BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 16-1402

17 JUNE 2020

UNITED STATES AIR FORCES IN EUROPE-AIR FORCES AFRICA
Supplement

10 MARCH 2021

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/AA
(Mr. Anthony P. Reardon)

Supersedes: AFI 16-1402, 5 August 2014

Pages: 19

(USAFEAFAFRICA)

OPR: USAFE-AFAFRICA/IP

Certified by: HQ USAFE-AFAFRICA /IP
(GS-14. Joel S. Alaimo)

Pages: 6

This instruction implements Public Law 114-328, Section 951, National Defense Authorization Act for Fiscal Year 2017 and Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*, and assigns responsibilities for the oversight and management of the Air Force Counter-Insider Threat Program (AF C-InTP). It establishes the requirement to report insider threat-related information and establishes the Air Force Counter-Insider Threat Hub (AF C-InT Hub) as the focal point for sharing insider threat information with the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC). This instruction is applicable for all Air Force military and civilian personnel members, to include the Regular Air Force (RegAF), Air Force Reserve, Air National Guard, International Military Students and Foreign Nationals (on AF installations), contractors (as applied by contract), consultants, non-DoD U.S. government agencies whose personnel, by mutual agreement, require support from or

conduct operational activity with the Air Force and others as defined by the 2017 National Defense Authorization Act, Section 951. 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. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. This Instruction requires the collection and or maintenance of information protected by the Privacy Act of 1974 authorized by 10 U.S.C. 137, Under Secretary of Defense for Intelligence and Security; 44 U.S.C. 3554, Federal agency responsibilities; 44 U.S.C. 3557, National security systems; Public Law 112-81, Section 922, National Defense Authorization Act for Fiscal Year 2012 (NDAA for FY12), Insider Threat Detection (10 U.S.C. 2224 note); Public Law 113-66, Section 907(c)(4)(H), (NDAA for FY14), Personnel security (10 U.S.C. 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 U.S.C. 1564 note); 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; National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; and DoD Directive (DoDD) 5205.16, The DoD Insider Threat Program. The applicable SORN, Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System (September 23, 2016, 81 FR 65631), is available at: **http://dpclo.defense.gov/Privacy/SORNs.aspx**. See Air Force Instruction (AFI) 33-360, *Publications and Forms Management*, 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 submitter's commander for non-tiered compliance items. Refer recommended changes and questions about this publication to the OPR using the Air Force Form 847, *Recommendation for Change of Publication*; route the Air Force Forms 847 from the field through appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Instruction 33-322, Records Management and Information Governance Program, and disposed of in accordance with Air Force Records Information Management System Records Disposition Schedule", or any updated statement provided by the AF Records Management office (SAF/CIO A6P). **(T-2)**

(USAFEAFAFRICA) This supplement implements and extends the guidance of Air Force Instruction (AFI) 16-1402 *Counter-Insider Threat Program Management*. This instruction applies to all USAFE-AFAFRICA Regular Air Force, and Air Force Reserve Command (AFRC) units that are tenants on United States Air Forces in Europe-Air Forces Africa (USAFE-AFAFRICA) installations and to the Air National Guard (ANG) only upon mobilization under United States Air Forces in Europe-Air Forces Africa Command. This publication includes links to C-InT reporting form, thresholds and potential risk indicators. This publication may be supplemented at any level. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFI 33-322, *Records Management*

and Information Governance Program, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication.* Route AF Form 847 from the field through the appropriate chain of command. The authorities to waive wing, and unit level requirements in this publication are identified with a tier number ("T-0, T-1, T-2, T-3") following the compliance statement. See Department of the Air Force Instruction (DAFI) 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate waiver approval authority, through the publication OPR. This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. 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 Air Force.

SUMMARY OF CHANGES

This publication has been substantially revised and must be reviewed in its entirety. Major changes include the removal of two-letter organizational responsibilities now incorporated into AFPD16-14, *Security Enterprise Governance*, revisions for AF C-InT Hub members and other organizations impacted by updated DoD Counter-Insider Threat policy and the incorporation of guidance found in the Air Force Guidance Memorandum to this instruction. 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 AFI establishes the following framework to integrate policies and procedures to detect, deter, and mitigate insider threats to national security and Air Force assets and establishes implementing guidance to:

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

1.2. Continuously evaluate personnel by enhancing technical capabilities to monitor and audit user activity within the confines of the DoD banner and all applicable laws on information systems.

1.3. Leverage legally applicable antiterrorism, counterintelligence, human resources, law enforcement, security (e.g. cyber, information, industrial, personnel, physical, and operations), medical, and other authorities 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 civil liberties and privacy rights are safeguarded.

1.5. Ensure the Air Force counter-insider threat analysis center, referred to as the AF C-InT Hub, shares reportable insider threat information and post-processed results of system monitoring, as appropriate, in accordance with thresholds published by the Office of the Under Secretary of Defense, Intelligence and Security with the DITMAC.

1.6. Establish the requirement for the AF C-InT Hub to deliver to the DITMAC post-processed results of user activity monitoring and information system monitoring, as appropriate, in accordance with thresholds published by the Office of the Under Secretary of Defense, Intelligence and Security.

1.7. Establish the requirement for Air Force commands to report insider threat information to the AF C-InT Hub.

2. Air Force Counter-Insider Threat Overview.

2.1. The Air Force Counter-Insider Threat Working Group (AF C-InTWG). The AF C-InTWG identifies strategic goals, approves program implementation, integrates policy and procedures, and develops prioritized resource recommendations. The AF C-InTWG coordinates with DoD and the intelligence community insider threat leads to represent Air Force interests. The requirement for the AF C-InTWG will be reviewed annually and the group will be disestablished when the Air Force Security Enterprise Executive Board no longer deems its services/functions are necessary. The AF C-InTWG will consist of representatives from the following organizations:

2.1.1. Deputy Chief Information Officer. **(T-2)**

2.1.2. General Counsel of the Air Force. **(T-2)**

2.1.3. Inspector General, Special Investigations Directorate (Co-chair). **(T-2)**

2.1.4. Director, Security, Special Program Oversight and Information Protection (Co-chair). **(T-2)**

2.1.5. Deputy Chief of Staff, Manpower, Personnel and Services. **(T-2)**

2.1.6. Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance and Cyber Effects Operations. **(T-2)**

2.1.7. Deputy Chief of Staff, Logistics, Engineering and Force Protection. **(T-2)**

2.1.8. The Air Force Judge Advocate General. **(T-2)**

2.1.9. The Air Force Surgeon General. **(T-2)**

2.1.10. Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics. **(T-2)**

2.1.11. Deputy Chief of Staff, Operations. **(T-2)**

2.1.12. Director, Test and Evaluation. **(T-2)**

2.1.13. AF Office of Special Investigations. **(T-2)**

2.1.14. Director, AF C-InT Hub. **(T-2)**

2.1.15. Insider Threat Liaisons at the Major Command, Direct Reporting Unit, and Field Operating Agency. **(T-2)**

2.2. The Air Force Counter-Insider Threat Hub (AF C-InT Hub) reports information to the DITMAC. The AF C-InT Hub provides the Air Force a centralized capability where all insider threat-related information flows and is subsequently disseminated to the proper functional or operational entities for action or resolution.

2.2.1. The AF C-InT Hub integrates policies and procedures to detect, deter, and mitigate insider threats to national security and Air Force Assets.

2.2.2. The AF C-InT Hub's effectiveness is based on the analytical results of technical data and information received from data sources and designated command responsibilities.

2.2.3. Commanders and Directors at all levels are critical to the reporting process by ensuring information that meets the DoD Insider Threat Management Analysis Center (DITMAC) reportable thresholds are reported in a timely manner to their Major Command, Direct Reporting Unit, or Field Operating Agency insider threat liaison.

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

3.1. Network monitoring and auditing. Available monitoring and auditing capabilities shall support insider threat detection and mitigation efforts. Monitoring and auditing capabilities shall be integrated into the overall insider threat mitigation process. Capabilities should constantly be improved to meet current and future Air Force mission requirements and to proactively incorporate best practices to prevent and detect anomalous activity. All monitoring will be conducted in accordance with the DoD banner's consent to monitor requirements.

3.2. Information Sharing. An effective AF C-InTP relies upon timely sharing of information. Counterintelligence, security, law enforcement, medical, legal, and human resources policies must ensure that pertinent information reaches AF C-InTP personnel so they can take appropriate action.

3.3. Training and Awareness. AF C-InTP personnel will receive training to ensure adherence to privacy, whistleblower, records retention, civil liberties, and information sharing requirements. AF C-InTP 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. **(T-2)**

3.4. Insider Threat Reporting and Response. Insider threat actors typically exhibit concerning behavior, such as interpersonal, technical, financial, personal, mental health, social network, or travel issues. Reporting and sharing behaviors of concern is necessary to determine the severity of the threat and appropriate response options.

3.5. 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.

4. Roles and 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 implement the AF C-InTP. SAF/AA will also ensure AF C-InTP activities are synchronized and integrated with Air Force mission assurance with respect to the protection of critical assets and missions in accordance with Headquarters Mission Directive (HAFMD) 1-6, *Administrative Assistant to the Secretary of the Air Force*.

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

4.2.1. Provide oversight for the AF C-InTP and coordinate with stakeholders to promulgate policy.

4.2.2. Coordinate with representatives of the AF C-InTWG to identify and make resource recommendations to SAF/AA.

4.2.3. Integrate insider threat detection and mitigation procedures into applicable security policies where appropriate.

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 Air Force and intelligence community policies for special access programs.

4.2.5. Ensure insider threat response action procedures (such as inquiries) are in place to clarify or resolve insider threat matters.

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

4.2.7. Co-chair the AF C-InTWG, which will be under the oversight of the Air Force Security Enterprise Executive Board in accordance with AFPD 16-14.

4.2.8. 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.

4.2.9. Coordinate AF C-InTP issues through the Air Force Security Enterprise Executive Board.

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

4.2.11. Advocate and program for appropriate resources to establish and maintain the AF C-InT Hub.

4.2.12. Facilitate oversight reviews by cleared officials to ensure compliance with insider threat policy guidelines, as well as applicable legal, privacy and civil liberty protections.

4.2.13. Ensure AF C-InTP activities are synchronized and integrated with AF mission assurance requirements with respect to the protection of AF and DoD critical assets and missions.

4.3. Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics (SAF/AQ) shall ensure policies and procedures are in place to implement applicable requirements of the AF C-InTP and ensure that all AF contracts include the requirement to participate in the AF C-InTP.

4.4. Chief of Information Dominance and Deputy Chief Information Officer (SAF/CN) shall:

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. All monitoring will be conducted in accordance with the DoD banner's consent to monitor requirements.

4.4.2. Develop strategy and policy that allows for regular and timely access to network and system audit information for AF C-InTP personnel to support the identification, analysis, and resolution of insider threat issues.

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

4.5. The General Counsel of the Air Force (SAF/GC) in coordination with the Judge Advocate General shall provide advice and counsel regarding DoD policy, laws and regulations that are applicable to the AF C-InTP. SAF/GC, through the Deputy General Counsel of Intelligence, International and Military Affairs (SAF/GCI), will provide professional oversight of the Attorney-Adviser imbedded in the AF C-InTP.

4.6. Inspector General (AF/IG) shall:

4.6.1. Integrate insider threat awareness training as provided by the AF C-InTP.

4.6.2. Provide AF C-InTP personnel training in law enforcement, counterintelligence, and security, procedures for conducting insider threat response actions, and applicable legal guidelines, to include whistleblower issues.

4.6.3. Establish procedures to securely provide AF C-InTP personnel regular, timely, and electronic access to information necessary to identify, analyze and resolve insider threat issues.

4.6.4. Provide access to counterintelligence and law enforcement reporting and analytic products relevant to insider threat.

4.6.5. Audit insider threat personnel's handling, use, and access to records and data.

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

4.7.1. Securely provide AF C-InTP 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 human resources 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.

4.7.2. Establish procedures for access requests by AF C-InTP personnel involving particularly sensitive or protected information.

4.7.3. Establish reporting guidelines for relevant organizational components to refer relevant insider threat (InT) information directly to the AF C-InTP.

4.7.4. Provide policy and guidance for integrating and vetting new/emerging AF C-InTP institutional education and training requirements or learning outcomes into accessions, professional military education, professional continuing education and ancillary training.

4.8. Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2) shall:

4.8.1. Develop, oversee and manage, in coordination with AF C-InTWG, a capability that enables the collection and analysis of relevant InT data for the intelligence community information environment.

4.8.2. Review, update and promulgate policies and procedures that support monitoring and auditing of intelligence assets and networks for InT detection and mitigation.

4.8.3. Oversee monitoring and auditing of Air Force intelligence community networks and assets for InT activities and establish procedures to securely provide AF C-InTP personnel regular, timely, and electronic access to information necessary to identify, analyze and resolve InT issues.

4.8.4. Provide AF C-InTP personnel access to intelligence reporting and analytic products relevant to insider threat.

4.9. Deputy Chief of Staff for Operations (AF/A3) shall:

4.9.1. Ensure cyber space operations support the capability to monitor and audit user activity in accordance with U.S. Cyber Command tasking orders.

4.9.2. Coordinate AF C-InTP information that may impact Air Force critical assets and missions.

4.10. Deputy Chief of Staff, Logistics, Engineering and Force Protection (AF/A4) shall:

4.10.1. Ensure procedures are in place to securely share law enforcement and other applicable information with authorized AF C-InTP personnel for the purpose of identifying, analyzing, and resolving InT issues.

4.10.2. Integrate InT detection and mitigation procedures into applicable security policies.

4.11. The Air Force Judge Advocate General (SAF/JA), in coordination with the SAF/GC, shall provide advice and counsel regarding DoD policy, laws and regulations that are applicable to the AF C-InTP and those pertaining to civil liberties, privacy, and whistleblower protection.

4.12. Air Force Surgeon General (AF/SG) shall ensure policies and procedures are in place for the sharing of information related to insider threats in already existing violence prevention programs and from medical records and provide the AF C-InT Hub with a representative who can provide medical analysis and medical evaluations on cases requiring medical expertise. Information sharing procedures will be in accordance with applicable laws and policies.

4.13. Director of Test and Evaluation (AF/TE) shall ensure policies and procedures are in place to implement applicable requirements of the AF C-InTP.

4.14. Director, Concepts, Development and Management Office (SAF/CDM) shall:

4.14.1. Serve as the responsible authority for the management and execution of the AF C-InTP.

4.14.2. Provide direction to the AF C-InTP program management office to execute the AF C-InTP.

4.14.3. Provide management oversight for the AF C-InTP program management office to ensure that the program is being executed, administered, and managed in accordance with published guidance and direction.

4.14.4. Plan, manage, and direct resources associated with the AF C-InTP in accordance with SAF/AAZ guidance and direction.

4.14.5. Ensure the AF C-InTP responds, as appropriate, to requests for information and inquiries from Air Force agencies.

4.15. Major Command, Direct Reporting Units, and Field Operating Agency Commanders and Directors, or their Deputies shall:

4.15.1. Ensure insider threat liaisons are designated throughout all command levels, as appropriate **(T-2)** and submit the designations to the Director, AF C-InT Hub. **(T-2)**

4.15.1.1. **(Added-USAFEAFAFRICA)** HQ USAFE-AFAFRICA/IP Directorate manages the Command C-InT Program through the appointment of an Insider Threat Program Manager and will act as the command insider threat liaison. The Program Manager assesses referrals generated from the Hub for possible initiation of a security incident.

4.15.2. Through their appointed security program executive, communicate and coordinate on insider threat issues relative to their command and support SAF/AA in executing the AF C-InTP as it evolves. **(T-1)**

4.15.2.1. **(Added-USAFEAFAFRICA)** The Deputy Commander, USAFE-AFAFRICA, is appointed as the security program executive and is designated as the lead for all command C-InTP policy, activities, operations and issues.

4.15.3. Ensure DITMAC threshold-level events are reported to the AF C-InT Hub through the DITMAC System of Systems – US Air Force (DSoS-USAF) (or successor system) in a timely manner **(T-1)**, and respond to AF C-InT Hub requests for information. Commanders who are unsure of whether an event meets the thresholds should coordinate with their MAJCOM insider threat liaison to determine whether reporting is required. **(T-1)** The thirteen DITMAC 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.

4.16. Designated Insider Threat Liaisons shall:

4.16.1. Request DITMAC DSoS-USAF (or successor system) accounts with the AF C-InT Hub within two weeks of appointment. **(T-1)**

4.16.2. Report DITMAC threshold-level events to the AF C-InT Hub **(T-1)** and respond to AF C-InT Hub request for information, as appropriate.**(T-1)** Coordinate with the AF C-InT Hub on any inquiries from Commanders in which it is unclear whether a threshold has been met prior to opening a case in DSoS-USAF. **(T-1)**

4.16.3. Ensure required information is entered in DSoS-USAF (or successor system). **(T-1)**

4.16.4. Ensure Commanders and Directors have access to the thirteen DITMAC reporting thresholds and potential risk indicators (PRIs). **(T-1)**

4.16.4. **(USAFEAFAFRICA)** The DITMAC reporting thresholds, potential risk indicators and C-InT reporting form are located on the following share point link. (**https://usaf.dps.mil/sites/ua-cs/IP/SitePages/Home.aspx?InitialTabId=Ribbon%2ERead&VisibilityContext=WSSTabPersistence**)

4.16.5. Comply with additional reporting requirements as determined by the Director, AF C-InT Hub. **(T-1)**

4.16.6. Develop processes for gathering and reporting information in DSoS-USAF (or successor system) to the AF C-InT Hub. **(T-1)**

4.16.7. Complete required insider threat training within thirty (30) days of appointment. **(T-1)**

4.16.8. Insider Threat Liaisons at the Major Command, Direct Reporting Unit, and Field Operating Agency levels serve as members of the AF InTWG. **(T-1)**

4.16.9. Assess referrals generated from the AF C-InT Hub for possible opening of a security incident and make a referral to the Information Protection office for resolution. **(T-1)**

4.16.10. Report to the AF C-InT Hub any response actions taken in regard to any insider threat referral from the AF C-InT Hub. **(T-1)**

4.16.11. Coordinate with base level authorities responsible for taking action on referred information. If base level authorities are not known, contact local security squadron for contact information. **(T-1)**

4.16.12. **(Added-USAFEAFAFRICA)** Coordinate with responsible Unit Commander/Director or other organizations responsible for action on referred information.

4.16.13. **(Added-USAFEAFAFRICA)** Update referred case information to the Hub using DITMAC System of Systems – US Air Force (DSoS-USAF) (or successor system), with appropriate level of response/mitigation actions taken on inquiries/investigations.

4.16.14. **(Added-USAFEAFAFRICA)** Provide feedback to the C-InTWG to inform and improve processes.

4.16.15. **(Added-USAFEAFAFRICA)** Receive C-InT reports from unit Commanders/Directors reported through the Wing IP offices.

4.16.16. **(Added-USAFEAFAFRICA)** Become familiar with the Potential Risk Indicators. (**https://usaf.dps.mil/sites/ua-cs/IP/SitePages/Home.aspx?InitialTabId=Ribbon%2ERead&VisibilityContext=WSSTabPersistence**).

4.17. Wing/Installation Commanders shall ensure insider threat threshold information is reported to their command designated insider threat liaisons and/or AF C-InT Hub, in accordance with this AFI and their Major Command guidance. **(T-1)** Seek guidance from the command designated insider threat liaison on those cases in which it is unclear if a threshold has been met prior to requesting the case be reported in DSoS-USAF. **(T-1)**

4.18. Commanders and Directors at the wing-level and below shall:

4.18.1. Report any incident meeting one or more of the DITMAC threshold-level events to the AF C-InT Hub **(T-1)** and respond to AF C-InT Hub requests for information, as appropriate. The thirteen DITMAC 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. Ensure these reports are submitted within Command prescribed timeframes, if established, but no later than five calendar days after the information becomes available. **(T-1)** Seek guidance from the command designated insider threat liaison on those cases in which it is unclear if a threshold has been met prior to requesting the case be reported in DoD System of Systems (DSoS)-USAF. **(T-1)**

4.18.1. **(USAFEAFAFRICA)** DITMAC Reporting thresholds can be located in the share point link: **https://usaf.dps.mil/sites/ua-cs/IP/SitePages/Home.aspx?InitialTabId=Ribbon%2ERead&VisibilityContext=WSSTabPersistence**

4.18.1.1. **(Added-USAFEAFAFRICA)** USAFE-AFAFRICA/IP will coordinate all reporting outside of the command (Air Reserve, Air National Guard, or parent units of tenants and GSUs).

4.18.1.2. **(Added-USAFEAFAFRICA)** Immediately report whenever a military member is notified of preferral of courts-martial charges, administrative discharge for misconduct is initiated or a civilian employee/contractor is provided an intent to remove or is fired for cause.

4.18.1.3. **(Added-USAFEAFAFRICA)** Ensure C-InT training is provided within 30 days of hire, and annually thereafter for all assigned personnel.

4.18.1.4. **(Added-USAFEAFAFRICA)** Provide USAFE-AFAFRICA/IPP updates to C-InT cases as additional information becomes available, or every 30 days until the USAFE-AFAFRICA/IPP determines follow-up is not needed, mitigation of the incident, or case closure.

4.18.1.5. **(Added-USAFEAFAFRICA)** Assess continuous evaluation referral notifications for possible opening of a security incident. Additionally, take action on referred information and report it through the Wing IPO to USAFE-AFAFRICA/IPP.

4.18.1.6. **(Added-USAFEAFAFRICA)** Report all imminent threats or consequences immediately to local AFOSI and law enforcement personnel. For example, if a reportable incident or situation has suspected or known imminent consequences, such as potential workplace violence or espionage which will result in loss of life/data, this information needs to be reported immediately to law enforcement (AFOSI, FBI, or Security Forces, etc.).

4.18.1.7. **(Added-USAFEAFAFRICA)** Subjects should not be alerted of any ongoing C-InT inquiry. Contact USAFE-AFAFRICA/IPP and/or AFOSI as appropriate for guidance.

4.18.1.8. **(Added-USAFEAFAFRICA)** Become familiar with the Potential Risk Indicators.

4.18.1.9. **(Added-USAFEAFAFRICA)** Chief, Wing Information Protection Office will:

4.18.1.9.1. **(Added-USAFEAFAFRICA)** Ensure Wing C-InTP liaison is appointed in writing by the Wing CV and provide documentation to USAFE-AFAFRICA/IP.

4.18.1.9.2. **(Added-USAFEAFAFRICA)** Ensure C-InTP cases are reported as incidents in to JPAS or DISS (or successor system).

4.18.1.9.3. **(Added-USAFEAFAFRICA)** Ensure all Commanders on the Installation are met with annually to discuss questions or concerns with the C-InTP.

4.18.1.9.4. **(Added-USAFEAFAFRICA)** Review all C-InT cases for accuracy and completeness (all pertinent documents available pertaining to the case (blotter entries, reports, clearance suspension decision.) prior to submitting to USAFE-AFAFRICA/IPP on the C-InT report form (**https://usaf.dps.mil/sites/ua-cs/IP/SitePages/Home.aspx?InitialTabId=Ribbon%2ERead&VisibilityContext=WSSTabPersistence**).

4.18.1.9.5. **(Added-USAFEAFAFRICA)** Provide incident details to the USAFE-AFAFRICA/IP for further reporting through DSOS using the USAFE-AFAFRICA/IP reporting form(s).

4.18.1.9.6. **(Added-USAFEAFAFRICA)** Provide USAFE-AFAFRICA/IPP updates to C-InT cases as additional information becomes available or every 30 days until the USAFE-AFAFRICA/IPP determines follow-up is not needed, mitigation of the incident, or case closure.

4.18.1.9.7. **(Added-USAFEAFAFRICA)** Become familiar with the Potential Risk Indicators.

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

4.18.2. **(USAFEAFAFRICA)** USAFE-AFAFRICA/IPP will coordinate all reporting outside of the command (Air Force Reserve, Air National Guard, or Tenant Unit parent Commands).

4.19. Director, AF C-InT Hub shall:

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

4.19.2. Serve as member of the AF C-InTWG. **(T-1)**

4.19.3. Establish internal procedures for insider threat analysis, insider threat referral process, and overall AF C-InT Hub operations. **(T-1)**

4.19.4. Gather, integrate, and analyze indicators of potential insider threats from approved authorized data sources to include:

4.19.4.1. User Activity Monitoring. **(T-1)**

4.19.4.2. Enterprise Audit Management. **(T-1)**

4.19.4.3. Cybersecurity. **(T-1)**

4.19.4.4. Law Enforcement. **(T-1)**

4.19.4.5. Counterintelligence. **(T-1)**

4.19.4.6. Personnel security. **(T-1)**

4.19.4.7. Human resources. **(T-1)**

4.19.4.8. Command reporting. **(T-1)**

4.19.4.9. Medical community. **(T-1)**

4.19.4.10. Legal. **(T-1)**

4.19.4.11. 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.

4.19.5. Ensure the functions and activities of the AF C-InT Hub will not supersede existing functional area (example: cybersecurity, personnel security, human resources) processes, investigative authorities, or command responsibilities to maintain good order and discipline within the Air Force. **(T-1)**

4.19.6. Use the DITMAC DSoS-USAF (or successor system) for workflow and case management. **(T-0)**

4.19.7. Ensure all AF C-InT Hub personnel with access to AF C-InTP records, data, and user activity monitoring methods and results are trained on:

4.19.7.1. How to handle, protect, and store the sources of information in accordance with their classification or as controlled unclassified information in accordance with AFI 16-1404, *Air Force Information Security Program*. **(T-0)**

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

4.19.7.3. Ensuring 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 located in the Air Force Records Information Management System. **(T-1)** 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 DSoS, System of Records Notice.

4.19.7.4. Civil liberties and privacy. **(T-1)**

4.19.8. Deliver to the DITMAC post-processed results of information system monitoring in accordance with thresholds published by the Office of the Under Secretary of Defense, Intelligence and Security. **(T-0)**

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

4.19.10. Develop and provide guidance to Major Command, Direct Reporting Units, and Field Operating Agencies designated liaisons related to minimum information requirements for reporting entered via DSoS-USAF (or successor system). **(T-1)**

4.19.11. Ensure Major Commands, Direct Reporting Units, and Field Operating Agencies designated InT liaisons have access to the thirteen DITMAC thresholds and PRIs. **(T-1)**

4.19.12. Manage the DSoS-USAF (or successor system). **(T-1)**

4.19.13. Ensure that each data source is approved by legal counsel before being incorporated into the AF C-InT Hub. **(T-1)**

4.19.14. Integrate policies and procedures to deter, detect, and mitigate insider threats to Air Force assets. **(T-1)**

4.19.15. Develop procedures to enable trained insider threat personnel to integrate necessary and relevant information, analyze and appropriately respond to mitigate the threat. **(T-1)**

4.20. All personnel with access to AF C-InTP Records, Data, and User Activity Monitoring Methods and Results shall:

4.20.1. Take prudent steps to protect insider threat-related information from unauthorized disclosure. **(T-1)**

4.20.2. Be properly trained on how to handle, protect, and store this information. **(T-1)**

4.20.3. Handle, protect, and store in accordance with their classification or as controlled unclassified information in accordance with AFI 16-1404. **(T-0)**

4.20.4. 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)**

ANTHONY P. REARDON
Administrative Assistant

(USAFEAFAFRICA)

SCOTT T. ALLIBONE, GS-15, DAF
Director, Information Protection

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

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

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

AFI 33-360, *Publications and Forms Management,* 1 December 2015

(Added-USAFEAFAFRICA) AFGM2020-16-01 Ver 2, *Air Force Guidance Memorandum for Controlled Unclassified Information (CUI),* 23 July 2020

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

(Added-USAFEAFAFRICA) DAFI33-360, *Publications and Forms Management*, 15 Dec 2018

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

(Added-USAFEAFAFRICA) E.O. 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, 7 October 2011

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

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

Prescribed Forms

(**Added-USAFEAFAFRICA**) None.

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

C—**InT Hub –**Counter-Insider Threat Hub

C—InTP – Counter-Insider Threat Program

C—InTWG – Counter-Insider Threat Working Group

(Added-USAFEAFAFRICA) CIP—Chief of Information Protection

(Added-USAFEAFAFRICA) CUI—Controlled Unclassified Information

(Added-USAFEAFAFRICA) DAFI—Department of the Air Force Instruction

DITMAC—DoD Insider Threat Management and Analysis Center

DoD—Department of Defense

DSoS USAF -DITMAC System of Systems—United States Air Force

InT—Insider Threat

(Added-USAFEAFAFRICA) IPO—Information Protection Office

(Added-USAFEAFAFRICA) MAJCOM—Major Command

OPR—Office of Primary Responsibility

PRI—Potential Risk Indicator

RegAF—Regular Air Force

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

U.S.—United States

Terms

(Added-USAFEAFAFRICA) Access—The ability and opportunity to obtain knowledge of classified or sensitive information or to be in a place where one could expect to gain such knowledge.

(Added-USAFEAFAFRICA) Adjudication—Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted or retain eligibility for access to classified information and continue to hold positions requiring a trustworthy decision.

(Added-USAFEAFAFRICA) Adverse Information—Any information that adversely reflects on the integrity or character of a cleared employee that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes as an insider threat.

(Added-USAFEAFAFRICA) Anomalous Activity—Irregular or unusual deviations from what is usual, normal, or expected; activity inconsistent with the expected norm. Also, network activities that are inconsistent with the expected norms that may suggest a trusted insider is exploiting access to information for nefarious and illegal activity.

(Added-USAFEAFAFRICA) Background Investigation—An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject.

(Added-USAFEAFAFRICA) Clearance—Formal security determination by an authorized adjudication authority that an individual is eligible for access, on a need-to-know basis, to a specific level of collateral classified information (TOP SECRET, SECRET, CONFIDENTIAL).

(Added-USAFEAFAFRICA) DoD Insider Threat Management and Analysis Center (DITMAC)—A cross-functional team of analysts that aggregates, integrates reviews, analyzes,

and shares information that is indicative of a potential insider threat. The DITMAC will exercise this information management capability with the ability to assess risk; refer issues for further consideration, investigation, and potential action; synchronize responses; and oversee resolution of identified issues across the Department within DoD-approved resources.

(Added-USAFEAFAFRICA) Elicitation—The attempted or successful acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation.

(Added-USAFEAFAFRICA) Foreign Intelligence Entity (FIE)—Any known or suspected foreign organization, person, or group that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service (FISS) and international terrorist organizations.

(Added-USAFEAFAFRICA) Honey Trap—The term universally applied to operations undertaken to ensnare an unwary target in a compromising sexual encounter that may leave the victim vulnerable to blackmail that might result in espionage.

(Added-USAFEAFAFRICA) Indicator—Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.

Insider—A person who has or had been granted eligibility for access to classified information or eligibility to hold a sensitive position. These individuals include Active and Reserve Component (including National Guard) military personnel, civilian employees (including non-appropriated fund employees), and DoD contractor personnel; this includes officials or employees from federal, State, local, tribal and private sector entities affiliated with or working with DoD who have been granted access to classified information by DoD based on an eligibility determination made by DoD or by another federal agency authorized to do so. (DoDD, *The DoD Insider Threat Program* 5205.16)

Insider Threat—The threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. 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. (DoDD, *The DoD Insider Threat Program* 5205.16) .

(Added-USAFEAFAFRICA) Insider Threat Hub—A centralized multi-disciplinary staff element or activity established by a component that possesses an integrated capability to monitor, audit, fuse, and analyze incoming information for insider threat detection and mitigation. Hub personnel will be able to analyze information and activity indicative of an insider threat and refer that data to the appropriate officials to investigate or otherwise resolve.

(Added-USAFEAFAFRICA) Mitigation—Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems.

(Added-USAFEAFAFRICA) Potential Risk Indicators—An action, event, or condition that precedes the insider act and is hypothesized to be associated with the act. The observable precursors contribute to increased risk (**https://usaf.dps.mil/sites/ua-cs/IP/SitePages/Home.aspx?InitialTabId=Ribbon%2ERead&VisibilityContext=WSSTabPersistence**).

(Added-USAFEAFAFRICA) Social Engineering—The act of manipulating people into performing actions or divulging confidential information. It relies on human interactions, such as trying to gain the confidence of someone through trickery or deception for the purpose of information gathering, fraud, or computer system access. This can take many forms, both online and offline.