance and Chief Information Officer (SAF/CIO A6) will:

4.3.1. Promulgate policies and procedures that support monitoring and auditing of applicable networks and assets to support insider threat deterrence, detection, and mitigation.

4.3.2. Develop strategy and policy that allows for regular and timely access to network and system audit information for insider threat program personnel to support the identification, analysis, and resolution of insider threat issues.

4.3.3. Develop guidelines and procedures for the retention of records and documents pertaining to insider threat inquiries.

4.3.4. Provide a representative to the InTWG.

4.4. The General Counsel of the Air Force (SAF/GC) in coordination with the Judge Advocate General, will:

4.4.1. Provide advice and counsel regarding DoD policy, laws and regulations that are applicable to the InTP and those pertaining to civil liberties, privacy, and whistleblower protection.

4.4.2. Provide a representative to the InTWG.

4.5. Inspector General (SAF/IG) will:

4.5.1. Co-chair the InTWG.

4.5.2. Develop and execute an insider threat awareness and training program for the workforce.

4.5.3. Ensure insider threat personnel are trained in counterintelligence, security, procedures for conducting insider threat response actions, and applicable legal issues, to include civil liberties, whistleblower and privacy issues.

4.5.4. Establish procedures to securely provide insider threat program personnel regular, timely, and electronic access to information necessary to identify, analyze and resolve insider threat issues. These procedures must be consistent with privacy laws, civil liberties, and regulations.

4.5.5. Provide access to counterintelligence reporting and analytic products relevant to insider threat.

4.5.6. Audit insider threat personnel's handling, use, and access to records and data to ensure compliance with privacy laws, civil liberties, and to ensure access is restricted only to insider threat personnel who require the information to perform their authorized functions.

4.6. Deputy Chief of Staff, Manpower, Personnel and Services (AF/A1) will:

4.6.1. Securely provide insider threat program personnel regular, timely, and if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes but is not limited to relevant HR databases and files to include but not limited to personnel files, payroll and voucher files, outsider activities requests, disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

4.6.2. Establish procedures for access requests by insider threat personnel involving particularly sensitive or protected information. Ensure procedures are consistent with privacy laws, civil liberties, and regulations.

4.6.3. Establish reporting guidelines for relevant organizational components to refer relevant insider threat information directly to the insider threat program.

4.6.4. Provide policy and guidance for integrating and vetting new/emerging insider threat institutional education and training requirements or learning outcomes into accessions, Professional Military Education, Professional Continuing Education and ancillary training.

- 4.6.5. Provide a representative to the InTWG.
- 4.7. Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2) will:
 - 4.7.1. Develop, oversee and manage, in coordination with InTWG, a capability that enables the collection and analysis of relevant insider threat data for the intelligence community information environment. Ensure procedures are consistent with privacy laws, civil liberties, and regulations.
 - 4.7.2. Review, update and promulgate policies and procedures that support monitoring and auditing of intelligence assets and networks for insider threat detection and mitigation in accordance with Air Force and IC policy.
 - 4.7.3. Oversee monitoring and auditing of Air Force IC networks and assets for insider threat activities and establish procedures to securely provide insider threat program personnel regular, timely, and electronic access to information necessary to identify, analyze and resolve insider threat issues.
 - 4.7.4. Provide insider threat program personnel access to intelligence reporting and analytic products relevant to insider threat.
 - 4.7.5. Provide a representative to the InTWG.
- 4.8. Deputy Chief of Staff for Operations, Plans, and Requirements (AF/A3/5) will ensure cyber space operations support the capability to monitor and audit user activity in accordance with U.S. Cyber Command tasking orders.
- 4.9. Deputy Chief of Staff, Logistics, Installations and Mission Support (AF/A4/7) will:
 - 4.9.1. Ensure procedures are in place to securely share law enforcement and other applicable information consistent with privacy laws, civil liberties and regulations with authorized insider threat program personnel to identify, analyze and resolve insider threat issues.
 - 4.9.2. Integrate insider threat detection and mitigation procedures into applicable security policies.
 - 4.9.3. Provide a representative to the InTWG.
- 4.10. The Air Force Judge Advocate General (AF/JA), in coordination with the Air Force General Counsel, will:
 - 4.10.1. Ensure the InTP operates in accordance with DoD policy, applicable laws, civil liberties, whistle blower protections, and privacy policy.
 - 4.10.2. Provide a representative to the InTWG.
- 4.11. Air Force Surgeon General (AF/SG) will:
 - 4.11.1. Ensure policies and procedures are in place for the sharing of information related to insider threats in already existing violence prevention programs. Information sharing procedures will be in accordance with applicable laws and policies.
 - 4.11.2. Provide a representative to the InTWG.
- 4.12. Director of Test and Evaluation (AF/TE) shall ensure policies and procedures are in place to implement applicable requirements of the InTP.

4.12.1. Provide a technical consultant representative as needed to the InTWG.

4.13. MAJCOM and DRUs will:

4.13.1. Through their appointed Security Program Executive, communicate and coordinate on insider threat issues relative to their command and support SAF/AA in executing the Air Force insider threat program as it evolves **(T-1)**.

PATRICIA ZARODKIEWICZ
Administrative Assistant

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

Air Force Policy Directive 16-14, *Security Enterprise Governance*, 17 October 2013

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*

Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, November 21, 2012

Air Force Instruction 33-360, *Communications and Information*, 25 September 2013

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

IC—Intelligence Community

InTP—Insider Threat Program

InTWG—Insider Threat Working Group

SEMAWG—Security Enterprise Mission Assurance Working Group

Terms

Insider Threat—The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.