BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF THE AIR FORCE INSTRUCTION 71-101 VOLUME 4

26 MAY 2026

Special Investigations

COUNTERINTELLIGENCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: SAF/IGX

Certified by: SAF/IG

Supersedes: AFI71-101V4, 2 July 2019

Pages: 27

This instruction implements Air Force Policy Directive (AFPD) 71-1, *Criminal Investigations and Counterintelligence*, and Air Force Mission Directive (AFMD) 39, *Air Force Office of Special Investigations (AFOSI)*. It provides guidance for the Air Force Office of Special Investigations (AFOSI) and DoD Cyber Crime Center (DC3) personnel conducting counterintelligence activities, and training and reporting requirements for Department of the Air Force (DAF) personnel. It applies to all civilian employees and uniformed members of the Regular Air Force, the Air Force Reserve, the Air National Guard, the United States Space Force, 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. Failure to obey **Chapter 3** constitutes a violation of Article 92, *Failure to Obey Order or Regulation*, Uniform Code of Military Justice. 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. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by DAF. This publication may be supplemented at any level, but all supplements that directly implement it must be routed to the Secretary of the Air Force (SecAF), Inspector General, Special Investigations (SAF/IGX), for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility using the DAF Form 847, *Recommendation for Change of Publication*. Route DAF Forms 847 from the field through Major Command publications and/or forms managers. 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 DAF 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 publication Office of Primary Responsibility for non-tiered compliance items. For purposes of disciplinary or punitive action against individuals whose actions are governed by this publication, nothing in the previous sentence will be interpreted as affecting the requirement for mandatory compliance with this publication or any other applicable laws, regulations, or policies by those to whom it applies. This publication guides the internal operation of a DoD agency, but it is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable by law against the United States (US), DoD, DAF or its officers, employees, contractors, or agents.

SUMMARY OF CHANGES

The publication has been revised and must be completely reviewed. This revision updates requirements for offensive counterintelligence (CI) and CI support to research, development, and acquisition; supply chain risk management; the defense critical infrastructure (DCI) program; the insider threat program; and updates roles and responsibilities.

Chapter 1

RESPONSIBILITIES

1.1. Air Force Office of Special Investigations. AFOSI is the sole DAF organization authorized to conduct CI investigations, operations, collection, analysis and production, CI functional services, and CI functional activities. All AFOSI personnel engaged in conducting CI activities must attend and satisfactorily complete formal CI training approved by the DoD or a Military Department.

1.1.1. AFOSI is the only DAF Military Department Counterintelligence Organization (MDCO) with CI authorities primarily derived from Executive Order (EO) 12333, *United States Intelligence Activities*, section (§) 1.7(f), *The Intelligence and Counterintelligence Elements of the Army, Navy, Air Force, and Marine Corps*.

1.1.2. In the US, AFOSI coordinates CI activities with the Federal Bureau of Investigation (FBI) when appropriate, in accordance with (IAW) the *Memorandum of Understanding Between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities*, annexes A *Counterterrorism Information Sharing*; B C*ounterintelligence Investigative Information Sharing*; and C *Investigative and Operational Responsibilities and Coordination Procedures*.

1.1.3. Outside the US, AFOSI coordinates CI activities with the Central Intelligence Agency and the FBI as appropriate.

1.1.4. AFOSI notifies and provides briefings to appropriate command officials on CI investigations that require determinations on continuing access to classified information and other personnel security actions.

1.1.5. The AFOSI Investigations Collections Operations Nexus Center (AFOSI ICON Center) serves as the DAF's sole reporting integration mechanism for matters pertaining to CI investigations, operations, and threats from foreign intelligence entities (FIE), international terrorist organizations, cyberspace actors, and unauthorized disclosures. The AFOSI ICON Center is responsible for administrative, headquarters-level oversight and management for AFOSI production, source, and collection management. The AFOSI ICON Center will:

1.1.5.1. Provide timely investigative data, threat reporting data, and analysis and production to the Commander, AFOSI (AFOSI/CC), and other senior DAF and DoD leaders.

1.1.5.2. Receive and synchronize information for the AFOSI ICON Center regional and specialty desks that AFOSI activities and other US Government (USG) agencies provide.

1.1.5.3. Manage AFOSI's Global Watch. The AFOSI Global Watch receives up-channel reporting from AFOSI units and personnel and coordinates with other DAF, DoD, and USG watch centers.

1.1.5.4. Coordinate investigative and CI activities with DAF human intelligence (HUMINT) activities, as necessary.

1.1.5.5. Coordinate and deconflict human source, investigative, and CI activities with DAF, DoD, Combatant Commands, and other USG HUMINT activities, as necessary.

1.1.6. AFOSI is the sole DAF agency responsible for conducting partner engagements with federal, state, tribal, local, and foreign law enforcement (LE), CI, and security agencies for matters falling within the AFOSI mission, IAW AFPD 71-1.

1.2. Department of Defense Cyber Crime Center. Pursuant to DoD Directive (DoDD) 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, DC3 functions as the DoD Center of Excellence for digital and multimedia forensics and provides LE and CI support to AFOSI, and other MDCOs through:

1.2.1. Digital and multimedia forensics examination and analysis to support LE and CI investigations and operations.

1.2.2. Specialized investigative and cyber training to DoD digital forensics examiners and cyber investigators responsible for the exploitation of digital media in support of LE and CI objectives.

1.2.3. Cyber intelligence analysis products and services to directly support AFOSI, and other MDCO, cyber investigations and operations, and leads a collaborative analytical and technical exchange with subject matter experts from AFOSI, DoD CI components, and other LE and CI agencies to build a threat picture and actionable content enabling proactive LE, CI, and cyber operations focused on nation-state threat actors.

1.2.4. Research, development, test, and evaluation (RDT&E) advancing digital and multimedia forensics technology, and certifies cyber CI tools, techniques, or other procedures to share with AFOSI and other DoD CI components through a central clearinghouse and repository.

1.3. Department of the Air Force General Counsel. Consistent with Headquarters Air Force (HAF) Mission Directive (MD) 1-14, *General Counsel and The Judge Advocate General*, the Secretary of the Air Force, General Counsel (SAF/GC), serves as legal counsel for DAF intelligence oversight issues together with the Air Force Office of the Judge Advocate General (AF/JA). SAF/GC provides advice to intelligence components on questions of legality and propriety, as required, and provides advice to AFOSI, Office of Special Projects (AFOSI PJ), on all investigative and operational activities.

1.4. Air Force Judge Advocate General. Serves as primary legal counsel for judge advocate intelligence oversight training and shares the function of advising on policy directives, regulations, and training policy. AF/JA provides advice to intelligence components on questions of legality and propriety, as required, and advice to AFOSI PJ, on all investigative and operational activities.

1.5. Department of the Air Force Commanders. DAF commanders consult with their servicing AFOSI unit to ensure that CI Awareness and Reporting training meets DoD and DAF requirements IAW DoDD 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*. Additionally, DAF commanders ensure that their personnel are notified and briefed on threats related to FIE, international terrorists, cyberspace, and unauthorized disclosures.

1.6. Department of the Air Force Personnel. DAF personnel will report threats related to FIE, international terrorists, cyberspace, and foreign ownership, control or influence, to their servicing MDCO without delay. DAF personnel must report unauthorized disclosures of classified information to AFOSI and the appropriate security authorities IAW DoD Manual (DoDM) 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information*, and DoDM5200.01 Volume 3_DAFMAN 16-1404 Volume 3, *Information Security Program: Protection of Classified Information*. Additionally, IAW DoDD 5148.13, *Intelligence Oversight*, all DAF personnel must report questionable intelligence activities and significant or highly sensitive matters involving intelligence activities that may have serious implications for the execution of DoD missions. DoD policy states that senior leaders and policymakers within the USG must be made aware of events that may erode the public trust in the conduct of DoD intelligence operations.

Chapter 2

COUNTERINTELLIGENCE AWARENESS AND REPORTING BRIEFING PROGRAM

2.1. Awareness and Briefing Programs. AFOSI conducts, manages, and coordinates CI awareness and briefing programs. CI awareness and briefing programs promote threat and reporting awareness responsibility and enable DAF personnel to identify threats and report suspicious situations and incidents to appropriate authorities IAW Security Executive Agent Directive 3*, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position*, DoDD 5240.06, and AFPD 71-1. Awareness and briefing efforts will emphasize individual reporting responsibilities and include a detailed discussion concerning insider threats, espionage, subversion, sabotage, assassination, sedition, terrorism, counterproliferation, treason, and standards discussed in this instruction.

2.2. Briefings. Briefings include threats related to FIE, international terrorists, cyberspace, and unauthorized disclosures. **(T-0)**

2.2.1. DAF commanders seek to instill in their personnel a high-level of awareness of the threat to classified, sensitive, and proprietary information from all unauthorized sources, foreign or domestic, as well as from inadvertent or deliberate disclosures by cleared personnel.

2.2.2. Highlight cyber threats to include indicators of FIE exploitation of people, programs, and resources during all CI awareness, briefing, and reporting programs IAW DoD Instruction (DoDI) S-5240.23, *(U) Counterintelligence (CI) Activities in Cyberspace*. Reference AFOSI's Secret Internet Protocol Router Network webpage to view current cyber threat assessments and DoDI S-5240.23 for examples of indicators for potential threat activity.

2.2.3. Military personnel must receive a briefing at or near the time of initial entry. **(T-0)** Military personnel require recurring briefings at least every 12 months or upon permanent change of station, whichever is more frequent. These briefings are provided through computer-based training obtained through Joint Knowledge Online, MyLearning, or successor training platforms.

2.2.4. AFOSI must brief civilian employees at or near the time of initial entry or hire. **(T-0)** Civilian employees require recurring briefings at least every 12 months or upon permanent change of station, whichever is more frequent.

2.2.5. The Air Education and Training Command provides initial awareness briefings to military personnel during basic training or pre-commissioning programs.

2.2.6. DAF commanders ensure that all civilian and military personnel entering the DAF directly (through means other than Air Education and Training Command) receive a briefing by leadership during their initial assignment. If conditions warrant, leadership will institute more frequent briefing intervals, and based on the nature of duties, some personnel may require more frequent briefings.

2.2.7. AFOSI is the installation level training agency for CI awareness briefings. **(T-0)** If AFOSI does not provide the training, AFOSI will ensure the provided training meets requirements.

2.3. Counterintelligence Briefers. CI briefers will tailor briefings to their audience and consider the associated subject matter for security requirements. The briefing will include:

2.3.1. Threats posed by foreign intelligence, foreign government-sponsored commercial enterprises, international terrorist threats, non-state entities or cyber actors, and transnational criminal organizations. **(T-0)**

2.3.2. Information regarding the early detection of espionage, foreign intelligence indicators, and international terrorist activities. **(T-0)**

2.3.3. Detailed information regarding sabotage, subversion, treason, and espionage. **(T-0)**

2.3.4. Relevant and current threats facing the specific installation, mission, functions, activities, and locations in which the audience is associated. **(T-0)**

2.3.5. Reporting requirements of this instruction and those described in DoDD 5240.06. **(T-0)** DAF personnel will report information concerning security violations and other information with potentially serious security significance regarding personnel with access to classified information or who are employed in a sensitive position IAW DoDM5200.01 Volume 1_AFMAN16-1404 Volume 1, *Information Security Program: Overview, Classification, and Declassification*; DoDM 5200.01V3; and DoDM5200.02_DAFMAN16-1405, *Department of Air Force Personnel Security Program*. **(T-0)**

2.4. Critical Program Information and Critical Programs and Technology. Pursuant to AFPD 71-1; DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*; and DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test and Evaluation (RDT&E)*, acquisition program, program management office, DoD and Service laboratories, and other RDT&E personnel working with Critical Program Information and Critical Programs and Technologies (CP&T) will notify AFOSI of all projected foreign travel prior to departure. **(T-0)** Such personnel will receive foreign intelligence and antiterrorism threat briefings prior to foreign travel. **(T-0)** Upon completion of travel, personnel will contact AFOSI to schedule a debriefing. **(T-0)**

2.5. Sensitive Compartmented Information and Special Access Programs. Pursuant to Intelligence Community Directive (ICD) 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*, personnel with sensitive compartmented information and special access incur special security obligations that include advance foreign travel notification for official and unofficial travel and defensive travel briefings. Upon completion of travel, personnel with sensitive compartmented information access will contact their servicing AFOSI office to schedule a debriefing. **(T-0)** IAW DoDM 5205.07, *Special Access Program Security Manual*, and AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, personnel with special access will contact their serving AFOSI PJ office.

2.6. Defense Critical Infrastructure Program. AFOSI will provide annual CI awareness briefings, at a minimum, to all personnel assigned to or supporting an identified DCI critical asset, IAW DoDD 5240.02, *Counterintelligence (CI)*; DoDD 3020.40, *Mission Assurance (MA)*; and DoDI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)*. **(T-0)** Prior to the event, personnel will notify AFOSI of all projected foreign travel or foreign visits; AFOSI will provide personnel foreign intelligence threat briefings prior to foreign visits and foreign travel. **(T-0)** Additionally, AFOSI will brief personnel on antiterrorism threats prior to projected foreign travel. **(T-0)** Upon completion of foreign travel or a foreign visit, these personnel will contact AFOSI to schedule a debriefing. **(T-0)**

Chapter 3

REPORTABLE INFORMATION AND CONTACTS

3.1. Reportable Information and Contacts. AFOSI is the sole DAF repository for the collection and retention of reportable CI information and contacts. DAF personnel with reportable contacts or who acquired reportable information must report the contact or information, verbally or in writing, to AFOSI or their servicing MDCO within 30 duty days of the contact. **(T-0)** If necessary, personnel can report the information to their commander, supervisor, or security officer who will immediately provide the information to their servicing AFOSI office. **Note:** For the purpose of this paragraph, "contact" means any exchange of information directed to an individual, including solicited or unsolicited telephone calls, text messages, interaction via social media and networking websites, e-mail, radio contact, or other means that enable communications, to include face-to-face discussions. This does not include contact by "mass media" such as television or radio broadcasts, public speeches, or other means not directed at specific individuals. It also excludes contact as part of the official duties of the member. Nothing in this paragraph replaces or eliminates the reporting required as part of official duties. Reference DoDD 5240.06 for reportable information.

3.2. Responsibility to Report Incidents. The following personnel must report incidents to their servicing MDCO without delay; all other personnel associated with DAF activities but not listed below will report CI incidents to their servicing MDCO as soon as possible:

3.2.1. US Air Force and US Space Force personnel and DAF civilian employees.

3.2.2. Air Force Reserve personnel while in active status and Category B reservists on inactive duty for training status.

3.2.3. Air National Guard personnel when performing or supporting a federal mission.

3.2.4. Foreign national employees of the DoD in foreign areas, as stipulated in command directives and Status of Forces Agreements.

3.2.5. DAF contract employees and DoD contractor personnel with security clearances.

3.2.6. Civilian employees of US defense agencies for which AFOSI provides CI support IAW AFPD 71-1 and DoDI O-5240.10, *Counterintelligence (CI) in the DoD Components*, and employees of the USG in foreign nations for whom the DAF provides support.

3.3. Failure to Report.

3.3.1. The reporting requirements in **Chapter 3** and DoDD 5240.06 are mandatory. Failure to observe the reporting requirements of this instruction by military personnel is a violation of Article 92, *Failure to Obey Order or Regulation*, Uniform Code of Military Justice.

3.3.2. Failure to observe the reporting requirements in **Chapter 3** and DoDD 5240.06 by civilian employees may result in administrative disciplinary action under applicable civilian personnel instructions without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

Chapter 4

COUNTERINTELLIGENCE PROGRAM

4.1. Counterintelligence Investigations. AFOSI is responsible for the conduct, management, coordination, and control of CI investigations within the DAF IAW DoDD 5240.02 and DoDI 5240.04, *Counterintelligence (CI) Investigations*. This includes investigations of active duty and reserve military personnel, DoD civilians, and other DoD affiliated personnel. AFOSI will:

4.1.1. Report incidents to the FBI meeting the criteria of Title 50 US Code (USC) § 3381(e), *Coordination of Counterintelligence Activities*, and refer CI investigative matters to the FBI IAW DoDI 5240.04 and Title 28 USC § 533, *Investigative and Other Officials; Appointment*. **(T-0)**

4.1.2. Ensure all personnel assigned to CI investigative duties successfully complete formal CI training IAW DoDD 5240.02. **(T-0)**

4.1.3. Respond within 14 calendar days after receiving a CI referral from a DoD component to the referring component and provide a determination to accept or decline the CI referral for investigation. **(T-1)**

4.1.4. Brief appropriate command officials regarding CI investigations that require continuing access to classified information determinations and other personnel security actions.

4.1.5. Keep the Combatant Commander and the DoD Component heads informed of CI investigations taking place within their respective areas of responsibility or affecting their interests. **(T-0)**

4.1.5.1. Take pertinent measures to protect investigative integrity and processes. **(T-0)**

4.1.5.2. Assist in periodic command briefings concerning these investigations IAW DoDI O-5240.10. **(T-0)**

4.1.6. Submit financial information requests for support to CI investigations. Maintain an annual tabulation of the occasions in which personnel utilized access procedures IAW DoDI 5400.15, *Guidance on Obtaining Financial Information from Financial Institutions*, Title 12 USC § 3414, *Special Procedures*, Title 15 USC § 1681V, *Disclosures to Governmental Agencies*, and Title 50 USC § 3162, *Requests by Authorized Investigative Agencies*. **(T-0)**

4.1.6.1. AFOSI, Judge Advocate (AFOSI/JA), will provide legal reviews of requests for financial information before submission to financial institutions. **(T-0)**

4.1.6.2. AFOSI/JA will conduct a legal review of financial institution responses to verify the response is within the scope of the request. **(T-0)**

4.1.7. Provide the Director, Defense Intelligence Agency, copies of all DoD unknown subject leads received from non-DoD agencies and CI investigative reporting IAW DoDI 5240.04. **(T-0)**

4.1.8. Return to the Defense Intelligence Agency all original documentation, results of all inquiries, files, leads, and all other relevant information provided by the Defense Intelligence Agency, if a DoD unknown subject investigation fails to identify the subject IAW DoDI 5240.04. **(T-0)**

4.1.9. Conduct CI investigations and activities in cyberspace to identify, disrupt, neutralize, penetrate, and exploit FIE threats targeting the DAF and DoD IAW DoDD 5240.02 and DoDI S-5240.23. **(T-0)**

4.1.10. Pursue, counter, and deter insiders who abuse their access to DAF and DoD information systems IAW DoDD 5240.06. **(T-0)**

4.2. Offensive Counterintelligence Operations. AFOSI will operate an Offensive CI Operations program IAW DoDI S-5240.09, *(U) Offensive Counterintelligence Operations (OFCO)*. **(T-0)** The Deputy Chief of Staff for Operations of the United States Air Force (AF/A3) supports Offensive CI Operations and serves as the approval authority for DAF proprietary items IAW DoDI S-5240.09, as required.

4.3. Counterintelligence Analysis and Production. AFOSI CI elements will produce analytic products to outline, describe, or illustrate the threat posed by espionage, international terrorism, subversion, sabotage, assassination, and covert activities. **(T-1)** This includes the analysis identifying opportunities to conduct Offensive CI Operations targeting a FIE, to identify CI investigative opportunities, and other activities possessing a FIE nexus, IAW DoDI 5240.18, *Counterintelligence (CI) Analysis and Production*. **(T-0)**

4.3.1. CI analytical products, unless otherwise exempt by ICD 501, *Discovery and Dissemination or Retrieval of Information Within the Intelligence Community*, will be included in the Library of National Intelligence. **(T-0)**

4.3.2. CI analytical products intended for release to foreign governments will be coordinated IAW applicable DAF and DoD policies and released only IAW Director of National Intelligence policies for disclosure of classified information and controlled unclassified information. **(T-0)**

4.3.3. CI analysis and production supports three pillars:

4.3.3.1. Lead. Support and generate timely and actionable field-level investigative, collection, and operational leads to AFOSI through proactive analysis and production.

4.3.3.2. Inform. Provide current and relevant criminal, intelligence, and terrorist threat information to AFOSI, DAF, DoD, National-level leadership, and other customers as appropriate.

4.3.3.3. Support. Provide CI, LE, and cyber subject matter expertise and analytic support to AFOSI investigations, collection activities, and operations.

4.4. Counterintelligence Collection and Reporting. AFOSI is the sole DAF agency authorized to perform CI collection activities. AFOSI unit and non-unit leaders will ensure personnel conducting CI activities adhere to policy and procedures IAW DAFI 14-404, *Intelligence Oversight*, DoDD 5240.01, *DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities*, DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, and DoDI S-5240.17, *(U) Counterintelligence Collection Activities (CCA)*.

4.4.1. Personnel engaged in CI collection activities and collection management responsibilities will be adequately trained, research applicable collection requirements, and prepare CI execution plans IAW DAF CI Strategy. **(T-0)**

4.4.2. Leadership will deconflict CI collection conducted with foreign counterpart intelligence, CI, security, and LE entities with other USG agencies, as needed. **(T-0)**

4.4.3. All CI collection and the use of public information must be consistent with limitations IAW DAFI 14-404, DoDI S-5240.17, DoDI 3115.12, *Open Source Intelligence (OSINT)*, DoDM 5240.01, and DoDD 3115.18, *DoD Access to and Use of Publicly Available Information*. **(T-0)** AFOSI authorizes CI elements to conduct the following activities as part of the CI mission:

4.4.3.1. Partner Engagement. Partner engagement meetings or events with US and foreign security, LE, CI, and intelligence organizations and non-DoD affiliated personnel.

4.4.3.2. Open Source and Media Exploitation. Open sources, captured documents, and other media may be exploited in support of validated CI collection requirements.

4.4.3.3. CI Briefings and Debriefings. Briefings, debriefings, and screenings of personnel who may possess information responsive to CI collection requirements.

4.4.3.4. CI Collection in Cyberspace. Operations in cyberspace are designed to collect and report information responsive to validated requirements.

4.4.3.5. Sources. AFOSI special agents, upon successful completion of designated training, may utilize confidential sources, formally recruited or non-recruited, to collect information responsive to validated requirements or to support CI operations and investigations.

4.4.3.6. CI Interrogation of Enemy Prisoners of War and Detainees. Conduct interrogations IAW DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*.

4.5. Counterintelligence Support to Research, Development and Acquisition of Critical Programs and Technology. IAW DoDI O-5240.24, AFOSI will conduct proactive and comprehensive CI activities in support of Research, Development, and Acquisition (RDA) of CP&T. **(T-0)** This includes the appointing of a CI subject matter expert to advise and assist the Assistant Secretary of the Air Force, Acquisition, Technology, and Logistics (SAF/AQ), and support the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S), and the Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E). It further includes helping to manage horizontal technology protection initiatives and support DAF milestone decision authority to determine sufficiency of CI support during reviews of DAF RDA program protection plans, technology area protection plans, and Science and Technology Protection Plans. **(T-0)**

4.5.1. AFOSI will conduct CI activities with international partners in support of RDA of CP&T, international transfers of export-controlled defense-related technology, and technology transfer of non-export controlled restricted technology; coordinate, synchronize, and deconflict CI activities supporting RDA with DoD and DAF HUMINT elements; and coordinate CI activities at a Cleared Defense Contractor with local Defense Counterintelligence and Security Agency CI personnel and the FBI for activities at a federally funded research and development center or university affiliated research center. **(T-0)**

4.5.2. AFOSI investigations into export-controlled technologies on the US Munitions List or the Commerce Control Listing must be coordinated with US Homeland Security Investigations, the FBI, and the Bureau of Industry and Security, Office of Export Enforcement, IAW EO 13558, *Export Coordination Enforcement Center*, Title 22 USC § 2778, *Control of Arms Exports and Imports*, and Title 50 USC§ 2411, *Director for Cost Estimating and Program Evaluation*. **(T-0)**

4.5.3. CI Analysis and Production in support of RDA will be completed IAW DoDI 5240.18 and applicable director of national intelligence policies.

4.5.4. IAW Title 32 Code of Federal Regulation (CFR) Part 117, *National Industrial Security Program Operating Manual (NISPOM)*, AFOSI will provide CI support normally provided by Defense Counterintelligence and Security Agency when a DAF installation commander retains security cognizance of a Cleared Defense Contractor facility handling collateral information on a DAF installation. **(T-0)**

4.5.4.1. AFOSI will identify a local point of contact for CI matters and include the facility in the local CI threat report, when applicable. **(T-0)**

4.5.4.2. AFOSI will receive and review security vulnerabilities and CI implication reports of security incidents identified during the installation commander's facility security review. AFOSI will also review countermeasures proposed in response to the facility security vulnerabilities. **(T-0)**

4.5.4.3. AFOSI will support small business innovation research and small business technology transfer due diligence programs with CI reviews of Foreign Ownership, Control, or Influence.

4.6. Counterintelligence Support to Supply Chain Risk Management. IAW DoDI O-5240.24 and DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, AFOSI will conduct threat analyses of supply chain risk to DAF requirements. **(T-0).** Additionally, AFOSI will conduct proactive and comprehensive criminal investigative and CI activities in support of supply chain risk management, IAW DoDI 4140.67, *DoD Counterfeit Prevention Policy*, in recognition of the interrelationship between counterfeiting and supply chain risk management threats, particularly to weapon system effectiveness and efficiency. **(T-0)** IAW DoDI 5240.18, AFOSI will conduct Analysis and Production activities in support of supply chain risk management.

4.7. Counterintelligence Support to the Defense Critical Infrastructure. IAW DoDI 5240.19, AFOSI will conduct proactive and comprehensive CI activities in support of DCI and will provide comprehensive, timely reporting of potential foreign threat incidents, events, and trends to DCI authorities and DoD Components. **(T-0)** IAW DoDI 5240.18, AFOSI will conduct Analysis and Production activities in support of DCI.

4.8. Counterintelligence Support to the Insider Threat Program. AFOSI will integrate and validate CI insider threat information requirements into other intelligence collection requirements and develop CI policy, programming, and resource requirements to implement a comprehensive insider threat program, IAW DoDI 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat*. **(T-0)**

4.8.1. AFOSI will address security equities across CI functions IAW DAF Policy Directive (DAFPD) 16-14, *Security Enterprise Governance*, and DAFI 16-1402, *Counter-Insider Threat Program Management*. **(T-0)**

4.8.2. AFOSI will provide supported organizations with CI insider threat briefings as part of the existing CI awareness program; establish and implement CI initiatives to identify and counter espionage, international terrorism, and CI insider threats; conduct information exchanges with federal, state, local, tribal, and foreign agencies on CI insider threats; and conduct anomaly-based detection activities. **(T-0)**

4.9. Counterintelligence Support to Force Protection. AFOSI will collect and provide threat data to command officials for the protection of DAF programs, personnel, and equities in deployed and in-garrison environments IAW DoDI 5240.18 and DoDI 5240.22, *Counterintelligence Support to Counterterrorism and Force Protection*. **(T-0)** AFOSI will provide personnel to support Force Protection Detachments and Joint Terrorism Task Force offices as determined by AFOSI; conduct liaison with federal, state, local, and foreign agencies for the collection and appropriate exchange of terrorist threat information; and provide tailored international terrorist briefings to supported commands as part of a CI awareness program IAW DoDD 5240.06. **(T-0)**

4.9.1. AFOSI will ensure that deploying personnel assigned to conduct CI activities complete specialized training for CI support to Force Protection IAW DoDI 5240.22. **(T-0)**

4.9.2. AFOSI will provide annual local threat report information to the installation threat working groups and/or appropriate threat and/or terrorism groups and will be active participants within these groups for threat data, IAW DAFI 31-101*, Integrated Base Defense*, and other applicable instructions pertaining to force protection and integrated defense. **(T-2)**

4.10. Counterintelligence Support to Combatant Commands and Other DoD Components. AFOSI will provide CI support to Combatant Commands and DoD Components IAW DoDI O-5240.10, to include providing assessments on the FIE threat. **(T-0)** Additionally, AFOSI will assign personnel with CI experience, as required, to serve as the Command CI Coordinating Authority to designated Combatant Commands and Joint Staff. **(T-0)**

4.11. Classifying Counterintelligence Information. CI information within the DAF is classified IAW DoDI C-5240.08, *Counterintelligence (CI) Security Classification Guide (U)*; DoDM 5200.01 Volume 2, *DoD Information Security Program: Marking of Information*; and DoDM 5200.01V3_DAFMAN 16-1404V3.

4.12. Collection of US Person Information. AFOSI may collect information regarding a US person, as defined in DoDM 5240.01, in its role as a Defense Intelligence Component, only as necessary to perform its assigned mission. **(T-0)**

4.12.1. The collection must meet the standard of information that can be collected IAW DoDM 5240.01 Procedure 2. **(T-0)** The existence of a collection category does not convey authorization to collect; a link is required between the US person information to be collected and the AFOSI CI mission.

4.12.1.1. AFOSI may collect US person information by any lawful means. **Note:** AFOSI must exhaust all feasible less intrusive means prior to requesting a more intrusive collection activity IAW DoDM 5240.01. **(T-0)**

4.12.1.2. Information acquired incidentally to an otherwise authorized collection may be retained up to five years for evaluation. **(T-0)**

4.12.2. Retention and dissemination must be IAW DoDM 5240.01 Procedure 3 and Procedure 4. **(T-0)**

4.12.2.1. Information regarding US persons may be retained temporarily IAW DoDM 5240.01 solely for the purpose of determining if the information may be permanently retained. If the information may not be retained, it must be appropriately disposed of or destroyed IAW DoDM 5240.01 and DAF instructions. **(T-0)**

4.12.2.2. Specific categories of authorized retention include information collected under the provisions of DoDM 5240.01; information necessary to understand or assess foreign intelligence or CI; information of foreign intelligence or CI collected from authorized electronic surveillance; or information that may indicate involvement in activities violating federal, state, local, or foreign law.

4.13. Specialized Techniques in Counterintelligence Investigations and Operations. AFOSI is the sole agency within the DAF authorized to use specialized techniques for CI purposes, as defined by DoDM 5240.01. This same definition applies even if AFOSI requests other agencies to use these techniques in support of the DAF. **Note:** For the purposes of this paragraph, AFOSI is a DoD intelligence component IAW DoDM 5240.01. The authority to conduct specialized techniques resides solely with the AFOSI/CC. The AFOSI/CC may delegate this authority in writing to a headquarters level senior official who exercises direct oversight authority of CI investigative operations. Although the authority may be delegated, the AFOSI/CC always retains authority over AFOSI operations. In all cases, AFOSI must comply with the requirements of DoDM 5240.01 and DAFI 14-404. **(T-0)**

4.13.1. The AFOSI/CC will provide SAF/GC and AF/JA prior notice, with a reasonable opportunity to respond, before taking action on the use of any specialized technique reasonably identifiable as being of high sensitivity, of specific interest to SecAF, or having the potential for significant Congressional, media, or public interest. **(T-1)** The AFOSI/CC may approve an emergency request prior to providing notice to SAF/GC or AF/JA but will provide SAF/GC and AF/JA a written record of the request and a written record of the action taken within 72 hours of the emergency approval. **(T-1)**

4.13.2. The procedures described in this instruction are for CI purposes only. In all other AFOSI activities, the procedures prescribed in DAFI 71-101 Volume 1, *Criminal Investigations Program*, apply.

4.13.3. Electronic Surveillance implements the Foreign Intelligence Surveillance Act Title 50 USC Chapter 36 Subchapter I, *Electronic Surveillance*, §§ 1801-1813, 50 USC Chapter 36 Subchapter VI, *Additional Procedures Regarding Certain Persons Outside the United States*, §§ 1881b-d, and EO 12333 § 2.5, *Conduct of Intelligence Activities-Attorney General Approval*. AFOSI may conduct electronic surveillance pursuant to an order issued by the Foreign Intelligence Surveillance Court or upon Attorney General authorization.

4.13.4. DoDM 5240.01 Procedure 6 governs concealed monitoring of any person inside the US or any US person outside the US for an authorized foreign intelligence or CI purpose by a Defense Intelligence Component or anyone acting on their behalf.

4.13.4.1. A subject's reasonable expectation of privacy is a determination that depends on the circumstances of a particular case and will be made only after consultation with the servicing legal office advising the DoD intelligence component concerned (i.e., AFOSI). **(T-0)** Reasonable expectation of privacy is the extent to which a particular person in particular circumstances have a reasonable belief that their activities, property, or communications are private. Concealed monitoring operations must be approved by the AFOSI/CC, or delegated authority, IAW DoDM 5240.01. **(T-0)**

4.13.4.2. Under Title 18 USC § 2511, *Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited*, the electronic communications of a computer trespasser transmitted to, though, or from a protected computer may be intercepted under the following circumstances: the owner/operator of the protected computer authorizes, in writing, the interception of the computer trespasser's communications on the protected computer; the interception is to be conducted pursuant to a lawful CI investigation; there is reason to believe the contents of the computer trespasser's communication is relevant to the investigation; and the interception does not acquire communications other than those transmitted to or from the computer trespasser.

4.13.5. DoDM 5240.01 Procedure 7 authorizes AFOSI to conduct nonconsensual physical searches of active duty military personnel or their property within the US for intelligence purposes, when approved by the Attorney General or Foreign Intelligence Surveillance Court.

4.13.6. DoDM 5240.01 Procedure 8 applies to mail covers and the opening of mail within US postal channels for foreign intelligence and CI purposes. AFOSI may search the mail of active-duty military personnel pursuant to an order issued by the Foreign Intelligence Surveillance Court or upon Attorney General authorization. DoDM 5240.01 Procedure 8 also applies to the opening of mail to or from other US persons or non-US persons when the mail is not in US postal channels and the mail opening occurs outside the US. AFOSI may request that United States Postal Service® authorities examine mail (mail cover) in United States Postal Service® channels for CI purposes. AFOSI may request mail cover outside United States Postal Service® channels IAW appropriate host nation law and procedures, and any Status of Forces Agreements.

4.13.7. DoDM 5240.01 Procedure 9 applies to nonconsensual physical surveillance for foreign intelligence or CI purposes. It does not apply to physical surveillance conducted as part of testing or training exercises in which the surveillance subjects are exercise participants. AFOSI may conduct nonconsensual physical surveillance of US persons only if they are a present or former military or civilian employee of a Defense Intelligence Component; a present or former contractor of a Defense Intelligence Component or a present or former employee of such a contractor; an applicant for such employment or contracting; or a military member employed by a non-intelligence element of the military; or persons in contact with those who fall into the above categories to the extent necessary to ascertain the identity of the person in contact. Surveillance does not include personnel of the broader intelligence community. Surveillance conducted outside a DoD installation or of civilians on DoD installations must be coordinated with the FBI and other LE agencies as appropriate. **(T-0)** AFOSI may conduct nonconsensual physical surveillance of a non-US person in the US for an authorized CI purpose.

4.13.8. DoDM 5240.01 Procedure 10 applies to AFOSI personnel participating in any organization within the US, or a US person organization outside the US, on behalf of AFOSI for CI purposes. It also applies when AFOSI requests an employee act within an organization for AFOSI's benefit, whether the employee is already a member of an organization or is asked to join an organization. Actions for AFOSI benefit include collecting information, identifying potential sources or contacts, and other activities directly relating to foreign intelligence or CI functions. DoDM 5240.01 Procedure 10 does not apply to personal participation. Activities conducted within an organization solely for personal purposes (i.e., activities undertaken upon the initiative and at the expense of a person for personal benefit).

4.13.9. Unless otherwise proscribed by law or DoD policy, specialized techniques may be authorized by the appropriate approving authority for a period of 180 calendar days (with exceptions addressed in **paragraph 4.13.9.1** and **paragraph 4.13.9.2**.). Extensions may be granted upon submission of appropriate justification. All requests and approvals will be documented in internal AFOSI records and will be disclosed only to competent authorities for official purposes. **(T-0)**

4.13.9.1. CI investigations utilizing DoDM 5240.01 Procedure 6, and the computer trespasser exception may be authorized by the AFOSI/CC, or delegated authority, for up to 12 months. AFOSI/JA will provide a legal review for the addition of new monitoring sites; once legally sufficient, the sites may become operational under the existing authority. **(T-1)** The AFOSI/CC or delegee may authorize extensions for cyber CI investigations annually with appropriate justification. All active monitoring sites are included in the overall operations plan for AFOSI commander extensions.

4.13.9.2. Investigations utilizing DoDM 5240.01 Procedure 10 may be authorized for 12 months.

4.13.10. The AFOSI/CC publishes internal instructions directing the conduct and approval process for all specialized and operational techniques. AFOSI documents the approvals, the specific techniques utilized, the identity of persons monitored, and the disposition of the products of such techniques in internal documentation. Operational plans and approvals must be maintained IAW AFI 33-322. **(T-1)**

4.13.11. In joint investigations and collection activities in which AFOSI cannot conduct CI activities under its own authority, the AFOSI/CC, or delegated authority, may approve AFOSI operating under the authority of another US intelligence agency, such as the FBI. **Note**: The AFOSI ICON Center must be notified if authorized US federal agencies request approval to initiate operational techniques under their own authority on a DoD installation or DoD leased property. **(T-0)** In addition, AFOSI may utilize specialized techniques under the approval authority of another authorized US federal agency after consultation with AFOSI/JA and if an agency's request contains the following:

4.13.11.1. AFOSI is operating under the requesting agency's authorities. **(T-0)**

4.13.11.2. The techniques to be used must have been approved by the appropriate agency's authority/policy. **(T-0)**

4.13.11.3. The agency must conduct its own legal review and concurrence of those techniques to be used. **(T-0)**

4.13.12. AFOSI/JA is the primary legal office authorized to provide legal guidance and conduct legal reviews of specialized techniques conducted by AFOSI. All specialized techniques must be reviewed for legal sufficiency prior to operation initiation. **(T-1)**

4.13.13. Procedures requiring approval outside AFOSI are staffed through AFOSI to SAF/GC and AF/JA. The requests are reviewed by SAF/GC and AF/JA, who ensure approval is obtained from the appropriate authority.

4.14. Other Operational Techniques Targeting United States Persons. AFOSI utilizes other techniques for CI purposes IAW DoDD 5240.01 and DoDM 5240.01. **Note:** For the purposes of this paragraph, AFOSI is a DoD intelligence component as defined in DoDD 5240.02. The AFOSI/CC, or delegated authority, must approve the following operational techniques prior to initiation:

4.14.1. Trash cover. **(T-1)**

4.14.2. National Security Letters. **(T-1)**

4.14.3. DoD Subpoena. **(T-1)**

4.14.4. AFOSI/JA is the primary legal office authorized to provide legal guidance and conduct legal reviews of other operational techniques in support of CI operations conducted by AFOSI. All other operational techniques must be legally reviewed prior to operation initiation. **(T-0)**

4.15. Interception of Wire, Oral, or Electronic Communications.

4.15.1. The AFOSI/CC, or delegated authority, must approve the consensual acquisition of nonpublic wire, oral or electronic communications in which at least one party to the communication consents to such interception. **(T-0)**

4.15.2. The AFOSI/CC authorities encompass all consensual interceptions within the US and all consensual interceptions of US person targets outside of the US. The activity may be approved verbally after consultation with AFOSI/JA only in emergency situations. A written approval and legal review must be conducted to document the decision. **(T-1)** Reference DAFI 71-101V1 for guidance on consensual interceptions for LE purposes.

4.15.3. Conduct non-consensual interceptions of non-public wire, oral, or electronic communications IAW DoDM 5240.01 Procedure 5 and this instruction. **(T-0)** SAF/GC and AF/JA will review the request and ensure approval is obtained from the appropriate authority. **(T-0)**

4.15.4. The AFOSI/CC, or delegated authority, must approve all interceptions of wire, oral, or electronic communications targeting non-US persons in foreign nations. **(T-1)** All US persons involved must be aware of the operation and consent to the monitoring. **(T-0)**

4.16. Operations Targeting Non-United States Persons. AFOSI may collect information regarding non-US persons in the role as a Defense Intelligence Component, only as necessary to perform the assigned mission.

4.16.1. Operations Targeting Non-US Persons within the US. AFOSI may collect information regarding non-US persons within AFOSI's jurisdiction or in conjunction with partner agencies that hold jurisdiction.

4.16.1.1. All specialized or other techniques that target non-US persons will be reviewed by AFOSI/JA and approved by the AFOSI/CC, or delegated authority. **(T-1)**

4.16.1.2. When the individual has a reasonable expectation of privacy and when a warrant would be required for LE purposes, concealed monitoring is treated and processed as electronic surveillance. Monitoring is considered within the US if the monitoring device, or the monitored target, is located within the US.

4.16.2. Operations Targeting Non-US Persons Outside the US. The use of specialized or other techniques in CI activities targeting non-US persons outside the US may be subject to limitations or requirements imposed by the Status of Forces Agreements. A review of Status of Forces Agreements requirements or limitations is normally accomplished in coordination with the applicable MAJCOM International Law attorney.

4.16.2.1. All specialized or other techniques that target non-US persons will be reviewed by AFOSI/JA and approved by the AFOSI/CC, or delegated authority. **(T-1)**

4.16.2.2. AFOSI will coordinate with the Central Intelligence Agency when conducting CI activities in foreign nations IAW ICD 304, *Human Intelligence,* and ICD 310, *Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States*.

4.16.2.3. In a deployed area of responsibility, the Combined Air Operations Center, Staff Judge Advocate, or deployed Staff Judge Advocate will review and approve the application of each technique to ensure compliance with Intelligence Oversight and/or the Law of War. **(T-1)** A copy of the approval must be provided to AFOSI/JA. **(T-1)**

4.17. Emergency and Extraordinary Expense Funds. Subject to the availability of appropriations, Title 10 USC § 127, *Emergency and Extraordinary Expenses*, provides the SecAF authority for any emergency or extraordinary expenses that cannot be anticipated or classified. AFOSI will use emergency and extraordinary expenses for authorized requirements that contribute to CI or investigative missions and/or aids in acquiring CI or criminal investigative information, IAW AFPD 71-1 and DAFI 71-101V1.

4.18. Counterintelligence Support to HUMINT Collection Activities. AFOSI provides CI support to DAF HUMINT Operations IAW the Defense Counterintelligence and Human Intelligence Enterprise Manual Volume II, *Human Intelligence Collection Operations (U) (DCHE-M) 3301.002*, to include: CI support to HUMINT collection, asset validation, and enabling activities IAW applicable law and policy. Where applicable, AFOSI will leverage the capabilities and resources of the DoD CI community to protect and enhance DAF HUMINT operations and ensure coordination between CI elements and HUMINT collectors at the relevant echelons.

DAVID B. LYONS
Lieutenant General, USAF
The Inspector General

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

10 USC § 127, *Emergency and Extraordinary Expenses*

12 USC § 3414, *Special Procedures*

15 USC § 1681V, *Disclosures to Governmental Agencies*

18 USC § 2511, *Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited*

22 USC § 2778, *Control of Arms Exports and Imports*

28 USC § 533, *Investigative and Other Officials; Appointment*

50 USC Subchapter I, *Electronic Surveillance*

50 USC Chapter 36 Subchapter VI, *Additional Procedures Regarding Certain Persons Outside the United States*

50 USC § 2411, *Director for Cost Estimating and Program Evaluation*

50 USC § 3162, *Requests by Authorized Investigative Agencies*

50 USC § 3381(e), *Coordination of Counterintelligence Activities*

EO 12333, *United States Intelligence Activities*

EO 12333 § 1.7(f), *The Intelligence and Counterintelligence Elements of the Army, Navy, Air Force, and Marine Corps*

EO 12333 § 2.5, *Conduct of Intelligence Activities-Attorney General Approval*

EO 13558, *Export Coordination Enforcement Center*

32 CFR Part 117, *National Industrial Security Program Operating Manual (NISPOM)*

DoDD 3020.40, *Mission Assurance (MA)*, 29 November 2016

DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 11 October 2012

DoDD 5148.13, *Intelligence Oversight*, 26 April 2017

DoDD 5240.01, *DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities*, 27 September 2024

DoDD 5240.02, *Counterintelligence (CI)*, 17 March 2015

DoDD 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*, 17 May 2011

DoDD 5505.13E, *DoD Executive Agent (EA) for The DoD Cyber Crime Center (DC3)*, 1 March 2010

DoDI 3115.12, *Open Source Intelligence (OSINT)*, 24 August 2010

DoDD 3115.18, *DoD Access to and Use of Publicly Available Information*, 20 August 2020

DoDI 4140.67, *DoD Counterfeit Prevention Policy*, 2 February 2024

DoDI 5200.39, *Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)*, 28 May 2015

DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, 16 February 2024

DoDI 5240.04, *Counterintelligence (CI) Investigations*, 1 April 2016

DoDI C-5240.08, *Counterintelligence (CI) Security Classification Guide (U)*, 28 November 2011

DoDI S-5240.09, *(U) Offensive Counterintelligence Operations (OFCO)*, 2 February 2015

DoDI O-5240.10, *Counterintelligence (CI) in the DoD Components*, 27 April 2020

DoDI S-5240.17, *(U) Counterintelligence Collection Activities (CCA)*, 14 March 2014

DoDI 5240.18, *Counterintelligence (CI) Analysis and Production*, 17 November 2009

DoDI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)*, 31 January 2014

DoDI 5240.22, *Counterintelligence Support to Counterterrorism and Force Protection*, 12 October 2022

DoDI S-5240.23, *(U) Counterintelligence (CI) Activities in Cyberspace*, 13 December 2010

DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research*, *Development, and Acquisition (RDA)*, 8 June 2011

DoDI 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat*, 4 May 2012

DoDI 5400.15, *Guidance on Obtaining Financial Information from Financial Institutions*, 12 February 2004

DoDM 5200.01V2, *DoD Information Security Program: Marking of Information*, 24 February 2012

DoDM 5200.01V3, *DoD Information Security Program: Protection of Classified Information*, 24 February 2012

DoDM 5205.07, *Special Access Program Security Manual*, 17 January 2025

DoDM 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, 8 August 2016

DAFPD 16-14, *Security Enterprise Governance*, 29 July 2025

AFPD 71-1, *Criminal Investigations and Counterintelligence,* 1 July 2019

DAFI 14-404, *Intelligence Oversight*, 23 January 2025

AFI 16-701, *Management, Administration and Oversight of Special Access Programs*, 18 February 2014

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

DAFI 31-101*, Integrated Base Defense*, 10 September 2024

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

DAFI 71-101V1, *Criminal Investigations Program*, 24 January 2025

HAFMD 1-14, *General Counsel and The Judge Advocate General*, 29 December 2016

AFMD 39, *Air Force Office of Special Investigations (AFOSI)*, 12 February 2024

DoDM5200.02_DAFMAN16-1405, *Department of Air Force Personnel Security Program*, 1 August 2018

DoDM5200.01V1_DAFMAN16-1404V1, *Information Security Program: Overview, Classification, and Declassification*, 6 April 2022

DoDM5200.01V3_DAFMAN16-1404V3, *Information Security Program: Protection of Classified Information*, 12 April 2022

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

Defense Counterintelligence and Human Intelligence Enterprise Manual Volume II, *Human Intelligence Collection Operations (U) (DCHE-M) 3301.002*, 22 June 2015

ICD 304, *Human Intelligence*, 9 July 2009

ICD 310, *Coordination of Clandestine Human Source and Human- Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States*, 27 June 2016

ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, 21 January 2009

ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*, 21 June 2013

Manual for Courts Martial *United States*, 2024 Edition

Security Executive Agent Directive 3, *Reporting Requirements for Personnel with Access to Classified Information or who Hold a Sensitive Position*, 12 June 2017

Memorandum of Understanding *Between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities*

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

§—Section

AFI—Air Force Instruction

AFMD—Air Force Mission Directive

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

CFR—Code of Federal Regulation

CI—Counterintelligence

CP&T—Critical Programs and Technologies

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFPD—Department of the Air Force Policy Directive

DC3—Department of Defense Cyber Crime Center

DCI—Defense Critical Infrastructure

DoDD—Department of Defense Directive

DoD—Department of Defense

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

EO—Executive Order

FBI—Federal Bureau of Investigation

FIE—Foreign Intelligence Entity

HUMINT—Human Intelligence

IAW—In Accordance With

ICD—Intelligence Community Directive

LE—Law Enforcement

MDCO—Military Department Counterintelligence Organization

RDA—Research, Development, and Acquisition

RDT&E—Research, Development, Test, and Evaluation

SecAF—Secretary of the Air Force

USC—United States Code

USG—United States Government

US—United States

Office Symbols

AF/A3—Deputy Chief of Staff for Operations of the United States Air Force

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

AFOSI ICON CENTER—AFOSI, Investigations Collections Operations Nexus Center

AFOSI PJ—AFOSI, Office of Special Projects

AFOSI/CC—Commander, AFOSI

AFOSI/JA—AFOSI, Judge Advocate

OUSD A&S—Office of the Under Secretary of Defense for Acquisition and Sustainment

OUSD R&E—Office of the Under Secretary of Defense for Research and Engineering

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

SAF/GC—Secretary of the Air Force, General Counsel

SAF/IGX—Secretary of the Air Force, Inspector General, Special Investigations

SAF/LL—Secretary of the Air Force, Legislative Liaison

SAF/PA—Secretary of the Air Force, Office of Public Affairs

Terms

Contact—Any form of meeting, association, or communication, in person, by radio, telephone, letter or other means, regardless of who started the contact or if it was for social, official, private, or other reasons.

Controlled Unclassified Information—Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and USG-wide policies.

Counterintelligence (CI)—Information gathered, and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their Agents, or international terrorist organizations or activities.

Counterintelligence Activities in Cyberspace—Activities to identify, disrupt, neutralize, penetrate, or exploit FIE activities, threats, or plans, as FIE operate in cyberspace or use it as a conduit to achieve some effect.

Counterintelligence Collection—The systematic acquisition of information concerning espionage, sabotage, terrorism, other intelligence activities or assassinations conducted by or on behalf of terrorists, foreign powers, and other entities.

Counterintelligence Functional Activities—One or more of the CI functions of analysis, collection, functional services, investigations, operations, and production.

Counterintelligence Functional Services—CI activities conducted to support the four missions of CI, investigations, operations, collection, analysis, and production and those which enable one or more of the other CI functions.

Counterintelligence Investigations—Formal investigative activities undertaken to determine if a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize such acts.

Counterintelligence Training—Institutional training in knowledge, skills, abilities, and core competencies unique to CI missions and functions.

Defensive Travel Briefings—Formal advisories alerting personnel of the potential for harassment, exploitation, provocation, capture, or entrapment while traveling. These briefings, based on actual experience when available, include information on courses of action helpful in mitigating adverse security and personnel consequences and advise of passive and active measures that personnel take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

Emergency and Extraordinary Expense Funds—Emergency and Extraordinary Expense Funds used to further the CI and investigative missions of the DAF. This subdivision of operation and maintenance (O&M) funds is allocated to AFOSI, through SAF/IG, by the SecAF under certain legal restrictions to reimburse investigators for authorized expenses incurred in the performance of their assigned duties.

Electronic Surveillance—Acquisition of nonpublic communication by electronic means without the consent of a person who is party to an electronic communication or in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication but not including the use of radio direction finding equipment solely to determine the location of the transmitter. Electronic surveillance within the US is subject to the definition in the Foreign Intelligence Surveillance Act of 1978.

Espionage—The act of obtaining, delivering, transmitting, communicating, or receiving information regarding the national defense with an intent or reason to believe that the information may be used to the injury of the US or to the advantage of any foreign nation. The offense of espionage applies during war or peace.

Foreign Intelligence Entity (FIE)—Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire US information, block or impair US intelligence collection, influence US policy, or disrupt US systems and programs. This term includes a foreign intelligence and security services and international terrorist organizations.

Foreign Interest—Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered, or incorporated under the laws of any country other than the US or its possessions and trust territories; and any person who is not a citizen or national of the US.

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

Military Department Counterintelligence Organization (MDCO) and DoD Counterintelligence Agency—Military department CI agencies include Army CI, the Naval Criminal Investigative Service, and AFOSI. DoD CI agencies include the foregoing plus the CI elements of the Defense Intelligence Agency, Defense Security Service, National Reconnaissance Office, National Security Agency, and Defense Threat Reduction Agency.

National Security—A collective term encompassing both national defense and foreign relations of the US.

Sabotage—An act or acts with the intent to injure or interfere with or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises, or utilities to include human or natural resources, under reference.

Source—A person, thing or activity from which information is obtained. For the purposes of this Instruction, a source is a person who provides information responsive to collection requirements.

Subversion—An act or acts inciting military or civilian personnel of the DoD to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, of discipline, of the Military Forces of the US.

Terrorism—The calculated use of violence or threat of violence to instill fear intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Treason—Whoever, owing allegiance to the US, levies war against them or adheres to their enemies, giving them aid and comfort within the US or elsewhere, is guilty of treason.

Unauthorized Disclosure—A communication or physical transfer of classified information to an unauthorized recipient.