BY ORDER OF THE COMMANDER AIR FORCE TECHNICAL APPLICATIONS CENTER

DEPARTMENT OF THE AIR FORCE INSTRUCTION 16-1402

10 MAY 2024

AIR FORCE TECHNICAL APPLICATIONS CETNER Supplement

29 SEPTEMBER 2025

Operations Support

AFTAC COUNTER-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: AFTAC/SSO

Certified by: AFTAC/SSO
(Mr. Patrick Reagan)
Pages: 13

This supplement implements and extends the guidance of DAFI 16-1402, Counter-Insider Threat Program Management. It applies to all Air Force Technical Applications Center (AFTAC) civilian employees and uniformed members of the United States Space Force (USSF), Regular Air Force (RegAF), Air Force Reserve (AFR), Air National Guard (ANG), and those with a contractual obligation to abide by the terms of Department of the Air Force (DAF) publications, non-Department of Defense (DoD) U.S. government agencies whose personnel, by mutual agreement, require support from or conduct operational activity within AFTAC facilities. Ensure 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 Disposition Schedule (RDS) located in the Air Force Records Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command to the Publications and Forms Manager, AFTAC/A6. This publication may not be supplemented at any level. The authorities to waive wing, unit, delta or garrison level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. 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. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Department of the Air Force.

4.18. Wing, Delta, Installation, or equivalent level Commanders will:

4.18.9. **(Added-AFTAC)** The Air Force Technical Applications Center Commander (AFTAC\CC) shall:

4.18.9.1. **(Added-AFTAC)** Serve as the Senior Official for AFTAC's C-InTP.

4.18.9.2. **(Added-AFTAC)** Appoint in writing a primary and alternate C-InTP liaisons within AFTAC's Information Protection Office (IPO).

4.18.9.3. **(Added-AFTAC)** Ensure the following representatives are part of the AFTAC C-InTP Collaboration Group:

4.18.9.3.1. **(Added-AFTAC)** AFTAC Personnel Security, AFTAC Legal Advisor, AFTAC Employee Manager Representative, unit/director First Sergeants, Counter Intelligence (CI) Representative, Cyber Security and Behavioral Health.

4.18.9.4. **(Added-AFTAC)** Approves all C-InTP reports prior to submission to DAF C-InT Hub.

4.18.10. **(Added-AFTAC)** The Air Force Technical Applications Center Deputy Commander (AFTAC/CD) shall:

4.18.10.1. **(Added-AFTAC)** Serve as the Deputy Senior Official for AFTAC's C-InTP and has all responsibility of the Senior Official in their absence.

4.18.10.2. **(Added-AFTAC)** Assess referrals generated from the DAF C-InT Hub for possible opening of a security incident for secret and below information.

4.18.11. **(Added-AFTAC)** Center Commanders, including detachment G-Series Commanders, Directors of Systems Directorate (SD), Strategic Integration (SI), Chief of Staff (CoS), Manpower, Personnel, and Services (A1), Intelligence & Operations (A2/3), Logistics (A4), Plans, Programs and Requirements (A5/8), Communications (A6) and their deputies will:

4.18.11.1. **(Added-AFTAC)** Report DoD Insider Threat Program enterprise threshold-level events to AFTAC's C-InTP Liaison in a timely manner but no later than 5 business days of discovering the information.

4.18.11.2. **(Added-AFTAC)** Will not alert subjects of any ongoing C-InT inquiry. Contact AFTAC C-InT Liaison for guidance.

4.18.12. **(Added-AFTAC)** Center Commanders, including detachment G-Series Commanders will:

4.18.12.1. **(Added-AFTAC)** Assess referrals generated from the DAF C-InT Hub for administrative actions, criminal investigations, personnel security incident reports, or other commander directed actions in coordination with authorities responsible for taking appropriate action or responding to referred information.

4.18.12.2. **(Added-AFTAC)** Report any substantiated allegation(s) as a result of a command directed or criminal investigation that meets any of the DoD Insider Threat Program enterprise threshold level events. Commanders will redact victim and third-party identifying information.

4.18.12.3. **(Added-AFTAC)** Promptly share information identified as a result of command-directed mental health evaluation that meets any of the DoD Insider Threat Program enterprise thresholds or is considered a potential risk indicator to the AFTAC C-InTP Liaison.

4.18.12.4. **(Added-AFTAC)** Immediately report whenever a military member is under investigation, administrative discharge for misconduct is initiated or a civilian employee/contractor is provided an intent to remove or is fired for cause.

4.18.13. **(Added-AFTAC)** AFTAC A1K will:

4.18.13.1. **(Added-AFTAC)** Ensure information on all civilian employees that meets any of the DoD Insider Threat Program enterprise thresholds or is considered a potential risk indicator is shared with the AFTAC C-InTP Liaison within 5 duty days of receipt.

4.18.14. **(Added-AFTAC)** Chief, AFTAC Information Protection Office (IPO) will:

4.18.14.1. **(Added-AFTAC)** Manage the Center's C-InTP and ensure primary and alternate C-InTP liaisons are designated on the MAJCOM appointment letter.

4.18.15. **(Added-AFTAC)** AFTAC's C-InTP Liaison will:

4.18.15.1. **(Added-AFTAC)** Establish processes and procedures for gathering and reporting information to and from the DAF C-InT Hub.

4.18.15.2. **(Added-AFTAC)** Report DoD Insider Threat Program enterprise threshold-level events to the DAF C-InT Hub within timelines established by DAFI 16-1402.

4.18.15.3. **(Added-AFTAC)** Report to the DAF C-InT Hub all mitigation and response actions taken to close out reporting actions with the DAF C-InT Hub in a timely manner, but no later than 5 business days of responsible commander's decision.

4.18.15.4. **(Added-AFTAC)** Notify all AFTAC directors of C-InT reports on personnel assigned to their directorates.

4.18.15.5. **(Added-AFTAC)** With approval from the Senior Official or Deputy Senior Official for AFTAC's C-InTP, share name and category of threshold with the Space

Launch Delta 45 (SLD) C-InTP liaison to ensure installation commander can manage the risk to their assets and resources within their area of responsibility.

4.18.15.6. **(Added-AFTAC)** With the approval of the Senior or Deputy Senior Official for AFTAC's C-InTP, gather the appropriate members of the AFTAC's C-InTP Collaboration Group when threshold-level information is received, or events occur, to provide the responsible commander with recommendations and assistance as needed.

4.18.15.7. **(Added-AFTAC)** Gather, integrate, and analyze indicators of potential insider threat from approved authorized data sources to include, User Activity Monitoring, Enterprise Audit Management, Cybersecurity, Law Enforcement, Counterintelligence, Personnel Security, Human Resources, Command reporting, medical community, Legal and other authorized sources that help detect potential insider threat activity or behaviors and support the assessment of consolidated insider threat risk to the Air Force.

4.18.15.8. **(Added-AFTAC)** Assesses referrals generated from the DAF C-InT Hub for possible initiation of an incident report/notification to the AFTAC Information Security Office for initiation of security incident.

4.18.15.9. **(Added-AFTAC)** Report all imminent threats immediately to local Air Force Office of Special Investigations (AFOSI) and SLD 45 law enforcement desk. Such reportable information includes potential workplace violence or espionage which will result in loss of life/data.

4.18.16. **(Added-AFTAC)** AFTAC Collaboration Group will:

4.18.16.1. **(Added-AFTAC)** Consist of the AFTAC legal Advisor, Cyber Security, Behavioral Health section of the Integrated Resilience Team, Employee Management Representative, the respective unit First Sergeants and C-InTP Liaison. The AFTAC C-InTP Liaison with approval from the Senior or Deputy Senior Official for AFTAC's C-InTP will gather the appropriate members of the AFTAC C-InTP Collaboration Group to provide the responsible commander with recommendations/ assistance. For situations involving civilians, representatives from Personnel Security, Employee Management Representative and AFTAC/JA are required advisors. For military personnel, representatives from Personnel Security, unit First Sergeant and AFTAC/JA are required advisors. For situations involving contractors, representatives from Personnel Security and AFTAC/JA are required advisors. Due to other regulations, some members of the collaboration group will provide advice to the responsible commander independent of the collaboration group.

4.18.16.2. **(Added-AFTAC)** Sign a Non-Disclosure Agreement prior to participating in any C-InT discussions.

4.18.16.3. **(Added-AFTAC)** Will not discuss the C-InT process or decisions with other members without AFTAC's C-InT Liaisons' approval. No restrictions exist for discussions to carry out responsibilities of their respective offices.

4.18.16.4. **(Added-AFTAC)** Will not alert subjects of any ongoing C-InT inquiry. Contact AFTAC C-InT Liaison for guidance.

4.18.17. **(Added-AFTAC)** All military, civilian and contractor personnel will:

4.18.17.1. **(Added-AFTAC)** Report DoD Insider Threat Program enterprise threshold-level events to AFTAC's C-InTP Liaison in a timely matter but no later than 5 business days of discovering the information.

CREIGHTON A. MULLINS, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDD 5205.16, *The DoD Insider Threat Program*, 30 September 2014

DAFI 16-1402, *Counter-Insider Threat Program Management*, 10 May 2024

AFI 33-322, *Records Management and Information Governance Program*, 28 July 2021

10 United States Code (USC) 137, *Under Secretary of Defense for Intelligence and Security,*

44 USC 3554, *Federal agency responsibilities*

44 USC 3557, *National security systems*

Public Law 112-81, Section 922, *National Defense Authorization Act for Fiscal Year 2012*, Insider Threat Detection (10 USC 2224 note)

Public Law 113-66, Section 907(c)(4)(H), *National Defense Authorization Act for Fiscal Year 2014*, Personnel security (10 USC 1564 note)

Public Law 114-92, Section 1086, *National Defense Authorization Act for Fiscal Year* 2016Reform and improvement of personnel security, insider threat detection and prevention, and physical security (10 USC 1564 note)

Public Law 114-328, Section 951, *National Defense Authorization Act for Fiscal Year 2017*

E.O. 12829, as amended, *National Industrial Security Program*

E.O. 12968, as amended, *Access to Classified Information*

E.O. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, June 30, 2008

E.O. 9397, as amended, *Numbering System for Federal Accounts Relating to Individual Persons*

E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*

Prescribed Forms

None

Adopted Forms

DAF Form 847*, Recommendation for Change of Publication*

Office Symbols

A1—Manpower, Personnel, and Services

A1K—Personnel

A2/3—Intelligence, Surveillance and Reconnaissance & Operations

A4—Logistics

A5/8—Plans, Programs and Requirements

A6—Communications

AF—Air Force

AFOSI—Air Force Office of Special Investigations

AFTAC—Air Force Technical Applications Center

AFTAC/CC—Air Force Technical Applications Center Commander

AFTAC/CD—Air Force Technical Applications Center Deputy Commander

AFTAC/IPO—Air Force Technical Applications Center Information Protection Office

ANG—Air National Guard

CoS—Chief of Staff

DAF—Department of the Air Force

DoD—Department of Defense

IPO—Information Protection Office

RegAF—Regular Air Force

SLD—Space Launch Delta 45

SD—Systems Development Directorate

SI—Strategic Integration Directorate

USSF—United States Space Force

Abbreviations and Acronyms

AFI—Air Force Instruction

AFMAN—Air Force Manual

CI—Counter Intelligence

C-InTP—Counter-Insider Threat Program

DAF—Department of the Air Force

DAF C-InT Hub — Department of the Air Force Counter-Insider Threat Hub

DAF C-InTP — Department of the Air Force Counter-Insider Threat Program

DAFI—Department of the Air Force Instruction

DoD—Department of Defense

FY—Fiscal Year

E.O.—Executive Order

NDAA—National Defense Authorization

OUSD (I&S)—Office of the Under Secretary of Defense for Intelligence and Security

OPR—Office of Primary Responsibility

USC—United States Code

Attachment 2

Air Force Technical Applications Center (AFTAC) Counter Insider Threat Program Non-Disclosure Agreement

Figure A2.1. Sample Non-Disclosure Agreement.

CUI

AIR FORCE TECHNICAL APPLICATIONS CENTER (AFTAC) COUNTER INSIDER THREAT PROGRAM NONDISCLOSURE AGREEMENT

1. The AFTAC Counter Insider Threat Program (C-lnTP) performs activities for the purpose of detecting, deterring, and mitigating damage to national security caused by persons with the inside knowledge and access to AFTAC information, facilities, and/or operations. The program operates under the authority of DoDD 5205.I6, The DoD Insider Threat Program, September 30, 2014, Air Force Policy Directive (AFPD) 16-14, Security Enterprise Governance, December 31, 2019, and Department of The Air Force Instruction 16-1402, May 10, 2024. The program has implemented a wide-ranging capability integrating system usage data, with other information on employee behavior/conduct to identify potential risks. The information maintained by the program regarding individuals, requires protection under Privacy Act and Personally Identifiable Information policies. The program also maintains information that demonstrates its detection and monitoring capabilities. Portions of this information must be properly safeguarded as Controlled Unclassified Information (CUI) to protect the privacy of individuals, while other portions are classified and must be protected accordingly to prevent harm to the national security of the United States.

2. The AFTAC Commander, designated as the Senior Official for the AFTAC's C-InTP, has determined it necessary for you to have access to sensitive information compiled and/or developed by the program. This information may include computer monitoring results and analyses of computer system use, personnel security background information, human resource system(s) data, medical and psychiatric records, employee financial data, and law enforcement data much of which is protected by the Privacy Act. The information source may be from AFTAC or other agency networks and/or compiled by the AFTAC C-InTP. It is vital that you understand the sensitivity of this information and the potential harm it may cause by its unauthorized disclosure. While AFTAC employees legally have no expectation of privacy with regard to the use of AFTAC and other agency information systems, the integrated data compiled by the program has the potential for compromising personal privacy protections required for employee personal and personnel data. Therefore, it is critical that all employees, military, civilian and contractor employees having access to this data understand that unauthorized disclosure could cause harm to the reputation and privacy interests of individuals subject to the program's activities, and it could compromise AFTAC's C-InT program.

3. Unauthorized disclosure of information protected by the Privacy Act may result in civil and criminal penalties. Unauthorized disclosure could also impede the United States Government from pursuing legal action. Additionally, you may be given access to information on the detection and monitoring capabilities of system tools used by the program. Information regarding the capabilities of detection and monitoring tools used for insider threat detection is classified and not releasable to foreign nationals. Before you are granted access to this data, you are required to sign this nondisclosure agreement acknowledging the sensitivity of this data, and the terms under which you

CUI
Page 1 of 3

are being granted access. By signing this agreement, you acknowledge that you understand and agree to the concerns and restrictions expressed above, in addition to the following provisions:

a. I acknowledge the Insider Threat Program Senior Designated Official is responsible for the direction, management and oversight of AFTACs' Counter Insider Threat Program.

b. I acknowledge access to counter insider threat tools and methodology specifically developed or acquired to support the C-InTP is controlled by the Senior Designated Official. I will not disclose to individuals not assigned to the program any information about, or provide access to, the tools and methodology without coordination through the AFTAC C-InTP Liaisons and written approval from the Senior Designated Official. Details regarding the development, deployment, and termination of threat detection rule resides solely with the program to prevent compromise of counter insider threat detection activity and or capability.

4. I understand access to audit data collected on user activity is restricted to personnel assigned duties in direct support of C-InTP, and I will not disclose user audit data to others including other members of the AFTAC C-InTP Collaboration Group without the authority of the Senior or Deputy Senior Official. Accordingly, I will not create and or deploy employee specific tailored rule sets or initiate video capture monitoring without approval by the Senior Designated Official. Further, I will not disclose or otherwise reveal information regarding the monitoring of employees to individuals not assigned to the program.

5. I understand disclosure of this information may damage national security by allowing others to detect the direction of a law enforcement investigation or counterintelligence inquiry. Disclosure may also expose law enforcement and counterintelligence capabilities that will greatly hinder the ability to detect dangerous insider activity in future cases.

6. I agree as a condition of access that I shall not use such information for any private purpose; share it with individuals or entities external to the program without permission; disclose to the originator of such information that I have had access to or viewed said content otherwise misuse or mishandle the information to which I have been granted access.

7. These provisions 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 and 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 agreement and are controlling.

8. This agreement does not supersede computer network reporting requirements by designated personnel to U.S. Cyber Command, Department of Defense or other Agencies as required by existing laws, policies and regulations. Additionally, the Incident Reporting requirements remain in effect by my signature below.

9. I acknowledge my participation in the specific case and all privileges are severed once I have provided the information or service request and will not maintain any information on the case in any manner. I also acknowledge my obligation to protect this information remains.

10. I affirm that I have read and understand the limitations set forth in this agreement and agree to abide by these limitations as a condition of access to information. This will be maintained as an operating document within official InTP program materials. In the event that I violate the terms of this agreement, I acknowledge that I may be subject to discipline under AFTAC, AF or DoD security and personnel policies, and applicable federal laws.

_____

Signature Date

_____

Printed Name Title

Attachment 3

Air Force Technical Applications Center (AFTAC) Counter Insider Threat Program Report Process

Figure A3.1. Reporting Process.