BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE INSTRUCTION 16-1402

10 MAY 2024

Operations Support

COUNTER-INSIDER THREAT PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: SAF/AAZ

Certified by: SAF/AAZ
(Mrs. Jennifer M. Orozco)

Supersedes: AFI16-1402, 17 June 2020

Pages: 24

This instruction implements Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*, is consistent with DAFPD 17-2, *Cyber Warfare Operations*, and assigns responsibilities for the oversight and management of the Department of the Air Force Counter-Insider Threat Program (DAF C-InTP). It establishes the requirement to report insider threat-related information and establishes the Department of the Air Force Counter-Insider Threat Hub (DAF C-InT Hub) as the focal point for sharing insider threat-related information and coordinating with the Defense Counterintelligence and Security Agency (DCSA). This publication applies to all Department of the Air Force (DAF) civilian employees and uniformed members of the United States Space Force, Regular Air Force (RegAF), Air Force Reserve, Air National Guard, the Civil Air Patrol when conducting missions as the official Air Force Auxiliary, and those with a contractual obligation to abide by the terms of DAF publications, foreign nationals on a DAF installation obligated under an international agreement to abide by the terms of DAF publications, non-DoD U.S. government agencies whose personnel, by mutual agreement, require support from or conduct operational activity with the DAF. Air Staff roles and responsibilities (e.g., Air Force Deputy Chief of Staff, Manpower and Personnel (AF/A1), etc.) will also apply to the equivalent Office of the Chief of Space Operations (CSO) Space Staff position or office (e.g., Deputy Chief of Space Operations for Personnel (SF/S1), etc.), as appropriate. 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. Supplementary guidance (which includes supplements and separate publications) cannot be less restrictive than the parent publication, but it can be more restrictive. The authorities to waive wing or unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3")

number following the compliance statement. See Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the tier numbers. Submit requests for waivers through the chain of command to the appropriate tier waiver approval authority or alternately to the requestor's commander for non-tiered compliance items. This instruction requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by 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 (NDAA) for Fiscal Year (FY) 2012, Insider Threat Detection (10 USC 2224 note); Public Law 113-66, Section 907(c)(4)(H), NDAA for FY14, Personnel security (10 USC 1564 note); Public Law 114-92, Section 1086, NDAA for FY16, Reform and improvement of personnel security, insider threat detection and prevention, and physical security (10 USC 1564 note); Public Law 114-328, Section 951, NDAA for FY17; Executive Order (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; and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. The applicable system of record notice, Department of Defense (DoD) Insider Threat Management and Analysis Center and DoD Component Insider Threat Records System (March 22, 2019, 84 FR 10803), is available at: **http://dpclo.defense.gov/Privacy/SORNs.aspx**. Refer recommended changes and questions about this publication to the OPR using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through appropriate functional chain of command. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. **(T-2)**

SUMMARY OF CHANGES

This publication has been substantially revised and must be reviewed in its entirety. Major changes include the inclusion of the United States Space Force, revisions for the DAF C-InTP, and incorporation of interim guidance memorandums. Additional revisions include organizational name changes attributed to Headquarters Air Force reorganization and the overall publication reformatting to comply with current publication guidance.

1. Purpose. This publication establishes the following framework to integrate policies and procedures to detect, deter, and mitigate insider threats to national security and DAF assets and establishes implementing guidance to:

1.1. Ensure existing and emerging insider threat awareness, training, and education programs are developed, implemented, and managed in accordance with policy.

1.2. Continuously evaluate personnel by enhancing technical capabilities to monitor and audit user activity on DAF operated information systems, as authorized by law and policy.

1.3. Leverage approved data sources, including but not limited to, antiterrorism, counterintelligence, human resources, law enforcement, workplace violence, publicly available information, security (e.g., cyber, information, industrial, personnel, physical, and operations), and medical to improve existing insider threat detection and mitigation efforts.

1.4. Detect, mitigate, and respond to insider threats through integrated and standardized processes and procedures while ensuring appropriate safeguards for privacy and civil liberty.

1.5. Ensure DAF C-InT Hub personnel coordinate reportable insider threat-related information and post-processed results of system monitoring, as appropriate, in accordance with DoD Insider Threat Program enterprise reporting thresholds published by the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). **(T-0)**

1.6. Establish the requirement for DAF commands to report insider threat-related information to the DAF C-InT Hub. **(T-0)**

2. Department of theAir Force Counter-Insider Threat Overview.

2.1. **DAF C-InTP.** This publication establishes the DAF C-InTP, comprised of personnel, processes, and information sharing procedures associated with the DAF C-InT Hub, information protection offices, and functional specialists amongst the Major Commands (MAJCOMs), Field Commands (FLDCOMs), Direct Reporting Units (DRUs), and Field Operating Agencies (FOAs).

2.2. **DAF C-InT Hub.** The DAF C-InT Hub provides the DAF a centralized capability where all insider threat-related information flows and is subsequently disseminated to the proper functional entities for action or resolution.

2.2.1. The DAF C-InT Hub has sole authority to coordinate insider threat-related information with the DCSA to further the assessment of risk across the DoD and the DAF. **(T-0)**

2.2.2. Assessing risk across the DoD and the DAF enables Commanders to evaluate risk holistically and make informed risk-based decisions.

2.2.3. The DAF C-InT Hub provides mitigation recommendations for Commanders but does not take independent adjudicative or disciplinary action.

2.2.4. The DAF C-InT Hub includes Air Force Intelligence Community (IC) personnel to remediate insider threat matters that impact the IC.

2.3. **DAF Counter-Insider Threat Working Group (C-InT WG).** This publication establishes the DAF C-InT WG to develop strategic goals, support program implementation, integrate policies and procedures, and develop prioritized resource recommendations.

2.3.1. Upon request, the DAF C-InT WG will consist of representatives from the DAF C-InT Hub, offices on the Headquarters of the Department of the Air Force (HAF) staff prescribed in this issuance, and MAJCOM, FLDCOM, or equivalent level information protection directorates. **(T-1)**

2.3.2. The DAF C-InT WG integrates policies and procedures to detect, deter, and mitigate insider threats to national security and Air and Space Force assets.

2.4. **Commanders, Directors, and their Deputies at all levels.** Leaders across the DAF at all levels are critical to the reporting process by ensuring information that meets one or more of the DoD Insider Threat Program enterprise reportable thresholds are reported in a timely manner to their wing, delta, or equivalent level C-InT liaison.

2.4.1. The 13 DoD Insider Threat Program enterprise reporting thresholds are: serious threat, allegiance to the United States, espionage/foreign considerations, personal conduct, behavioral considerations, criminal conduct, unauthorized disclosure, unexplained personnel disappearance, handling protected information, misuse of information technology, terrorism, criminal affiliations, and adverse clearance actions.

2.4.2. The DoD Insider Threat Program enterprise reporting thresholds align with the Security Executive Agent Directive–4, *National Security Adjudicative Guidelines*.

2.4.3. Information protection offices must provide Commanders with training and guidance that provides clarity and objectivity on the DoD Insider Threat Program enterprise reportable threshold events. **(T-1)**

2.4.4. Information protection offices have access to additional information that provides examples of events that may or may not constitute the need for reporting. Unless an incident or series of incidents implicate insider threat concern, it should not form the basis for an insider threat report. Seeking voluntary mental health counseling or being the victim of sexual assault or other violent crimes are examples of events that shall not be reported as an insider threat. **(T-0)**

2.5. **Disclosure Guidance.** 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.

3. Objectives. The DAF C-InTP consist of the following focus areas:

3.1. **Network Monitoring and Auditing.** Available monitoring and auditing capabilities support insider threat detection and mitigation efforts. Monitoring and auditing capabilities will be integrated into the overall insider threat mitigation process. Capabilities should be constantly improved to meet current and future DAF mission requirements and to proactively incorporate best practices to prevent and detect anomalous activity. All monitoring will be conducted in accordance with applicable law and policy.

3.2. **Information Sharing.** An effective C-InTP relies upon timely sharing of information. To effectively assess holistic risk, the DAF C-InT Hub needs timely, recurring, and electronic access to data in an intelligible form. Consistent with DoD Directive (DoDD) 5205.16, *The DoD Insider Threat Program*, the DAF has authority to establish a centralized capability to access, analyze, and store personally identifiable information, protected health information, and law enforcement sensitive information, relevant to countering insider threat. Counterintelligence, security, law enforcement, medical, legal, and human resources policies must ensure that relevant information, as permissible by law and policy, is shared with the DAF C-InT Hub to clarify insider threat matters and support mitigation recommendations for the Commander. **(T-0)** Information sharing, and access will be consistent with Department of the Air Force Instruction (DAFI) 90-7001, *Enterprise Data Sharing & Data Stewardship*. **(T-1)**

3.3. **Training and Awareness.** DAF C-InTP personnel must receive training to ensure adherence to privacy, whistleblower, records retention, civil liberties, and information sharing requirements. **(T-0)**. Commanders and supervisors must receive training on identifying, reporting, and mitigating insider threats **(T-3)**. Additionally, all DAF employees are required to complete insider threat training within 30 days of hire, and annually thereafter. **(T-2)**

3.4. **Insider Threat Reporting and Response.** Airmen and Guardians at risk typically exhibit concerning behavior associated with interpersonal, technical, financial, personal, mental health, social network, foreign travel, or a combination of. Reporting and sharing behaviors of concern is necessary to assess holistic risk and appropriate response options. Proactive and early reporting increases the likelihood of positive and favorable outcomes.

4. Roles and Responsibilities.

4.1. **Administrative Assistant to the Secretary of the Air Force (SAF/AA) is the senior official of the DAF C-InTP and will provide policy, oversight, and management of the DAF C-InTP. (T-1)** In accordance with this issuance and Headquarters Air Force Mission Directive 1-6, *Administrative Assistant to the Secretary of the Air Force*, SAF/AA will:

4.1.1. Serve as the HAF lead authority for the C-InTP, coordinating and engaging across the HAF staff to collaborate, integrate, and remediate conflicts in policy or guidance associated with the detection, deterrence, and mitigation of insider threats. **(T-1)**

4.1.2. Ensure DAF C-InTP activities are synchronized and integrated with DAF mission assurance with respect to the protection of DAF and DoD critical assets and missions. **(T-0)**

4.1.3. In coordination with the DAF Chief Information Officer (SAF/CN), Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6), and Deputy Chief of Space Operations for Intelligence (SF/S2), maintain oversight of user activity monitoring (UAM) tools, requirements, configuration, use, and any acquisition from cyber elements or service providers that provide UAM capabilities for the DAF. **(T-1)**

4.1.4. Issue policy and guidance for UAM in coordination with SAF/CN, AF/A2/6, SF/S2, as needed. **(T-1)**

4.1.5. Ensure, to include by issuing authoritative guidance, that any relevant data and information needed to clarify or assess risk posed to the DAF is made available to the DAF C-InT Hub on a timely and reoccurring basis consistent with DAFI 90-7001, *Enterprise Data Sharing & Data Stewardship*. **(T-1)**

4.1.6. Identify the necessary requirements for the DAF C-InTP and request sufficient resources, through appropriate channels, in collaboration with relevant stakeholders. **(T-1)**

4.1.6.1. Advocate for the resources necessary for the DAF C-InTP to execute requirements, on behalf of planning, programming, budgeting, and execution (PPBE) objectives, within the DAF corporate structure. **(T-1)**

4.1.7. Provide an annual report to the Secretary of the Air Force on the state of the DAF C-InTP, including program accomplishments, resource requirements, insider threat risks, program impediments or challenges, and recommendations for program improvements. **(T-0)**

4.1.8. Ensure the DAF C-InTP is integrated with the DAF's operations security program, in accordance with National Security Presidential Memorandum-28, *The National Operations Security Program*. **(T-0)**

4.1.9. Delegate duties and responsibilities, applicable to the role of senior official of the DAF C-InTP, to the Director, Security, Special Program Oversight and Information Protection (SAF/AAZ), as needed. **(T-1)**

4.2. **Director, Security, Special Program Oversight and Information Protection (SAF/AAZ) will:**

4.2.1. Serve as the designated senior representative to SAF/AA for the DAF C-InTP, responsible for the management and accountability of the DAF C-InTP. **(T-1)**

4.2.1.1. Perform duties and responsibilities of senior official of the DAF C-InTP, as delegated by SAF/AA. **(T-1)**

4.2.2. Provide oversight for the DAF C-InTP and coordinate with stakeholders to promulgate policy. **(T-1)**

4.2.3. Integrate insider threat detection, mitigation, and information sharing procedures into applicable special access program and security policies where appropriate. **(T-1)**

4.2.4. Promulgate policies and procedures supporting the monitoring and auditing of special access program networks and assets for insider threat detection and mitigation in accordance with DAF and IC policies for special access programs. **(T-1)**

4.2.5. Establish processes and procedures for reporting unauthorized disclosures attributed to DAF personnel to the DAF C-InT Hub. **(T-1)**

4.2.6. Ensure any DAF entity that utilizes UAM capabilities outside of the DAF C-InT Hub has received written concurrence from SAF/AA and developed procedures to securely share and provide timely and electronic access to relevant information indicative of risk or potential threat with the DAF C-InT Hub. **(T-1)**

4.2.7. Support the mission assurance assessment process for the DAF C-InTP, in collaboration with the appropriate mission assurance entities. **(T-1)**

4.2.7.1. Evaluate findings provided by DAF mission assurance staff associated with the DAF C-InTP and address systemic issues identified, as needed. **(T-1)**

4.2.8. Establish a training plan for the DAF C-InTP. **(T-1)**

4.2.9. Approve data sources and other information for integration into the DAF C-InTP. **(T-1)**

4.2.10. Chair and facilitate the DAF C-InT WG and represent DAF C-InT WG equities at insider threat-related forums amongst the DoD. **(T-1)**

4.2.10.1. Ensure the DAF C-InT WG is employed to monitor implementation, progress, and maturity of the DAF C-InTP. **(T-1)**

4.2.10.2. Ensure the DAF C-InT WG coordinates recommendations and challenges with DoD. **(T-1)**

4.2.11. Ensure insider threat response action procedures, such as insider threat administrative investigations, are established to clarify or support matters related to insider threat risk. **(T-1)**

4.2.12. Ensure procedures are established for documenting insider threat matters reported and mitigation and response action(s) taken. **(T-1)**

4.2.13. Provide a representative to departmental and interagency forums engaged in countering insider threats. **(T-1)**

4.2.14. Advocate and program for appropriate resources to establish and maintain the DAF C-InTP. **(T-1)**

4.2.15. Facilitate oversight reviews by cleared officials, on behalf of the DAF C-InT Hub, to ensure compliance with applicable law and policy guidelines, including privacy and civil liberty protections. **(T-1)**

4.3. **Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ) and the Assistant Secretary of the Air Force for Space Acquisition and Integration (SAF/SQ) will:**

4.3.1. Ensure policies and procedures are in place to support implementation or compliance with insider threat requirements applicable to the DAF C-InTP and the national industrial security program. **(T-1)**

4.4. **Department of the Air Force Chief Information Officer (SAF/CN) will:**

4.4.1. Promulgate policies and procedures that support monitoring and auditing of applicable networks and assets to support insider threat deterrence, detection, and mitigation. **(T-1)** All monitoring will be conducted in accordance with applicable law and policy.

4.4.2. Promulgate policies, strategy, and procedures that support the integration of cybersecurity activities with the DAF C-InTP, enabling and allowing for regular and timely access to network and system audit information for DAF C-InT Hub personnel to support the identification, analysis, and resolution of insider threat issues. **(T-1)**

4.4.3. Ensure UAM and other applicable DAF C-InTP requirements are incorporated into PPBE processes and coordinate programming data, briefings, and spend plans with SAF/AAZ and the insider threat resource management council, in accordance with Headquarters Operating Instruction (HOI) 65-6, *Insider Threat Resource Governance and Management Process*. **(T-1)**

4.4.4. Develop guidelines and procedures for the retention of records and documents pertaining to insider threat inquiries. **(T-1)**

4.4.5. Ensure the DAF C-InTP and insider threat awareness activities are incorporated into cybersecurity awareness activities. **(T-1)**

4.4.6. Incorporate UAM and the DAF C-InTP into strategic planning regarding the protection of national security systems. **(T-0)** This includes implementation of the National Security Memorandum-8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*. **(T-0)**

4.5. **General Counsel of the Department of the Air Force (SAF/GC) will:**

4.5.1. Through the Deputy General Counsel, Intelligence, International and Military Affairs Division (SAF/GCI), provide oversight of the attorney-advisor embedded in the DAF C-InT Hub, who will ensure DAF C-InT Hub processes, procedures, access to information and data, and deliverables are consistent with applicable law and policy. **(T-1)**

4.5.2. Provide oversight and guidance on all legal matters pertaining to C-InTP policy, procedures, and activities. **(T-1)**

4.5.3. Review and provide consultation regarding the availability of C-InTP derived information for the purposes of disciplinary proceedings including courts-martial, non-judicial punishment, and adverse administrative proceedings. **(T-1)**

4.6. **The Office of the Judge Advocate General of the Air Force (AF/JA) will:**

4.6.1. Provide oversight and guidance on all legal matters pertaining to C-InTP policy. **(T-1)**

4.6.2. Review and provide advice regarding the availability of C-InTP derived information for the purposes of disciplinary proceedings including courts-martial, non-judicial punishment, and adverse administrative proceedings. **(T-1)**

4.7. **Deputy Under Secretary of the Air Force for International Affairs (SAF/IA) will:**

4.7.1. Ensure policies and procedures associated with credentialed recurring access decisions for international military students and their accompanying family members, military-sponsored visitors, and the DAF security cooperation enterprise are integrated with the DAF C-InTP. **(T-1)**

4.7.2. Promulgate policy to establish the DAF international military student assessment panel—responsible for credential recurring access determinations for international military students and their accompanying family members for DAF training installations in the United States (US) when derogatory information is discovered that may lead to an assessment of potential risk. **(T-1)** This authority applies to fitness determinations prior to US travel.

4.7.3. Promulgate policy and guidance to ensure international military student offices are trained in insider threat reporting requirements. **(T-1)**

4.8. **Department of the Air Force Inspector General (SAF/IG) will:**

4.8.1. Integrate insider threat awareness training as provided by the DAF C-InTP. **(T-1)**

4.8.2. Ensure procedures are established to securely provide DAF C-InT Hub personnel regular, timely, and electronic access to information necessary to identify, analyze and resolve insider threat issues. **(T-1)**

4.8.3. Provide access to counterintelligence and law enforcement reporting and analytic products relevant to insider threat. **(T-1)**

4.8.4. Audit DAF C-InTP personnel's handling, use, and access to records and data. **(T-1)**

4.8.5. Provide audits and inspections of DAF C-InTP activities for the MAJCOMs, FLDCOMs, DRUs, and FOAs. **(T-1)**

4.8.6. Enable and oversee the Department of the Air Force Office of Special Investigations (AFOSI) in supporting DAF C-InTP activities in accordance with section 4.20 of this issuance and guidance from SAF/AA. **(T-1)**

4.8.7. Ensure insider threat requirements are incorporated into PPBE processes and programming data, briefings, and spend plans are coordinated with SAF/AAZ and the insider threat resource management council, in accordance with HOI 65-6. **(T-1)**

4.9. **Assistant Secretary of the Air Force for Manpower and Reserve Affairs (SAF/MR) will:**

4.9.1. Ensure procedures are established to securely provide DAF C-InT Hub personnel regular, timely, and electronic access to information necessary to identify, analyze, and resolve insider threat matters as permissible by law and policy. Such access and information include adjudicated outcomes on personnel security appeal decisions and equal opportunity cases. **(T-1)**

4.10. **Director of Public Affairs (SAF/PA) will:**

4.10.1. Promulgate policies and procedures to support the integration of insider threat awareness into DAF-wide public affairs operations and capabilities, including social media, articles, and graphics. **(T-1)**

4.10.2. Provide communication planning expertise to SAF/AA in efforts related to insider threat awareness. **(T-1)**

4.10.3. Provide guidance to SAF/AA and the DAF C-InTP as it pertains to policy and procedures associated with the use of publicly available information and social media in DAF C-InTP operations. **(T-1)**

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

4.11.1. Promulgate suitability policies and procedures to support insider threat deterrence, detection, and mitigation. **(T-1)**

4.11.2. Ensure procedures are established to securely provide DAF C-InT Hub personnel regular, timely, and electronic access to the information necessary to identify, analyze, and resolve insider threat matters. **(T-0)** Such access will include relevant human resources databases and files, such as personnel files, outsider activities requests, disciplinary files, unfavorable information files, senior official unfavorable information files, climate survey information, and personal contact records, as may be necessary for resolving or clarifying insider threat matters. **(T-0)**

4.11.3. In coordination with SAF/AA, SAF/GC, and AF/JA, establish procedures for access requests by DAF C-InT Hub personnel involving particularly sensitive or protected information. **(T-1)**

4.11.4. Establish reporting guidelines for relevant organizational components, including the Air Force Personnel Center, to refer relevant insider threat information to the DAF C-InTP. **(T-1)**

4.11.5. Provide guidance to SAF/AA on integrating and vetting insider threat education and training requirements into applicable accessions, professional military education, professional continuing education, and ancillary training. **(T-1)**

4.12. **Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations (AF/A2/6) will:**

4.12.1. In coordination with SAF/AA, support the implementation and management of UAM on applicable assets and networks, including the Air Force IC information environment and Air Force Network. **(T-1)**

4.12.2. Promulgate policies and procedures that support monitoring and auditing of assets and networks to support insider threat detection and mitigation. **(T-1)**

4.12.2.1. Ensure user attributable auditing of Air Force sensitive compartmented information (SCI) activities are implemented in accordance with applicable IC standards. **(T-1)**

4.12.2.2. Ensure user attributable auditing information collected from Air Force SCI activities is shared with the DAF C-InT Hub **(T-1)**

4.12.3. Ensure procedures are established to securely provide DAF C-InT Hub personnel regular, timely, and electronic access to information necessary to identify, analyze and resolve insider threat issues. **(T-0)**

4.12.4. Enable DAF C-InT Hub access to publicly available information capabilities and reporting products associated with intelligence or cyber activities relevant to insider threat. **(T-1)**

4.12.5. Ensure UAM and other applicable DAF C-InTP requirements are incorporated into PPBE processes and coordinate programming data, briefings, and spend plans with SAF/AAZ and the insider threat resource management council, in accordance with HOI 65-6. **(T-1)**

4.12.6. Provide guidance to Commander, AFOSI, on implementation of Intelligence Community Directive (ICD) 750, *Counterintelligence Programs*. **(T-1)**

4.12.7. Incorporate UAM and the DAF C-InTP into strategic planning regarding the protection of national security systems. **(T-0)** This includes implementation of the National Security Memorandum-8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*. **(T-0)**

4.13. **Deputy Chief of Staff for Operations (AF/A3) will:**

4.13.1. Ensure procedures are established to securely provide DAF C-InT Hub personnel with regularly, timely, and electronic access to reporting associated with communications security monitoring and activities relevant to insider threat. **(T-0)**

4.13.2. Ensure insider threat awareness and reporting requirements are integrated into operations security policy, planning, and awareness efforts. **(T-1)**

4.13.3. Ensure operational reporting reports that meet DoD Insider Threat Program enterprise reporting thresholds and in accordance with Air Force Manual (AFMAN) 10-206, *Operational Reporting (OPREP)*, are shared with appropriate SAF/AA personnel, including the DAF C-InT Hub. **(T-1)**

4.14. **Deputy Chief of Staff, Logistics, Engineering and Force Protection (AF/A4) will:**

4.14.1. Ensure procedures are established to securely share physical security, law enforcement, and other applicable information relative to insider threat with DAF C-InT Hub personnel for the purpose of identifying, analyzing, and resolving insider threat issues. **(T-0)**

4.14.2. Coordinate with appropriate entities to facilitate and enable the sharing of information relative to insider threat with the DAF C-InT Hub for the purpose of identifying, analyzing, and resolving insider threat issues. **(T-1)**

4.14.3. Promulgate policies and procedures to support insider threat deterrence, detection, and mitigation. **(T-1)**

4.14.4. Integrate insider threat detection and reporting procedures into applicable security-related policies. **(T-1)**

4.15. **Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration (AF/A10) will:**

4.15.1. Promulgate policies and procedures associated with the personnel reliability assurance program to support the integration of insider threat reporting and deterrence. **(T-1)**

4.15.2. Ensure procedures are established to securely provide the DAF C-InT Hub with relative information associated with individuals that are enrolled in, decertified, or removed from the personnel reliability assurance program for the purpose of identifying, analyzing, and resolving insider threat issues. **(T-1)**

4.16. **Air Force Surgeon General (AF/SG) will:**

4.16.1. In coordination with the Defense Health Agency, ensure policies and procedures are in place with the Air Force Medical Command Agency for the sharing of information relevant to insider threats, as authorized by law and policy. **(T-1)**

4.16.2. Ensure policies and procedures are in place requiring commanders to promptly share information identified as a result of command-directed evaluation to a mental healthcare provider with the DAF C-InTP that meets one of the DoD Insider Threat Program enterprise thresholds or is considered a potential risk indicator. **(T-0)** The disclosure of information causing or resulting from a command-directed evaluated referral is authorized pursuant to AFI 44-172, *Mental Health.*

4.17. **Major Command, Field Command, Direct Reporting Unit, and Field Operating Agency Commanders will:**

4.17.1. Designate the information protection directorate to provide oversight, guidance, and supplemental policy, as appropriate, regarding implementation of the C-InTP. **(T-2)** This includes but is not limited to the following:

4.17.1.1. Provide oversight of C-InTP annual self-assessments through the management internal control toolset (MICT) self-assessment checklist (SAC), in accordance with DAFI 90-302, *The Inspection System of the Department of the Air Force*. **(T-1)** Recommendations must be provided to SAF/AAZ to improve the C-InTP MICT SAC, as needed. **(T-2)**

4.17.1.2. Submit consolidated list of designated C-InT liaisons to the DAF C-InT Hub in the form of an appointment memorandum. **(T-1)** This list must be reviewed annually and updated, as needed. **(T-2)**

4.17.1.3. Ensure C-InT liaisons are designated at the wing, delta, or equivalent level host-based information protection offices. **(T-1)**

4.17.1.4. Ensure reporting is routed through the host-based information protection offices, as applicable. **(T-1)**

4.17.1.5. Identify an information protection office to report on behalf of wings, deltas, or equivalent organizations that reside on an installation or facility hosted by a sister Service or non-DAF entity. **(T-2)**

4.17.1.6. Ensure all subordinate organizations are covered by an information protection office for reporting purposes. **(T-1)**

4.17.2. Ensure the security program executive and information protection directorate promote a month-long awareness and information campaign each September to inform all DAF-affiliated personnel of potential threats and risks posed by insiders and how to report. **(T-2)**

4.17.3. Coordinate significant insider threat issues relative to their command with SAF/AA through the security program executive. **(T-2)**

4.17.4. Ensure information protection directorates are adequately resourced to provide program management and oversight of the C-InTP for the command. **(T-2)**

4.17.5. Ensure all Commanders, Directors, or their Deputies at the wing, delta, or equivalent level and below are trained on the DoD Insider Threat Program enterprise reporting thresholds. **(T-1)**

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

4.18.1. Designate member(s) of the host base information protection office to serve as C-InT liaison(s) to coordinate reporting actions. **(T-1)** Appointment designations at the wing, delta, or equivalent level must be submitted to the MAJCOM, FLDCOM, or equivalent level information protection directorate. **(T-2)** C-InT liaisons must facilitate insider threat reporting actions to and from the DAF C-InT Hub on behalf of the host base Commander and do the following:

4.18.1.1. Request an account or access to the designated reporting platform with the DAF C-InT Hub within two weeks of appointment through their MAJCOM, FLDCOM, or equivalent level information protection directorate. **(T-2)**

4.18.1.2. Report DoD Insider Threat Program enterprise threshold-level events to the DAF C-InT Hub and ensure required information is entered into the designated reporting platform. **(T-0)**

4.18.1.3. Ensure Commanders, Directors, or their Deputies have access to and are trained on the 13 DoD Insider Threat Program enterprise reporting thresholds and potential risk indicators (PRIs). **(T-2)**

4.18.1.4. Follow reporting procedures, as determined by the Director, C-InT Hub. **(T-1)**

4.18.1.5. Establish processes and procedures for gathering and reporting information to and from the DAF C-InT Hub. **(T-2)** Processes and procedures must cover wing, delta, or equivalent level tenants. **(T-2)** Information must be coordinated to ensure the host installation commander is able to manage the risk to their assets and resources within their area of responsibility. **(T-2)**

4.18.1.6. Assess referrals generated from the DAF C-InT Hub for possible opening of a security incident, administrative or criminal investigation, or other commander directed actions in coordination with base level authorities responsible for taking appropriate action or responding to referred information. **(T-2)**

4.18.1.7. 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 twenty (20) business days. **(T-1)** Ensure the Hub receives the final disposition or outcome of all reporting actions to and from the C-InT Hub once they have been concluded if it has not yet been provided. **(T-1)**

4.18.1.8. Promote a month-long awareness and information campaign each September, in coordination with the information protection directorate, to inform all DAF-affiliated personnel of potential threats and risks posed by insiders and how to report. **(T-3)**

4.18.1.9. Ensure personnel reliability assurance program security concerns are integrated with insider threat reporting actions, as appropriate **(T-1)**. Guidance on the personnel reliability assurance program is provided in Department of Defense Manual (DoDM)5210.42_DAFMAN13-501, *Nuclear Weapons Personnel Reliability Program (PRP)*.

4.18.1.10. Complete training in privacy and civil liberties. **(T-0)** This can be accomplished through the completion of online learning course, insider threat privacy and civil liberties, INT260.16, located on the center for development of security excellence website (**www.cdse.edu/**).

4.18.2. Ensure all personnel under their authority and responsibility are covered by a C-InT liaison(s). **(T-2)**

4.18.3. Establish a routine process with the designated C-InT liaison(s), to ensure awareness of all reporting actions to and from the DAF C-InT Hub under their authority and responsibility. **(T-1)**

4.18.4. Ensure any incident or behavior that meets one or more DoD Insider Threat Program enterprise threshold-level events are reported to the DAF C-InT Hub through the reporting platform and method designated by the DAF C-InT Hub in a timely manner but no later than 20 business days and respond to DAF C-InT Hub requests for information. **(T-1)** Commanders who are unsure of whether an event meets a DoD Insider Threat Program enterprise threshold should coordinate with the MAJCOM, FLDCOM, or equivalent level information protection directorate to determine whether reporting is required. Reportable events include the following:

4.18.4.1. Security incidents in accordance with DoDM 5200.01V3_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information*, and DoDM 5200.02_DAFMAN 16-1405, *Air Force Personnel Security Program*. **(T-0)** If an individual is removed from the personnel reliability assurance program for a security incident, the Commander is required to provide notification to the C-InT liaison. **(T-1)**

4.18.4.2. A credible report or suspicion of extremist activities, in accordance with DAFI 51-508, *Political Activities, Free Speech and Freedom of Assembly*. **(T-0)**

4.18.4.3. Any allegation that results in the initiation of a command directed or criminal investigation when it, if substantiated, would meet one or more DoD Insider Threat Program enterprise threshold level events. **(T-0)** Commanders must ensure victim and third-party identifying information is redacted. **(T-0)**

4.18.4.4. Information that meets one or more DoD Insider Threat Program enterprise threshold level events identified during Command-Directed Evaluations to a mental healthcare provider. **(T-0)**

4.18.4.5. Information related to the international military student population and their accompanying family members who are assigned to a DAF installation or training facility that meets one or more DoD Insider Threat Program enterprise threshold level events. **(T-0)**

4.18.4.6. Events or information which are disclosed, admitted to, or remain unsolved as a result of a polygraph process and meets one or more DoD Insider Threat Program enterprise threshold level events. **(T-0)**

4.18.4.7. Intentional and unintentional unauthorized disclosures that are user-attributed or attributed to DAF personnel. **(T-0)** Information regarding unauthorized disclosures attributed to personnel with an unknown government affiliation may be provided to the DAF C-InT Hub to support identity resolution.

4.18.4.8. Adverse or questionable information concerning a contractor employee who has been cleared or is in the process of being cleared for access to classified information which may indicate that such access is not clearly consistent with national interest and in accordance with DoDM 5220.22V2_AFMAN 16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*. **(T-1)**

4.18.5. Ensure reporting is coordinated through the unit of assignment for individuals assigned to Air Force Reserve Components. **(T-1)**

4.18.6. Ensure all Commanders, Directors, and their staffs are trained on how to report incidents that meet one or more DoD Insider Threat Program enterprise threshold level events. **(T-1)**

4.18.7. Ensure the C-InTP SACs are completed annually through MICT, in accordance with DAFI 90-302, *The Inspection System of the Department of the Air Force*. **(T-1)**

4.18.8. Ensure host base information protection offices are adequately resourced to fulfill C-InTP responsibilities for the command. **(T-2)**

4.19. **Director, DAF C-InT Hub will:**

4.19.1. Serve as the responsible supervisor for planning, directing, organizing, and exercising control over C-InT Hub personnel and resources. **(T-1)**

4.19.2. Establish, mature, and sustain a centralized multi-disciplinary capability to gather, integrate, and analyze indicators of potential insider threats from approved authorized data sources to include:

4.19.2.1. UAM. **(T-0)**

4.19.2.2. Enterprise Audit Management. **(T-0)**

4.19.2.3. Cybersecurity and Information Assurance. **(T-0)**

4.19.2.4. Law Enforcement. **(T-0)**

4.19.2.5. Counterintelligence. **(T-0)**

4.19.2.6. Personnel, Physical, and Information Security. **(T-0)**

4.19.2.7. Human Resources (including civilian and military personnel management) **(T-0)**

4.19.2.8. Command Reporting. **(T-0)**

4.19.2.9. Medical Community. **(T-0)**

4.19.2.10. Legal. **(T-0)**

4.19.2.11. Publicly Available Information. **(T-0)**

4.19.2.12. Inspector General. **(T-0)**

4.19.2.13. Other authorized sources that help detect or clarify potential insider threat activity or behaviors and support the assessment of holistic insider threat risk to the DAF. **(T-1)**

4.19.3. Establish approximate timelines to provide deliverables to the commander or civilian equivalent based on risk level or severity upon receipt of reportable events. **(T-1)** Notification to risk owners must be provided when factors arise that impede the DAF C-InT Hub from meeting the established approximate timelines. **(T-1)**

4.19.4. Establish procedures for DAF entities to submit request for information in support of their administrative, counterintelligence, or criminal investigations. **(T-1)**

4.19.5. Establish internal procedures for insider threat analysis, insider threat referral processes, and operations. **(T-1)** Process and procedures must be established within a comprehensive standard operating procedures doctrine and approved by SAF/AAZ. **(T-1)** At a minimum, the procedures must provide the following:

4.19.5.1. Procedures for receiving, validating, and investigating field-level allegations and other reporting that has not been previously validated by a government entity. **(T-1)** These procedures must be coordinated with AFOSI liaisons to the DAF C-InT Hub. **(T-1)**

4.19.5.2. Process and procedures to ensure insider threat response actions, such as initiating insider threat administrative investigations and responding to inquiries, are in place to clarify or support matters related to insider threat risk. **(T-1)**

4.19.5.3. Process and procedures for documenting insider threat matters reported and response action(s) taken. **(T-1)**

4.19.5.4. Process and procedures to share information with the designated senior official that will inform on reportable events associated with general officers, flag officers, and senior executive service staff. **(T-1)**

4.19.5.5. Process and procedures to hold information or results in abeyance when it has been determined necessary by the entity leading an administrative or criminal investigation. **(T-1)**

4.19.5.6. Process and procedures to conduct independent audits of DAF C-InT Hub personnel with access to UAM tools. **(T-1)**

4.19.5.7. Handling and safeguarding privileged communications if acquired inadvertently through authorized monitoring. **(T-1)**

4.19.6. Maintain operational control and validation authority of UAM tools, requirements, configuration, use, and acquisition from cyber elements or service providers that provide UAM capabilities. **(T-1)** Requirements and configurations must be approved by the embedded SAF/GCI attorney/advisor and periodically reviewed. **(T-1)**

4.19.7. Ensure the functions and activities of the DAF C-InT Hub will not interfere with nor impede existing functional area (e.g., cybersecurity, personnel security, human resources) processes, investigative authorities, execution of statutory and policy requirements, or command responsibilities to maintain good order and discipline within the DAF. **(T-1)**

4.19.8. Establish and employ an advanced analytics capability with data integration methodologies to identify risks. **(T-1)**

4.19.9. Ensure all DAF C-InT Hub personnel with access to DAF C-InTP records, data, and UAM methods and results are trained on:

4.19.9.1. How to handle, protect, and store the sources of information in accordance with their classification or as controlled unclassified information. **(T-0)** This must be done in accordance with DoDM 5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification and Declassification,* DoDM 5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Classified Information,* and DoDM 5200.01V3_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information*. **(T-0)**

4.19.9.2. Providing these data sources only on a strict need-to-know basis to individuals only after validating the individual's authority to have such records. **(T-1)**

4.19.9.3. 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 in accordance with the Air Force Records Disposition Schedule located in the Air Force Records Information Management System. **(T-2)** This is the system for addressing National Archives and Records Administration General Records Schedule 5.6: Security Records, as approved by the Headquarters Air Force Records Manager, and in accordance with the existing applicable System of Records Notice.

4.19.9.4. Privacy and civil liberties. **(T-0)**

4.19.10. Deliver to the DCSA post-processed results in accordance with DoD Insider Threat Program enterprise thresholds published by the OUSD(I&S). **(T-0)**

4.19.11. Ensure all individuals (i.e., contractor, civilian, or RegAF, Air Force Reserve, Air National Guard, and Space Force) working within the DAF C-InT Hub, sign individual non-disclosure agreements with the government and maintain them for two years after employment is terminated. **(T-1)**

4.19.12. Develop and provide guidance to major command, field command, direct reporting unit, and field operating agency designated C-InT liaisons on minimum information requirements for reporting. **(T-1)**

4.19.13. Ensure MAJCOM, FLDCOM, DRU, and applicable FOA designated C-InT liaisons have access to the most current version of the DoD Insider Threat Program enterprise thresholds and PRIs. **(T-1)**

4.19.14. Manage the designated reporting platform. **(T-1)**

4.19.15. Ensure that each data source is approved by SAF/AAZ before being incorporated into the DAF C-InT Hub. **(T-1)**

4.19.16. Integrate policies into procedures to deter, detect, and mitigate insider threats to DAF assets. **(T-1)**

4.19.17. Submit reports regarding contractor personnel to the DCSA when information becomes known to the government contracting activity that suggests the contractor employee poses a significant risk to the DoD, in accordance with DoDM 5220.32, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, unless it is has been confirmed that the government contracting activity has already submitted reporting to the DCSA. **(T-1)**

4.19.18. Provide appropriate reporting to the Air Force IC security coordination center for incidents regarding personnel or users attributed to SCI networks and information. **(T-1)**

4.20. **Commander, Department of the Air Force Office of Special Investigations (AFOSI) will:**

4.20.1. Assign AFOSI personnel to the DAF C-InT Hub to serve as liaisons and support staff. **(T-1)** At a minimum, AFOSI personnel assigned to the DAF C-InT Hub will:

4.20.1.1. Evaluate information to determine whether counterintelligence or law enforcement support is necessary and ensure actions are documented in accordance with Hub procedures. **(T-0)**

4.20.1.2. Facilitate information sharing from AFOSI Tip Line that contain credible allegations. **(T-1)**

4.20.1.3. Provide relevant counterintelligence and law enforcement information. **(T-0)**

4.20.1.4. Support general operations, including case management and analysis, as needed. **(T-1)**

4.20.1.5. Conduct counterintelligence analysis. **(T-0)**

4.20.1.6. Coordinate with AFOSI detachments regarding insider threat related incidents, as needed. **(T-1)**

4.20.2. Ensure AFOSI activities related to countering insider threats are coordinated with the DAF C-InT Hub. **(T-1)**

4.20.3. Coordinate programming data, briefings, and spend plans with SAF/AAZ and the insider threat resource management council, in accordance with HOI 65-6. **(T-1)**

4.20.4. Ensure capabilities resourced to support AFOSI insider threat activities are integrated with and shared in support of DAF C-InT Hub activities. **(T-1)**

4.20.5. Establish procedures to securely provide the DAF C-InT Hub recurring, timely, and electronic access to law enforcement and counterintelligence information, including information from currently open and closed case files, polygraph examination results, and eGuardian reports, to support the identification, analysis, and resolution of insider threat matters. On a case-by-case basis, the Commander, AFOSI, may reasonably delay reporting in joint-agency investigations in which AFOSI is not the lead investigative agency. **(T-0)**

4.20.6. Coordinate counterintelligence policies and guidance with AF/A2/6 to ensure compliance with IC issuances, including but not limited to the ICD 750.

4.21. **Commander, Sixteenth Air Force (16 AF) will:**

4.21.1. Establish procedures to securely share and provide DAF C-InT Hub personnel with reoccurring, timely, and electronic access to information and data related to insider threat, including network and system audit information from cybersecurity activities relevant to insider threat. **(T-0)**

4.21.2. Ensure the Air Force information network security operations center provides the DAF C-InT Hub with read-only access to cybersecurity event reporting systems and/or databases to provide situational awareness of user-attributable cybersecurity events indicating deliberate misuse of information technology or a pattern of negligent noncompliance with policies, rules, procedures, guidelines, or regulations pertaining to information technology. **(T-0)**

4.22. **Commander, Air Force Installation and Mission Support Center (AFIMSC) will:**

4.22.1. Securely share and provide reoccurring, timely, and electronic access to information and data relative to insider threat, as permissible by law and policy, to DAF C-InT Hub personnel. **(T-0)** Such access and information include physical security, force protection, law enforcement, counterintelligence, human resources, payroll and voucher files, and other applicable information relevant to insider threat. **(T-0)**

4.23. **Commander, Air Force Personnel Center (AFPC) will:**

4.23.1. Securely share and provide reoccurring, timely, and electronic access to information and data relative to insider threat, as permissible by law and policy, to DAF C-InT Hub personnel. **(T-0)** Such access and information include military and civilian personnel management, human resources, and other applicable information relevant to clarifying insider threat matters. **(T-0)**

4.24. **All personnel with access to DAF C-InTP Records, Data, and UAM Methods and Results will:**

4.24.1. Take prudent steps to protect insider threat-related information from unauthorized disclosure. **(T-0)**

4.24.2. Be properly trained on how to handle, protect, and store this information. **(T-0)**

4.24.2.1. Handle, protect, and store this information in accordance with their classification or as controlled unclassified information. **(T-0)** This must be done in accordance with DoDM 5200.01V1_AFMAN16-1404V1, DoDM 5200.01V2_AFMAN16-1404V2, and DoDM 5200.01V3_AFMAN16-1404V3. **(T-0)**

4.24.3. Provide insider threat information only on a strict need-to-know to individuals only after validating the individual's authority to have such records. **(T-1)**

EDWIN H. OSHIBA
Administrative Assistant

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 USC § 552a, *Records maintained on individuals* (Privacy Act of 1974)

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 44-172, *Mental Health*, 13 November 2015

AFMAN 10-206, *Operational Reporting (OPREP)*, Incorporating Change 1, 1 September 2020

AFPD16-14, *Security Enterprise Governance*, 31 December 2019

Committee on National Security Systems Directive 504, *Directive on Protecting National Security Systems from Insider Threat*, 15 September 2021

DAFI 51-508, *Political Activities, Free Speech and Freedom of Assembly*, *24 March 2023*

DAFI 90-160, *Publications and Forms Management*, 21 June 2023

DAFI 90-302, *The Inspection System of the Department of the Air Force*, 15 March 2023

DAFI 90-7001, *Enterprise Data Sharing & Data Stewardship*, 22 April 2021

DAFPD 17-2, *Cyber Warfare Operations*, 22 October 2020

DAFMAN 90-161, *Publishing Processes and Procedures*, 18 October 2023

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

DoDI 5505.17, *Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities*, 29 November 2016

DoDM 5200.01V1_AFMAN16-1404V1, *Information Security Program: Overview, Classification and Declassification*, 5 April 2022

DoDM 5200.01V2_AFMAN16-1404V2, *Information Security Program: Marking of Classified Information*, 7 January 2022

DoDM 5200.01V3_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information*, 12 April 2022

DoDM 5200.02_DAFMAN 16-1405, *Air Force Personnel Security Program*, 30 November 2022

DoDM 5220.22V2_AFMAN 16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 8 May 2020

Headquarters Air Force Mission Directive 1-6, *Administrative Assistant to the Secretary of the Air Force*, 22 December 2014

Headquarters Operating Instruction 65-6, *Insider Threat Resource Governance and Management Process*, 11 May 2018

Intelligence Community Directive 750, *Counterintelligence Programs*, 5 July 2013

National Security Memorandum-8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, 19 January 2022

National Security Presidential Memorandum-28, *The National Operations Security Program*, 13 January 2021

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

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

C-InT—Counter-Insider Threat

DAF—Department of the Air Force

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

DAF C—InT WG—Department of the Air Force Counter-Insider Threat Working Group

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

DAFI—Department of the Air Force Instruction

DCSA—Defense Counterintelligence and Security Agency

DoD—Department of Defense

DoDM—Department of Defense Manual

DRU—Direct Reporting Unit

E.O.—Executive Order

FLDCOM—Field Command

FOA—Field Operating Agency

FY—Fiscal Year

HAF—Headquarters of the Department of the Air Force

HOI—Headquarters Operating Instruction

IC—Intelligence Community

ICD—Intelligence Community Directive

MAJCOM—Major Command

MICT—Management Internal Control Toolset

NDAA—National Defense Authorization Act

OPR—Office of Primary Responsibility

OPREP—Operational Reporting

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

PPBE—Planning, Programming, Budgeting, and Execution

PRI—Potential Risk Indicator

RegAF—Regular Air Force

SAC—Self-assessment Checklist

SCI—Sensitive Compartmented Information

UAM—User Activity Monitoring

US—United States

USC—United States Code

Office Symbols

16 AF—Sixteenth Air Force

AF/A1—Deputy Chief of Staff for Manpower, Personnel and Services

AF/A2/6—Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations

AF/A3—Deputy Chief of Staff for Operations

AF/A4—Deputy Chief of Staff for Logistics, Engineering and Force Protection

AF/A10—Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration

AF/JA—The Judge Advocate General of the Air Force

AF/SG—Surgeon General

SAF/AA—Administrative Assistant to the Secretary of the Air Force

SAF/AAZ—Secretary of the Air Force, Director, Security, Special Program Oversight and Information Protection

SAF/AQ—Assistant Secretary of the Air Force for Acquisition, Technology and Logistics

SAF/CN—Chief Information Officer

SAF/GC—General Counsel

SAF/GCI—Deputy General Counsel of Intelligence, International and Military Affairs

SAF/IA—International Affairs

SAF/IG—Inspector General

SAF/MR—Assistant Secretary of the Air Force for Manpower and Reserve Affairs

SAF/PA—Director of Public Affairs

SAF/SQ—Assistant Secretary of the Air Force for Space Acquisition and Integration

SF/S1—Deputy Chief of Space Operations for Personnel

SF/S2—Deputy Chief of Space Operations for Intelligence

Terms

DAF Counter-Insider Threat Hub—A singular centralized focal point for identifying, gathering, integrating, and analyzing potential insider threat indicators through information sharing; command reporting; and the monitoring of user activity on government systems; providing actionable assessments and facilitating recommended mitigation and response actions to reduce risk to DAF resources, including but not limited to personnel, facilities, programs, and technologies.

Insider Threat—With respect to the Department, a threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department; and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace. (Public Law 114-328, Section 951, *National Defense Authorization Act for Fiscal Year 2017*)

Unauthorized Disclosure—A communication or physical transfer of classified information or controlled unclassified information to an unauthorized recipient. (DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI))*

User Activity Monitoring—The required technical functions, prescribed in the Committee on National Security Systems Directive (CNSSD) No. 504, *Directive on Protecting National Security Systems from Insider Threat*, as they relate to national security systems or classified systems to include keystroke monitoring, full application content (e.g., e-mail, chat, data import, data export), screen capture, and file shadowing for all lawful purposes (e.g., the ability to track documents when the names and locations have changed) and that the collected user activity monitoring data must be attributable to a specific user.