BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 71-101 VOLUME 4

2 JULY 2019

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 (Lt Gen Sami D. Said)

Supersedes: AFI71-101 V4, 8 November 2011

Pages: 31

This volume implements Air Force Policy Directive (AFPD) 71-1, *Criminal Investigations and CI*, and provides guidance for conducting counterintelligence activities. It further implements requirements as identified in DoD Instruction S-5105.63, *Implementation of DoD Cover and Cover Support Activities*; DoDD 5240.01, *DoD Intelligence Activities*; DoD Instruction S-5240.09, *Offensive Counterintelligence Operations (U)*; DoD Instruction 5240.22, *Counterintelligence Support to Force Protection*; DoD Instruction S-5240.23, *Counterintelligence (CI) Activities in Cyberspace (U)*; DoD Instruction O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*; and DoD Instruction 5240.26, *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat.* This publication applies to Regular Air Force, Air Force Reserve Units, the Air National Guard, and the Civil Air Patrol performing an Air Force assigned-mission.

Failure to observe the prohibitions and mandatory provisions of this instruction in **Chapter 3** by military personnel is a violation of Article 92, *Failure to Obey Order or Regulation*, Uniform Code of Military Justice. Similarly, failure to observe the prohibitions and mandatory provisions of this instruction in **Chapter 3** 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. 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. 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 requestor's commander for non-tiered compliance items. This publication may be supplemented at any level, but all direct supplements must be routed to SAF/IGX for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the OPR using the AF Form 847, *Recommendation for Change of Publication;* route AF Forms 847 from the field through appropriate chain of command. This publication requires the collection and or maintenance of information protected by the Privacy Act of 1974. The authority to collect and or maintain the records prescribed in this publication is Title 10 U.S. Code Sections 801-940. Forms affected by the Privacy Act have an appropriate Privacy Act statement. The applicable Privacy Act System Notice F071 AF OSI A, Counterintelligence Operations and Collections Records is available online at: **https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/569918/f071-af-osi-a/**. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System.

SUMMARY OF CHANGES

The publication has been revised. This rewrite of AFI 71-101, Volume 4 includes implementing requirements for offensive counterintelligence and counterintelligence support to research, development and acquisition; supply chain risk management; defense critical infrastructure program; the insider threat program and updates roles and responsibilities of the Air Force Office of Special Investigations' (AFOSI) Investigations Collections Operations Nexus (ICON) Center.

Chapter 1

RESPONSIBILITIES

1.1. Air Force Office of Special Investigations (AFOSI). AFOSI is the sole Air Force organization authorized to conduct counterintelligence (CI) investigations, operations, collections, functional services and other related activities. All AFOSI personnel engaged in conducting CI activities must attend and satisfactorily complete commensurate formal CI training approved by the Department of Defense or a Military Department. **(T-0).**

1.1.1. AFOSI is the only AF Military Department CI Organization (MDCO), with its CI authorities primarily derived from Executive Order 12333, § 1.7(f)(1-4).

1.1.2. In the U.S., AFOSI coordinates these activities with the Federal Bureau of Investigation (FBI) when appropriate, in accordance with the 2011 "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 (Counterintelligence Investigative Information Sharing), and C (Investigative and Operational Responsibilities and Coordination Procedures).

1.1.3. Outside the U.S., AFOSI coordinates these activities with the Central Intelligence Agency (CIA) and the FBI as appropriate.

1.1.4. The exercise of these authorities may be under the operational control (OPCON) of the Combatant Commander (CCDR) when specified by a military operation or operation order. The Secretary of the Air Force (SecAF) retains administrative control for those Air Force CI resources under OPCON of the CCDR.

1.1.5. 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.

1.1.6. The AFOSI ICON Center serves as the Air Force's sole reporting integration mechanism for matters pertaining to CI, investigations, and threats from foreign intelligence entities (FIE), international terrorists, cyberspace actors, and unauthorized disclosures. The AFOSI ICON Center provides timely investigative data and threat reporting data to the Commander, AFOSI, and other senior Air Force and DoD leaders. The AFOSI ICON Center is organized by regional and specialty desks, which receive and synchronize information received from AFOSI activities and other U.S. Government agencies. The AFOSI ICON Center manages AFOSI's Global Watch, which receives up-channel reporting from AFOSI field units and nonunits; the Global Watch also coordinates with other Air Force, DoD, and U.S. Government watch centers. The AFOSI ICON Center coordinates investigative and CI activities with AF human intelligence (HUMINT) activities as necessary.

1.1.7. AFOSI is the sole AF agency responsible for conducting liaison with federal, state, local and foreign law enforcement, CI and security agencies, in accordance with AFPD 71-1, *Criminal Investigations and CI*.

1.2. DoD Cyber Crime Center (DC3). Pursuant to Department of Defense 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 operates as a law enforcement and counterintelligence support activity. Component elements of DC3, such as the following, provide a broad range of support to AFOSI and DoD CI programs.

1.2.1. The DC3 Cyber Training Academy provides specialized cyber training to include digital forensics that focuses on training and improving the effectiveness of AFOSI and the DoD CI personnel that conduct CI Cyber investigations, operations, and collections.

1.2.2. DC3 Technical Solutions Development is the research, development, test and evaluation (RDT&E) component of DC3, which develops and certifies digital/multi-media forensic tools for use by AFOSI and DoD CI, intelligence, law enforcement, information assurance, and information operations personnel.

1.2.3. The DC3 Computer Forensics Laboratory supports AFOSI and DoD counterintelligence investigations and operations at the field level through the forensic analysis of digital devices and media, as well as maintains a digital forensics capability at the National Media Exploitation Center in support of Document and Media Exploitation (DOMEX) and other operations.

1.2.4. The DC3 Analytical Group leads a collaborative analytical and technical exchange with subject matter experts from AFOSI, DoD, and other federal CI, intelligence, and law enforcement agencies to build a threat picture and actionable content enabling proactive CI, law enforcement, and cyber operations focused on nation-state threat actors.

1.3. Air Force General Counsel (SAF/GC). Shall serve as legal counsel for Air Force intelligence oversight issues together with the Office of the Judge Advocate General (AF/JA). SAF/GC provides advice to intelligence components on questions of legality and propriety, as required.

1.4. Air Force Judge Advocate General (AF/JA). Shall, with Air Force General Counsel (SAF/GC), share the function of advising on policy directives, regulations and training policy. Shall serve as primary legal counsel for JA intelligence oversight training.

1.5. Air Force Commanders. Shall consult with their servicing AFOSI unit to ensure counterintelligence training meets DoD and Air Force requirements. **(T-0).** Additionally, commanders shall ensure their personnel are made aware and briefed on threats related to FIE, international terrorists, cyberspace, and unauthorized disclosures. **(T-0).** This awareness and briefing effort should emphasize individual reporting responsibilities, and include a detailed discussion about insider threats, the crimes of espionage and treason, and standards discussed in **Chapter 2**.

1.6. Air Force Personnel. Shall report threats related to FIE, international terrorists, and cyberspace to their servicing MDCO without delay. **(T-0).** Air Force personnel must report unauthorized disclosures of classified information to the appropriate security authorities in accordance with Department of Defense Manual (DoDM) 5200.01, Volume 3, *DoD Information Security Program: Protecting Classified Information*. **(T-0).** Additionally, in accordance with DoDD 5148.13, *Intelligence Oversight*, all AF personnel must report questionable intelligence activities. **(T-0).** Air Force personnel must also report significant or highly sensitive matters involving intelligence activities that may have serious implications for the execution of DoD missions. **(T-0).** It is DoD policy that senior leaders and policymakers within the Government be made aware of events that may erode the public trust in the conduct of DoD intelligence operations.

Chapter 2

COUNTERINTELLIGENCE AWARENESS AND BRIEFING PROGRAM

2.1. Air Force Awareness and Briefing Programs. AFOSI conducts, manages, and coordinates a CI awareness and briefing program. Air Force awareness and briefing programs promote threat and reporting awareness responsibility and enable Air Force personnel to identify threats, as well as the reporting of suspicious situations and incidents to appropriate authorities, in accordance with Security Executive Agent Directive 3, *Reporting Requirements for Personnel with Access to Classified Information or who Hold a Sensitive Position*, and AFPD 71-1. This awareness and briefing effort should emphasize individual reporting responsibilities, and include a detailed discussion about insider threats, the crimes of espionage**,** subversion, sabotage, assassination, sedition, terrorism, counterproliferation, and treason, and standards discussed in this instruction.

2.2. Briefings. Briefings shall include threats related to FIE, international terrorists, cyberspace, and unauthorized disclosures. **(T-0).** This awareness and briefing effort should emphasize individual reporting responsibilities, and include a detailed discussion about insider threats, the crimes of espionage and treason, and standards discussed in this instruction. **(T-0).**

2.2.1. Air Force 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 in accordance with DoDI S-5240.23, *Counter Intelligence (CI) Activities in Cyber Space (U)*. Examples of indicators of potential threat activity are listed within Department of Defense Instruction (DoDI) S-5240.23. Also refer to current cyber threat assessments posted on AFOSI's Secret Internet Protocol Router Network webpage.

2.2.3. Military personnel must receive the briefing at or near the time of initial entry. **(T-0).** Recurring briefings are required at least every 12 months or upon permanent change of station – whichever is less.

2.2.4. Civilian employees must receive the briefing at or near the time of initial entry or hire. **(T-0).** Recurring briefings occur at least every 12 months or upon permanent change of station – whichever is less.

2.2.5. The Air Education and Training Command (AETC) provides military members with their initial awareness briefing during basic training or pre-commissioning programs.

2.2.6. Air Force commanders ensure that military personnel entering the Air Force directly, through means other than AETC, and all civilian personnel receive the briefing during their initial assignment. More frequent briefing intervals should be instituted if conditions warrant, and some personnel may require more frequent briefings based on the nature of their duties.

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

2.3. CI Briefers. CI briefers should tailor the briefing for the audience and take into account the security requirements associated with the subject matter. The briefing shall include:

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

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

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

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

2.3.5. The reporting requirements of this instruction, as well as those described in DoDD 5240.06, *Counterintelligence Awareness and Reporting (CIAR)*. **(T-0).** Personnel shall report information concerning security violations and other information with potentially serious security significance regarding someone with access to classified information or who is employed in a sensitive position in accordance with AFI 16-1404_AFGM2018-01, *Air Force Information Security Program*; DoDM 5200.01, Volume 3; and AFMAN 16-1405, *Air Force Personnel Security Program*. **(T-0).**

2.4. Critical Program Information. Acquisition program personnel working with Critical Program Information pursuant to AFPD 71-1 and DoDI 5200.39, *Critical Information (CPI) Identification and Protection Within Research, Development, Test and Evaluation (RTD&E),* shall 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. Personnel with Access to Sensitive Compartmented Information (SCI) and Special Access Programs. Pursuant to Intelligence Community Directive (ICD) 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information*, and other applicable policies, personnel with SCI and special access incur special security obligations that include advance foreign travel notification for official and/or unofficial travel and defensive travel briefings. Upon completion of travel, personnel will contact AFOSI to schedule a debriefing. **(T-0).** Personnel with special access should contact their servicing AFOSI Office of Special Projects (AFOSI PJ) activity, in accordance with DoDI 5205.11 and AFI 16-701, *Management, Administration and Oversight of Special Access Programs*.

2.6. Defense Critical Infrastructure Program (DCIP). Personnel assigned to or supporting an identified DCIP critical asset, pursuant to DoDD 5240.02, *Management, Administration, and Oversight of DOD Special Access Programs (SAPs)*, DoDD 3020.40, *Mission Assurance (MA)*, and DoDI 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)*, will receive an annual CI awareness briefing at a minimum. **(T-0).** Such personnel will notify AFOSI of all projected foreign travel or foreign visits prior to the event and will receive foreign intelligence threat briefings prior to foreign visits and foreign travel. **(T-0).** Additionally, personnel projected for foreign travel will receive antiterrorism threat briefings prior to 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 Air Force repository for the collection and retention of reportable information as described below. Individuals who have reportable contacts or acquire reportable information must immediately (within 30 duty days of the contact) report the contact or information, either verbally or in writing, to AFOSI. **(T-0).** If necessary, the individual can report the information to their commander, supervisor, or security officer who immediately provides the information to their servicing AFOSI field office. 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 does not include contact as part of the official duties of the member. However, nothing in this paragraph replaces or eliminates reporting required as part of official duties. **Tables 3.1** through **3.3** contain reportable contacts, activities, indicators, behaviors, and cyber threats associated with FIEs, international terrorism, and cyberspace.

Table 3.1. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors.

Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 22 may be subject to judicial and/or administrative action in accordance with **paragraph 3.3** of this instruction. The activities in items 23 and 24 are reportable, but failure to report these activities solely may not serve as the basis for punitive action under Article 92, Uniform Code of Military Justice (UCMJ).	
Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors	
1.	When not related to official duties, contact with anyone (regardless of nationality) known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against the Department of the Air Force, other DoD or U.S. facilities, organizations, personnel, or information systems.
2.	When not related to official duties, contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization, to include attachés from any other country.
3.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties. See **Note 1**.
4.	Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.
5.	Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.
6.	Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
7.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.

8.	Discovery of suspected listening or surveillance devices in classified or secure areas.
9.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
10.	Discussions of classified information over a non-secure communication device.
11.	Reading or discussing classified or sensitive information in a location where such activity is not permitted.
12.	Transmitting or transporting classified information by unsecured or unauthorized means.
13.	Removing or sending classified or sensitive material out of secured areas without proper authorization.
14.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
15.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
16.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
17.	Unwarranted work outside of normal duty hours.
18.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
19.	Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.
20.	Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.
21.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
22.	Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or Social Networking Sites.
23.	Trips to foreign countries that are: Short trips inconsistent with logical vacation travel or not part of official duties. Trips inconsistent with an individual's financial ability and official duties.
24.	Unexplained or undue affluence. a. Expensive purchases an individual's income does not logically support. b. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture. Sudden reversal of a bad financial situation or repayment of large debts.
	Note 1: Certain Air Force members and civilian employees in positions designated as "sensitive" by their Air Force component also may be required to notify their commanders or supervisors in advance of the nature and reason for contacting a foreign diplomatic establishment.

Table 3.2. Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors.

Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 9 may be subject to judicial and/or administrative action in accordance with **paragraph 3.3** of this instruction. The activity in item 10 is reportable, but failure to report this activity solely may not serve as the basis for punitive action under Article 92, UCMJ.	
Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors	
1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organization.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the U.S. or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

Table 3.3. Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors.

Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 10 may be subject to judicial and/or administrative action in accordance with **paragraph 3.3** of this instruction. The indicators in items 11 through 19 are reportable, but failure to report these indicators solely may not serve as the basis for punitive action under Article 92, UCMJ.	
Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors	
1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of DoD account credentials by unauthorized parties.
5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus (USB), removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized e-mail traffic to foreign destinations.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data exfiltrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19.	Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

3.2. Responsibility to Report Incidents. The following persons are required to report incidents to their servicing MDCO without delay; all other persons associated with Air Force activities but not listed below should report counterintelligence incidents to their servicing MDCO as soon as possible:

3.2.1. Regular Air Force personnel and Air Force 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 (SOFA).

3.2.5. Air Force contract employees and DoD contractor personnel with security clearances.

3.2.6. Civilian employees of U.S. defense agencies for which AFOSI provides counterintelligence support in accordance with AFPD 71-1 and DoDI 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense Agencies*, and employees of the U.S. Government in foreign nations for whom the Air Force provides support.

3.3. Sanctions. The reporting requirements articulated in this chapter and outlined in **Tables 3.1**, **Table 3.2** and **Table 3.3** 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. Similarly, failure to observe the reporting requirements of this instruction in this chapter and outlined in **Tables 3.1, Table 3.2 and Table 3.3** 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

AFOSI COUNTERINTELLIGENCE PROGRAM

4.1. Counterintelligence Investigations. AFOSI is responsible for the conduct, management, coordination, and control of CI investigations within the Air Force in accordance with DoDD 5240.02, *Counterintelligence (CI)*, to include investigations of active and reserve military personnel, DoD civilians, and other DoD affiliated personnel. AFOSI shall:

4.1.1. Report to the FBI those incidents meeting the criteria of Title 50 United States Code (USC) Section 3381 (e), and refer CI investigative matters to the FBI according to guidance prescribed in DoDI 5240.04, *Counterintelligence (CI)* and 28 USC § 533 **(T-0).**

4.1.2. Ensure all personnel assigned to CI investigative duties have successfully completed formal CI training in accordance with DoDD 5240.02. **(T-0).**

4.1.3. Within 14 calendar days after receiving a CI referral from a DoD Component, respond to the referring component with a determination to either accept or decline the CI referral for investigation. **(T-1).**

4.1.4. Brief appropriate command officials on CI investigations that require determinations on continuing access to classified information and other personnel security actions. Additionally, keep the Combatant Commanders and the DoD Component heads informed of CI investigations taking place within their respective areas of responsibility or affecting their interests and assist in periodic command briefings concerning these investigations in accordance with DoDI 5240.10. **(T-0).**

4.1.5. Submit requests for financial information to support CI investigations and maintain an annual tabulation of the occasions in which access procedures for financial records were used in accordance with DoDI 5400.15, *Guidance on Obtaining Financial Information from Financial Institutions*, 12 USC § 3414, 15 USC § 1681v, and 50 USC § 3162. AFOSI/JA will provide legal reviews of requests for financial information before submission to financial institutions and will conduct a legal review of financial institution responses to ensure they are within the scope of the request. **(T-0).**

4.1.6. AFOSI shall provide the Director, DIA, copies of all DoD unknown subject leads received from non-DoD agencies, as well as CI investigative reporting in accordance with DoDD 5240.02. Additionally, AFOSI shall, in accordance with DoDI 5240.04, return to DIA all original documentation, results of all inquiries, files, leads, and all other relevant information provided by DIA to the department if a DoD unknown subject investigation is unable to identify the subject. **(T-0).**

4.1.7. Conduct CI investigations and activities in cyberspace to identify, disrupt, neutralize, penetrate, and exploit FIE threats targeting the Air Force and DoD, in accordance with DoDD 5240.02, DoDI S-5240.23, as well as all other applicable laws and instructions. **(T-0).** AFOSI shall also pursue, counter, and deter insiders who abuse their access to AF and DoD information systems in accordance with DoDD 5240.06, *Counterintelligence Functional Services (CIFS)*. **(T-0).**

4.2. Offensive Counterintelligence Operations. AFOSI will operate an Offensive Counterintelligence Operations (OFCO) program consistent with the requirements outlined in DoDI S-5240.09. **(T-0).** As required, AF/A3 supports OFCO and serves as the approval authority for AF- proprietary items, as outlined in DoDI S-5240.09, *Offensive Counterintelligence Operations (OFCO) (U)*.

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 analysis used to identify opportunities to conduct OFCO targeting a FIE, as well as to identify CI investigative opportunities and other activities that have a FIE nexus, in accordance with DoDI 5240.18, *Counterintelligence (CI) Analysis and Production*. **(T-0).**

4.3.1. CI analytical products, unless otherwise exempted by ICD 501, *Discovery and Dissemination Or Retrieval Of Information Within The Intelligence Community*, shall 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 in accordance with applicable Air Force and DoD policies, and only released consistent with Director of National Intelligence policies for disclosure of classified information and controlled unclassified information. **(T-0).**

4.4. AF Counterintelligence Collection & Reporting. AFOSI is the only Air Force agency authorized to collect and report CI information. AFOSI establishment, unit, and nonunit leaders will ensure personnel conducting CI activities adhere to policy and procedures in accordance with AFI 14-104, *Oversight of Intelligence Activities*, DoDD 5240.01, *DoD Intelligence Activities*, DoDM 5240.01, *Procedures Governing The Conduct Of DOD Intelligence Activities*, and DoD 5240.1-R, *The Procedures Governing The Activities Of DOD Intelligence Components That Affect United States Persons*. **(T-0).**

4.4.1. Personnel engaged in CI collection and collection management responsibilities will be adequately trained and research and prepare collection plans and/or operating directives consistent with applicable collection requirements. **(T-0).**

4.4.2. CI collection conducted with foreign counterpart intelligence, CI, security, and law enforcement entities will be deconflicted with other U.S. Government agencies as required. **(T-0).**

4.4.3. All collection and use of the public information environment must be consistent with limitations of AFI 14-104, DoDI S-5240.17, *Counterintelligence Collection Activities (CCA) (U)*, and DoDM 5240.01. **(T-0).** As part of the CI mission, CI elements are authorized to conduct the following activities:

4.4.3.1. **Liaison.** Liaison meetings or events with U.S. and foreign security, law enforcement, 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 Debriefings and Briefings.** Briefings/debriefings and screenings of personnel who may possess information that may be responsive to CI collection requirements.

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

4.4.3.5. **Sources.** In the conduct of its CI mission, AFOSI special agents, upon successful completion of AFOSI's Basic Special Investigators Course, may utilize confidential sources, whether 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 in accordance with DoDD 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*.

4.5. Counterintelligence Support to Research, Development and Acquisition (RDA). AFOSI shall conduct proactive and comprehensive CI activities in support of RDA, in accordance with DoDI O-5240.24. **(T-0).** This includes appointing a CI subject matter expert to provide advice and assistance to the Air Force Acquisition Executive (SAF/AQ), as well as support to OUSD for Acquisition and Sustainment and OUSD for Research and Engineering-managed horizontal technology protection initiatives, and support an Air Force milestone decision authority to determine sufficiency of CI support during reviews of an Air Force RDA program protection plan. Additionally, AFOSI shall conduct CI activities with international partners in support of RDA programs and international transfers of export-controlled defense-related technology; coordinate, synchronize, and deconflict CI activities supporting RDA with Air Force HUMINT elements; and coordinate CI activities at a Cleared Defense Contractor (CDC) with local Defense Security Service (DSS) CI personnel and with the FBI for activities at a Federally-Funded Research & Development Center or University Affiliated Research Center. **(T-0).**

4.5.1. AFOSI investigations into export-controlled technologies that are on the U.S. Munitions List (USML) or dual-use must be coordinated with Immigration and Custom Enforcement – Homeland Security Investigations (ICE-HSI), FBI, and Department of Commerce Bureau of Industry and Security as appropriate in accordance with Executive Order (EO) 13558, 22 USC § 2778, 50 USC§ 2411, and other applicable laws. **(T-0).**

4.5.2. In accordance with DoDM 5220.22, Volume 2, *National Industrial Security Program: Industrial Security Procedures For Government Activities*, when an Air Force installation commander retains security cognizance of a CDC facility handling collateral information on an Air Force installation, AFOSI provides CI support normally provided by DSS. AFOSI will identify a local point of contact for CI matters and include the facility in its local CI threat assessment. **(T-0).** When provided by the installation's industrial security manager, AFOSI will review for CI implications reports of facility security incidents, security vulnerabilities identified during installation commander's security reviews of the facility, and countermeasures proposed in response to those vulnerabilities. **(T-0).**

4.6. Counterintelligence Support to Supply Chain Risk Management (SCRM). AFOSI shall conduct threat analyses of supply chain risk to Air Force requirements in accordance with DoDI O-5240.24 and DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*. **(T-0).** Additionally, recognizing the interrelationship between counterfeiting and SCRM threats, particularly to weapon system effectiveness and efficiency, AFOSI shall conduct proactive and comprehensive criminal investigative and CI activities in support of SCRM, as appropriate, in accordance with DoDI 4140.67, *DOD Counterfeit Prevention Policy*. **(T-0).**

4.7. Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP). AFOSI shall conduct proactive and comprehensive CI activities in support of DCIP, as well as provide comprehensive, timely reporting of potential foreign threat incidents, events, and trends to DCIP authorities and the DoD Components, in accordance with DoDI 5240.19. **(T-0).**

4.8. Counterintelligence Support to the Insider Threat Program. AFOSI shall integrate and validate CI insider threat information requirements into other intelligence collection requirements, as well as develop CI policy, programming, and resource requirements to implement a comprehensive insider threat program, in accordance with DoDI 5240.26, *Countering Espionage International Terrorism, and the Counterintelligence (CI) Insider Threat*, and AFOSI will address security equities across their CI functions in accordance with AFPD 16-14, *Security Enterprise Governance*, and AFI 16-1402, *Insider Threat Program Management*. **(T-0).** Additionally, AFOSI shall 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 (FP). AFOSI shall collect and provide threat data to command officials for the protection of Air Force programs, personnel, and equities in deployed and in-garrison environments in accordance with DoDI 5240.18 and DoDI 5240.22, *Counterintelligence Support to Force Protection*. **(T-0).** Additionally, AFOSI shall provide personnel to support Force Protection Detachments and Joint Terrorism Task Force offices as determined by AFOSI; conduct liaison with Federal, State, and 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 in accordance with DoDD 5240.06. **(T-0).**

4.9.1. AFOSI shall ensure deploying personnel assigned to conduct CI activities will complete specialized training for CI support to FP in accordance with DoDI 5240.22. **(T-0).**

4.9.2. AFOSI will provide annual local threat assessment information to the installation Threat Working Groups (TWG) and/or appropriate threat/terrorism groups, as well as be an active participant within these group for threat data, in accordance with AFI 31-101, *Integrated Base Defense,* and other applicable instructions pertaining to force protection and integrated defense. **(T-2).**

4.10. AFOSI Counterintelligence Support to Combatant Commands (CCMD) and Other DoD Components. AFOSI shall provide CI support to CCMDs and DoD Components as outlined in DoDI 5240.10, to include providing assessments on the FIE threat to each respective CCMD or DoD Component. **(T-0).** Additionally, AFOSI shall assign personnel with CI experience, as required, to serve as Command CI Coordinating Authority (CCICA) to designated CCMDs and Joint Staff for duty. **(T-0).**

4.11. Classifying Counterintelligence Information. CI information within the Air Force is classified in accordance with DoDI C-5240.08, *Counterintelligence (CI) Security Classification Guide (U)*; DoDM 5200.01, Volume 2, *DOD Information Security Program: Marking of Information*; and AFI 16-1404.

4.12. Acquiring Intelligence Information about U.S. Persons. AFOSI may collect information about a U.S. person, as defined in DoDM 5240.01, in its role as a designated CI component only if it is necessary to perform its assigned mission.

4.12.1. The collection must meet the standard of information that can be collected as defined by Procedure 2 of DoDM 5240.01, which are incorporated by reference. **(T-0).** The fact that a collection category exists does not convey authorization to collect. A link is required between the U.S. person information to be collected and the AFOSI CI mission and function.

4.12.1.1. AFOSI may collect U.S. person information by any lawful means, but must exhaust all feasible less intrusive means prior to requesting a more intrusive collection activity, in accordance with DoDM 5240.01. **(T-0).**

4.12.1.2. Information acquired incidentally to an otherwise authorized collection may be retained in accordance with DoDM 5240.01. Specific categories of authorized retention include (a) the information is collected under the provisions of Procedure 2, DoDM 5240.01; (b) the information is necessary to understand or assess foreign intelligence or counterintelligence; (c) the information is foreign intelligence or counterintelligence collected from authorized electronic surveillance; or (d) may indicate involvement in activities that may violate Federal, State, local, or foreign law.

4.12.2. The collection, retention, and dissemination must be in accordance with Procedure 3 and Procedure 4 of DoDM 5240.01, which are incorporated by reference. **(T-0).** Information about U.S. persons may be retained temporarily in accordance with DoDM 5240.01, solely for the purpose of determining whether the information may be permanently retained. If the information may not be retained, it must be appropriately disposed of or destroyed in accordance with DoDM 5240.01 and Air Force instructions. **(T-0).**

4.13. Use of Specialized Techniques in Counterintelligence Investigations and Operations Targeting U.S. Persons. AFOSI is the sole agency within the Air Force authorized to use specialized techniques for counterintelligence purposes, as defined by Procedures 5 through 10, in DoDM 5240.01. This same definition applies if AFOSI requests other agencies to use these techniques in support of the Air Force. For the purposes of this paragraph, AFOSI is a DoD intelligence component as defined in DoDM 5240.01. The authority to conduct specialized techniques resides solely with the Commander, AFOSI. The Commander, AFOSI, may delegate this authority in writing to a headquarters-level senior official who exercises direct oversight authority of counterintelligence investigative operations. Although the authority may be delegated, the Commander, AFOSI, retains authority over AFOSI operations at all times. The following subparagraphs describe the specialized techniques under DoDM 5240.01 available to AFOSI for CI activities. In all cases, AFOSI must comply with the requirements of DoDM 5240.01 and AFI 14-104, *Oversight of Intelligence Activities*. **(T-0).**

4.13.1. The Commander, AFOSI, will provide SAF/GC prior notice, with a reasonable opportunity to respond, before taking action on 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 Commander, AFOSI, may approve an emergency request prior to providing notice to SAF/GC, but in such event will provide SAF/GC a written record of the request and action taken on it within 72 hours of the emergency approval. **(T-1).**

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

4.13.3. Electronic Surveillance, implements the Foreign Intelligence Surveillance Act (50 USC §§ 1801-1812). AFOSI may conduct electronic surveillance pursuant to an order issued by the Foreign Intelligence Surveillance Court or upon Attorney General authorization.

4.13.4. Procedure 6, Concealed Monitoring, applies to concealed monitoring only for counterintelligence purposes conducted by AFOSI within the U.S. or directed against a U.S. person who is outside the U.S. where the subject of such monitoring does not have a reasonable expectation of privacy and in accordance with DoDM 5240.01.

4.13.4.1. Whether a subject has a reasonable expectation of privacy is a determination that depends upon the circumstances of a particular case, and shall be made only after consultation with the legal office responsible for advising the DoD intelligence component concerned (i.e., AFOSI). **(T-0).** Reasonable expectation of privacy is the extent to which a person in particular circumstances has a reasonable belief that his or her activities, property, or communications are private. Concealed monitoring operations must be approved by the Commander, AFOSI, or delegated authority, in accordance with DoDM 5240.01. **(T-0).**

4.13.4.2. Under 18 USC § 2511(2)(i), the electronic communications of a computer trespasser transmitted to, through, or from a protected computer may be intercepted under the following circumstances: (a) the owner/operator of the protected computer authorizes, in writing, the interception of the computer trespasser's communications on the protected computer; (b) the interception is to be conducted pursuant to a lawful CI investigation; (c) there is reason to believe the contents of the computer trespasser's communication is relevant to the investigation; and (d) the interception does not acquire communications other than those transmitted to or from the computer trespasser.

4.13.5. Procedure 7, Physical Search, AFOSI is authorized to conduct nonconsensual physical searches of active duty military personnel or their property within the U.S. when authorized by a military commander empowered to approve physical searches for law enforcement purposes under the provisions of the Manual for Courts Martial, and there is probable cause to believe that the subject is acting as an agent of a foreign power in accordance with DoDM 5240.01.

4.13.6. Procedure 8, Mail Searches and Examination, applies to mail covers and the opening of mail within U.S. postal channels for foreign intelligence and counterintelligence 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. Procedure 8 also applies to the opening of mail to or from other U.S. persons or non-U.S. persons where the mail is not in U.S. postal channels and the mail opening occurs outside the U.S. AFOSI may request that U.S. Postal Service (USPS) authorities examine mail (mail cover) in USPS channels for CI purposes. AFOSI may request mail cover outside USPS channels in accordance with appropriate host nation law and procedures, and any SOFAs.

4.13.7. Procedure 9, Physical Surveillance, 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 only conduct nonconsensual physical surveillance of U.S. persons who 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 law enforcement agencies as appropriate. **(T-0).** AFOSI may conduct nonconsensual physical surveillance of a non-U.S. person in the United States for an authorized CI purpose.

4.13.8. Procedure 10, Undisclosed Participation, applies to AFOSI personnel participating in any organization within the U.S., or a U.S. person organization outside the U.S., on behalf of AFOSI for CI purposes. It also applies when an employee is asked to take action within an organization for AFOSI benefit, whether the employee is already a member 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 counterintelligence functions. It does not apply to participation for purely personal reasons if undertaken at the AFOSI employee's initiative and expense and for the employee's 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 **4.13.9.2** below). Extensions may be granted upon submission of appropriate justification. All requests and approvals will be documented in internal AFOSI records and be disclosed only to competent authorities for official purposes. **(T-0).**

4.13.9.1. Counterintelligence investigations utilizing Procedure 6, Concealed Monitoring, DoDM 5240.01 and the computer trespasser exception may be authorized by the Commander, AFOSI, 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 Commander, AFOSI or delegee may authorize extensions for cyber counterintelligence 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 Procedure 10, Undisclosed Participation, DoDM 5240.01, may be authorized for 12 months.

4.13.10. The Commander, AFOSI, 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 will be maintained in accordance with AFMAN 33-363, *Management of Records*. **(T-1).**

4.13.11. In joint investigations where AFOSI cannot conduct counterintelligence activities under its own authority, the Commander, AFOSI, or delegated authority, may approve AFOSI operating under the authority of another U.S. intelligence agency, such as the FBI. **Note:** The AFOSI ICON Center must be notified if authorized U.S. 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 U.S. federal agency after consultation with AFOSI/JA and if an agency's request containing 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/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. The requests are reviewed by SAF/GC, who ensures approval is obtained from the appropriate authority.

4.14. Other Operational Techniques Targeting U.S. Persons. AFOSI also utilizes other techniques for counterintelligence purposes in accordance with DoDD 5240.01 and DoDM 5240.01. For the purposes of this paragraph, AFOSI is a DoD intelligence component as defined in DoDM 5240.01. The Commander, AFOSI, 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 counterintelligence operations conducted by AFOSI. All specialized techniques must be legally reviewed prior to operation initiation. **(T-0).**

4.15. Interceptions of Wire, Oral, or Electronic Communications. The Commander, AFOSI, or delegated authority, must approve the consensual acquisition of nonpublic wire, oral or electronic communications where at least one party to the communication consents to such interception **(T-0).** The AFOSI commander's authorities encompass all interceptions within the U.S. and all interceptions of U.S. person targets outside of the U.S. In emergency situations only, the activity may be approved verbally after consultation with AFOSI/JA. A written approval and legal review must be conducted to document the decision. **(T-1).** See AFI 71-101 Volume 1, for guidance on consensual interceptions for law enforcement purposes.

4.15.1. Nonconsensual interceptions of nonpublic wire, oral, or electronic communications will be conducted in accordance with Procedure 5, Electronic Surveillance, DoDM 5240.01, and this instruction. **(T-0).** The request will be reviewed by SAF/GC who will ensure approval is obtained from the appropriate authority. **(T-0).**

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

4.16. Operations Targeting Non-U.S. Persons. AFOSI may collect information about Non-U.S. persons in its role as a designated counterintelligence component only if it is necessary to perform its assigned mission.

4.17. Operations Targeting Non-U.S. Persons within the U.S. AFOSI may collect information about non-U.S. persons within AFOSI's jurisdiction or in conjunction with partner agencies that hold jurisdiction. All specialized or other techniques targeting non-U.S. persons will be reviewed by AFOSI/JA and approved by the Commander, AFOSI, or delegated authority. **(T-1).** Within the U.S., when the individual has a reasonable expectation of privacy and under circumstances where a warrant would be required for law enforcement purposes, concealed monitoring is treated and processed as electronic surveillance. Monitoring is considered within the U.S. if the monitoring device, or the monitored target, is located within the U.S.

4.18. Operations Targeting Non-U.S. Persons outside the U.S. All specialized or other techniques targeting non-U.S. persons will be reviewed by AFOSI/JA and approved by the Commander, AFOSI, or delegated authority. **(T-1).**

4.18.1. Status of Forces Agreement (SOFA). The use of specialized or other techniques in CI activities targeting non-U.S. persons outside the U.S. may be subject to limitations or requirements imposed by the SOFA. A legal review of the technique should be obtained prior to approval.

4.18.2. Coordinate with the CIA when conducting CI activities in foreign nations in accordance with 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.*

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

4.19. Using Emergency and Extraordinary Expense Funds (E-Funds). Subject to the availability of appropriations, 10 USC § 127 provides the SecAF authority for any emergency or extraordinary expenses that cannot be anticipated or classified. In accordance with AFPD 71-1 and AFI 71-101, Volume 1, AFOSI uses E-Funds for any authorized requirement that contributes to counterintelligence and/or investigative missions or aids in acquiring counterintelligence or criminal investigative information.

SAMI D. SAID,
Lieutenant General, USAF
The Inspector General

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

10 USC §§ 801-940, *Uniform Code of Military Justice (UCMJ)*

10 USC § 127, *Emergency and Extraordinary Expenses*

12 USC § 3414, *Special Procedures*

15 USC § 1681v, *Disclosures to governmental agencies for counterterrorism purposes*

18 USC § 2511, *Interception and disclosure of wire, oral, or electronic communications prohibited*

18 USC § 2831, *Treason*

28 USC § 533, *Investigative and other officials; appointment*

50 USC §§ 1801-1812, *Electronic Surveillance*

50 USC § 3162, *Requests by authorized investigative agencies*

50 USC § 3381, *Coordination of counterintelligence activities*

AFI 14-104, *Oversight of Intelligence Activities,* 5 November 2014

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

AFI 16-1402, *Insider Threat Program Management*, 5 August 2014

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

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

AFI 71-101, Volume 1, *Criminal Investigations Program,* 8 October 2015

AF Manual 33-363, *Management of Records,* 1 March 2008

AFPD 16-14, *Security Enterprise Governance*, 24 July 2014

AFPD 71-1, *Criminal Investigations and CI*, 13 November 2015

DoD Directive 3020.40, *Mission Assurance,* 29 November 2016

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

DoD Directive 5148.13, *Intelligence Oversight*, 26 April 2017

DoD Directive 5240.01, *DoD Intelligence Activities,* 27 August 2007

DoD Directive 5240.02, *Counterintelligence,* 17 March 2015

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

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

DoD Instruction S-5105.63, *Implementation of DoD Cover and Cover Support Activities,* 20 June 2013.

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

DoD Instruction 5240.04, *Counterintelligence (CI) Investigations,* 1 April 2016

DoD Instruction 5240.10, *Counterintelligence (CI) in the Combatant Commands and Other DoD Components,* 5 October 2011

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

DoD Instruction 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program,* 31 January 2014

DoD Instruction 5240.22, *Counterintelligence Support to Force Protection,* 24 September 2009

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

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

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

DoD Instruction S-5240.09, *Offensive Counterintelligence Operations (U),* 2 February 2015

DoD Instruction S-5240.17, *DoD Counterintelligence Collection Activities,* 14 March 2014

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

DoD Manual 5200.01 Volume 2, *DoD Information Security Program: Marking of Classified Information,* 24 February 2012

DoD Manual 5200.01 Volume 3, *DoD Information Security Program: Protection of Classified Information,* 24 February 2012

DoD Manual 5220.22 Volume 2, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* 1 August 2018

DoD Regulation 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,* 7 December 1982

Executive Order 12333, *U.S. Intelligence Activities,* 4 December 1981

Executive Order 13526, *Classified National Security Information,* 29 December 2009

Intelligence Community Directive 304, *Human Intelligence,* 9 July 2009

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

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

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

Manual for Courts Martial United States, 2012 Edition

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

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFOSI ICON—AFOSI Investigations, Collections, Operations Nexus

AFPD—Air Force Policy Directive

CCDR—Combatant Commander

CCIA—Command CI Coordinating Authority

CCMD—Combatant Command

CDC—Cleared Defense Contractor

CI—Counterintelligence

CIA—Central Intelligence Agency

DC3—DoD Cyber Crime Center

DCIP—Defense Critical Infrastructure Program

D/MM—Digital Multi-Media Forensics

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DOMEX—Document and Media Exploitation

DSS—Defense Security Service

E—**Funds**—Emergency and Extraordinary Expense Funds

EO—Executive Order

FBI—Federal Bureau of Investigation

FIE—Foreign Intelligence Entity

HUMINT—Human Intelligence

HSI—Homeland Security Investigations

ICD—Intelligence Community Directive

ICS—Immigration and Custom Enforcement

IRR—Intelligence Information Report

MDCO—Military Department Counterintelligence Organization

OFCO—Offensive Counterintelligence Operation

OPCON—Operational Control

OPR—Office of Primary Responsibility

RDA—Research, Development and Acquisition

RDS—Air Force Records Disposition Schedule

SCI—Sensitive Compartmented Information

SCRM—Supply Chain Risk Management

SecAF—Secretary of the Air Force

SOFA—Status of Forces Agreement

TWG—Threat Working Group

UCMJ—Uniform Code of Military Justice

USB—Universal Serial Bus

USC—United States Code

USML—U.S. Munitions List

USPS—United States Postal Service

Terms

Anomalies—Foreign power activity or information suggesting foreign knowledge of U.S. national security information, processes or capabilities.

Classified National Security Information—Information that has been determined pursuant to Executive Order 13526 or any predecessor Executive Order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in document form.

Contact—Any form of meeting, association, or communication, in person, by radio, telephone, letter or other means, regardless of who started the contact or whether 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 Government-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.

CI 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.

CI Threat Assessment—A comprehensive analysis or study of a relevant CI topic, event, situation, issue, or development. CI threat assessments require exhaustive research and the production timeline can range from days to months.

Counterintelligence Collections—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 Investigations—Formal investigative activities undertaken to determine whether 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 should take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

Digital Multi-Media (D/MM) Forensics—In its strictest connotation, D/MM forensics is the application of computer science and investigative procedures involving the examination of digital media that may contain evidence to be used in court; following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony. Beyond traditional legal purposes, the same techniques, scientific rigor, and procedural precision are used to support a wide-range of military needs for discovery and recovery of data stored using digital media.

E-Funds—Emergency and Extraordinary Expense Funds used to further the counterintelligence and investigative missions of the Air Force. 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 U.S. is subject to the definition in the Foreign Intelligence Surveillance Act of 1978).

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

Foreign Diplomatic Establishment—Any embassy, consulate, or interest section representing a foreign country.

Foreign Intelligence Entity (FIE)—Any known or suspected foreign organization, person, or group (public, private, or governmental) 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 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 U.S. or its possessions and trust territories; and any person who is not a citizen or national of the U.S..

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

Intelligence Information Report (IIR)—The IIR is the primary vehicle to provide human intelligence information to the consumer. It uses a message format structure that supports automated data entry into Intelligence Community databases.

Military Department CI Organization (MDCO) and DoD CI Agency—The military department CI agencies include Army Counterintelligence, the Naval Criminal Investigative Service and the Air Force Office of Special Investigations. 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 U.S.

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.

Spying—During wartime, any person who is found lurking as a spy or acting as a spy in or about any place, vessel or aircraft, within the control or jurisdiction of any of the Armed Forces or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the U.S., or elsewhere.

Subversion—An act or acts inciting military or civilian personnel of the Department of Defense 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 U.S..

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 U.S., levies war against them or adheres to their enemies, giving them aid and comfort within the U.S. or elsewhere, is guilty of treason (see 18 USC § 2831)

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