

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

AIR FORCE INSTRUCTION 71-101 VOLUME 4

8 NOVEMBER 2011

Special Investigations

COUNTERINTELLIGENCE



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/IGX

Certified by: SAF/IGX
(Col James L. Hudson)

Supersedes: AFI71-101V4, 1 August 2000

Pages: 22

This volume implements AAFP 71-1, *Criminal Investigations and Counterintelligence*, and provides guidance for conducting counterintelligence activities. It further implements DoD 5240.1-R - *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, DoD Instruction 3305.11, *DoD Counterintelligence (CI) Training*, DoD Instruction 5240.04, *Counterintelligence (CI) Investigations*, DoD Instruction 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense Agencies*, DoD Instruction S-5240.15, *Force Protection Response Group (FPRG) (U)*, DoD Instruction S-5240.17, *Counterintelligence Collection (U)*, DoD Instruction 5240.18, *Counterintelligence Analysis and Production*, DoD Instruction 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program*, DoD Instruction O-5240.21, *Counterintelligence (CI) Inquires (U)*, DoD Instruction 5240.22, *Counterintelligence Support to Force Protection*, DoD Instruction S-5240.23, *Counterintelligence (CI) Activities in Cyberspace (U)*, DoD Instruction C-5240.08, *Counterintelligence Security Classification Guide (U)*, DTM 08-11, *Intelligence Oversight Policy Guidance*, and DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*. This publication applies to Air Force Reserve Command (AFRC) Units, the Air National Guard (ANG), and the Civil Air Patrol (CAP) performing an Air Force assigned mission. Failure to observe the prohibitions and mandatory provisions of this instruction in paragraph 3.1 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 paragraph 3.1 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. 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 Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through appropriate chain of command. This volume authorizes the collection and maintenance of information protected by the Privacy Act of 1974. The authority to collect and maintain this information is in Title 10, United States Code (U.S.C.), Sections 801-940. 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 Air Force Records Disposition Schedule (RDS) located at: <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>.

SUMMARY OF CHANGES

This instruction has been substantially revised. Significant changes include guidance for responsibilities, CI awareness and briefing program, critical program information, personnel with access to SCI and SAP, specialized techniques targeting U.S. and non-U.S. persons, AF CI collections and reporting, CI analysis and production, CI support to force protection, the use of emergency and extraordinary expense funds (E-Funds), digital and multimedia forensics, and CI investigations. The following new/updated DoD issuances have been incorporated: DoD Directive 5240.01, *DoD Intelligence Activities*, DoD Directive O-5240.02, *Counterintelligence (U)*, DoD Directive 5505.13E, *DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, DoD Instruction 3305.11, *DoD Counterintelligence (CI) Training*, DoD Instruction 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, DoD Instruction 5240.04, *Counterintelligence (CI) Investigations*, DoD Instruction 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense Agencies*, DoD Instruction S-5240.15, *Force Protection Response Group (FPRG) (U)*, DoD Instruction S-5240.17, *Counterintelligence Collection (U)*, DoD Instruction 5240.18, *Counterintelligence Analysis and Production*, DoD Instruction 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program*, DoD Instruction O-5240.21, *Counterintelligence (CI) Inquires (U)*, DoD Instruction 5240.22, *Counterintelligence Support to Force Protection*, DoD Instruction S-5240.23, *Counterintelligence (CI) Activities in Cyberspace (U)*, DoD Instruction 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs*, DTM 08-11, *Intelligence Oversight Policy Guidance*, and DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*.

Chapter 1—RESPONSIBILITIES	4
1.1. The Air Force Office of Special Investigations (AFOSI).	4
1.2. Investigations, Collections and Operations Nexus (ICON).	4
1.3. National Cyber Investigative Joint Task Force (NCIJTF).	4
Chapter 2—COUNTERINTELLIGENCE AWARENESS AND BRIEFING PROGRAM	5
2.1. Air Force Awareness and Briefing Programs.	5
2.2. Briefings.	5
2.3. CI Briefers.	5

2.4. Critical Program Information. 6

2.5. Personnel with Access to Sensitive Compartmented Information (SCI) and Special Access Programs (SAP). 6

Chapter 3—REPORTABLE INFORMATION AND CONTACTS 7

3.1. Reportable Information and Contacts. 7

3.2. Responsibility to Report Incidents. 8

3.3. Sanctions. 8

Chapter 4—COUNTERINTELLIGENCE PROGRAM 9

4.1. Counterintelligence Investigations. 9

4.2. Counterintelligence Analysis and Production. 9

4.3. AF Counterintelligence Collections & Reporting. 10

4.4. Counterintelligence Support to Force Protection. 10

4.5. Digital and Multimedia Forensics. 11

4.6. Classifying Counterintelligence Information. 11

4.7. Acquiring Intelligence Information about US Persons. 11

4.8. Use of Specialized Techniques in Counterintelligence Investigations and Operations Targeting U. 12

4.9. Other Operational Techniques targeting U. 14

4.10. Interceptions of Wire, Oral, or Electronic Communications. 15

4.11. Operations targeting Non-U. 15

4.12. Operations targeting Non-U. 15

4.13. Operations targeting Non-US persons outside the United States. 15

4.14. Sources. 16

4.15. Using Emergency and Extraordinary Expense Funds (E-Funds). 16

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 17

Chapter 1

RESPONSIBILITIES

1.1. The Air Force Office of Special Investigations (AFOSI). The 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.

1.1.1. AFOSI's CI authorities primarily derive from Executive Order 12333, § 1.7(f)(1-4).

1.1.2. In the United States, AFOSI coordinates these activities with the Federal Bureau of Investigation (FBI) when appropriate.

1.1.3. Outside the United States, 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 will notify and provide briefings to appropriate command officials on CI investigations that require determinations on continuing access to classified information and other personnel security actions.

1.2. Investigations, Collections and Operations Nexus (ICON). ICON is the Air Force's sole investigative and counterintelligence (CI) threat reporting integration mechanism. The ICON provides timely investigative data and threat reporting data to the Commander, AFOSI, and other senior AF and DoD leaders. The ICON is organized by regional and specialty desks, which receive and synchronize information received from AFOSI field units and other U.S. Government agencies. The ICON manages AFOSI's Global Watch, which receives up-channel reporting from AFOSI field units; the Global Watch also coordinates with other Air Force, DoD, and U.S. Government Watches. ICON will coordinate, as necessary, investigative and CI activities with AF human intelligence (HUMINT) activities.

1.3. National Cyber Investigative Joint Task Force (NCIJTF). The FBI leads the NCIJTF as the multiagency national focal point for coordinating cyber investigations across all national security and criminal law enforcement programs. The NCIJTF is composed of the Information Operations Group (IOG), which prioritizes, coordinates, facilitates, and fosters investigative and operational activities related to cyber threat investigations and operations. It also has the Analytical Group (AG), which leads an "analytical collaborative" to synthesize intrusion event reporting as a basis to drive proactive counterintelligence cyber operations and investigations within the purview of the NCIJTF. AFOSI coordinates and deconflicts cyber operations with NCIJTF at the national level while providing the task force with cyber data and information. The Department of Defense Cyber Crimes Center (DC3) retains operational control over the NCIJTF-AG.

Chapter 2

COUNTERINTELLIGENCE AWARENESS AND BRIEFING PROGRAM

2.1. Air Force Awareness and Briefing Programs. Air Force awareness and briefing programs shall promote threat and reporting awareness responsibility, enable Air Force personnel to identify CI threats and the reporting of suspicious situations and incidents to appropriate authorities.

2.2. Briefings. Air Force commanders will ensure their personnel are briefed on CI threats related to foreign intelligence entities (FIE), international terrorists, cyberspace, and unauthorized disclosures. This awareness effort should emphasize individual reporting responsibilities. These briefings should include a detailed discussion about insider threats, the crimes of espionage and treason, and standards discussed in this instruction.

2.2.1. Air Force commanders should 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. Include threats in cyberspace for all CI awareness, briefing, and reporting programs in accordance with DoDI S-5240.23, *Counterintelligence (CI) Activities in Cyberspace (U)*. Examples of indicators of potential threat activity on DoD networks are listed within DoDI S-5240.23.

2.2.3. Military personnel must receive the briefing at or near the time of initial entry. 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. 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 personnel may require more frequent briefings predicated on the nature of their duties.

2.2.7. AFOSI is the installation-level training agency for counterintelligence awareness briefings. If AFOSI does not provide the training, AFOSI must ensure the training provided meets the required level of awareness.

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 should include:

2.3.1. The threat posed by foreign intelligence, foreign government-sponsored commercial enterprises, all pertinent terrorist threats, and international narcotics trafficking organizations.

2.3.2. Information about early detection of espionage, foreign intelligence indicators, and international terrorist activities.

2.3.3. Detailed information regarding the crimes of sabotage, subversion, treason, and espionage.

2.3.4. Relevant and current threats facing the specific installation, mission, functions, activities, and locations the audience is associated with.

2.3.5. The reporting requirements of this instruction as well as those described in DoDD 5240.6.

2.3.5.1. Personnel shall report information pursuant to E.O. 13526, *Classified National Security Information*, and DoDD 5200.2, *DoD Personnel Security Program*, 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.

2.4. Critical Program Information. Acquisition program personnel working with Critical Program Information pursuant to AFD 71-1 and DoDI 5200.39, *Critical Program Information (CPI) Protection within the Department of Defense*, shall notify AFOSI of all projected foreign travel prior to departure. Such personnel will receive foreign intelligence and antiterrorism threat briefings prior to overseas travel. Upon completion of travel, personnel will contact AFOSI to schedule a debriefing.

2.5. Personnel with Access to Sensitive Compartmented Information (SCI) and Special Access Programs (SAP). Pursuant to Director of Central Intelligence Instruction (DCID) 1/20, *Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)* and *Revision 1 Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement*, 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. Personnel with special access should contact their servicing AFOSI-PJ detachment.

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 days of the contact) report the contact or information, either verbally or in writing, to AFOSI. If necessary, the individual can report the information to his/her commander, supervisor, or security officer who must immediately provide the information to their servicing AFOSI detachment. 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, etc., in addition to face-to-face meetings. 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. Individuals are required to report the following:

3.1.1. Personal contact with an individual (regardless of nationality) who suggests that a foreign intelligence or any terrorist organization may have targeted them or others for possible intelligence exploitation.

3.1.2. A request by anyone (regardless of nationality) for illegal or unauthorized access to classified or unclassified controlled information or systems containing such information.

3.1.3. Contact with a known or suspected intelligence officer to include attachés from any country.

3.1.4. Contact for any reason, other than for official duties, with a foreign diplomatic establishment whether in the United States or abroad. **NOTE:** 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.

3.1.5. Activities related to planned, attempted, actual, or suspected espionage, terrorism, unauthorized technology transfer, sabotage, sedition, subversion, spying, treason, or other unlawful intelligence activities targeted against the Department of the Air Force, other U.S. facilities, organizations, or U.S. citizens.

3.1.6. Information indicating military members, civilian employees or DoD contractors have contemplated, attempted, or effected the deliberate compromise or unauthorized release of classified or unclassified controlled information.

3.1.7. Unauthorized intrusion into U.S. automated information systems, networks, or other cyber capabilities, whether classified or unclassified; unauthorized transmissions of classified or unclassified controlled information without regard to medium, destination, or origin.

3.1.8. Unauthorized attempts to bypass automated information systems security devices or functions, unauthorized requests for passwords, or unauthorized installation of modems or other devices into automated information systems (including telephone systems) whether classified or unclassified.

3.1.9. Any additional information as designated by DoDD 5240.6.

3.2. Responsibility to Report Incidents. The following persons are required to report incidents. All other persons associated with Air Force activities but not listed below should be encouraged to report counterintelligence incidents:

3.2.1. Active duty Air Force personnel and Air Force civilian employees.

3.2.2. U.S. Air Force Reserve personnel while in active status and Category B reservists on inactive duty for training (IDT) 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 overseas 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 the overseas employees of the U.S. government for whom the Air Force provides support.

3.3. Sanctions. The reporting requirements articulated in paragraph 3.1 are MANDATORY. Failure to observe the reporting requirements of this instruction in paragraph 3.1 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 paragraph 3.1 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 Air Force in accordance with DoDD O-5240.02, *Counterintelligence*, to include investigations of active and reserve military personnel, DoD civilians, and other DoD affiliated personnel as clarified in DoDI 5240.04, *Counterintelligence (CI) Investigations*.

4.1.1. AFOSI will report to the FBI those incidents meeting the criteria of section 402a(e) of Title 50, U.S.C. and refer CI investigative matters to the FBI according to guidance prescribed in DoDI 5240.04, and section 533 of Title 28, U.S.C.

4.1.2. 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.

4.1.3. AFOSI will evaluate CI inquiry referrals and initiate CI investigations in accordance with DoDI 5240.04 when warranted.

4.1.4. AFOSI will conduct CI activities in cyberspace to identify, disrupt, neutralize, penetrate, and exploit foreign intelligence entity (FIE) threats against the Air Force and DoD, in accordance with applicable DoD instructions, such as DoDI S-5240.23 and law.

4.2. Counterintelligence Analysis and Production. In accordance with AFPD 71-1 and DoDI 5240.18, *Counterintelligence (CI) Analysis and Production*, AFOSI CI elements will produce analytic products to address the threat posed by espionage, international terrorism, subversion, sabotage, assassination, and covert activities. This includes other activities that have an FIE nexus.

4.2.1. The ICON is the Air Force's sole investigative and counterintelligence threat reporting integration mechanism. The ICON provides timely investigative data and threat reporting data to the Commander, AFOSI, and other senior AF and DoD leaders. The ICON is organized by regional and specialty desks, which synchronize information received from AFOSI field units and other U.S. government agencies. It manages AFOSI's Global Watch, which receives up-channel reporting from AFOSI field units. The Global Watch also coordinates with other Air Force, DoD, and U.S. Government Watches. The ICON will coordinate, as necessary, investigative and CI activities with AF human intelligence (HUMINT) activities. Finally, the ICON is a central clearinghouse for data gleaned from its liaison officers assigned to AFOSI's partner agencies in the U.S. Government, such as the FBI, CIA, and National Security Agency.

4.2.2. CI analysis and production elements will produce and disseminate products in response to prioritized production requirements.

4.2.3. Products intended for release to foreign governments will be coordinated in accordance with applicable Air Force and DoD policies, and consistent with Director of National Intelligence (DNI) policies for disclosure of classified information and controlled unclassified information.

4.2.4. CI analytical products shall adhere to standards in a manner appropriate to the length, purpose, classification, and production timeframe of each product consistent with Intelligence Community Directive (ICD) Number 203, *Analytic Standards*, and contain appropriate source references consistent with ICD 206, *Sourcing Requirements For Disseminated Analytic Products*.

4.3. AF Counterintelligence Collections & Reporting. AFOSI is the only Air Force agency authorized to collect and report CI information. Commanders will ensure personnel conducting CI activities adhere to policy and procedures under AFI 14-104, *Oversight of Intelligence Activities* and DoDD 5240.01 and DoD 5240.1-R.

4.3.1. Personnel engaged in CI collection and collection management responsibilities must be adequately trained and will provide for the establishment of collection plans and/or operating directives consistent with existing collection requirements.

4.3.2. CI collections conducted with foreign counterpart intelligence, CI, security, and law enforcement entities will be deconflicted with the Military Department CI organizations and the Defense Counterintelligence and HUMINT Center (DCHC).

4.3.3. At a minimum, collections requirements will be revalidated annually.

4.3.4. All collection and use of the public information environment must be consistent with limitations of AFI 14-104 and DOD 5240.1-R. When conducting CI overt reporting activities to validated CI collection requirements and local needs, CI elements are authorized to:

4.3.4.1. Conduct liaison meetings or events with U.S. and foreign security, law enforcement, CI and intelligence organizations, and non-DoD affiliated personnel to discuss and obtain information responsive to commanders' critical information or intelligence collection requirements.

4.3.4.2. Collect and use open-source media, internet, social networking, and other freely available and open to public information environments for the furtherance of CI collection requirements.

4.3.4.3. Conduct briefings/debriefings and screenings of personnel who may possess information which may be useful in supporting CI collection requirements.

4.4. Counterintelligence Support to Force Protection. AFOSI is responsible for ensuring the Air Force maintains comprehensive, effective, and integrated CI capabilities employing all appropriate CI options to support Force Protection (FP) programs.

4.4.1. Deploying personnel assigned to conduct CI activities will complete specialized training for CI support to FP.

4.4.1.1. CI personnel are expected to comply with requirements defined in DoDI 5240.18 when producing CI assessments to combat terrorism and FP requirements of in-garrison and deployed forces.

4.4.2. AFOSI will conduct liaison with Federal, State, and local agencies and foreign agencies for the collection and appropriate exchange of international terrorist threat information.

4.5. Digital and Multimedia Forensics. Pursuant to DoDD 5505.13E, DC3 functions as the DoD Center of Excellence for digital and multimedia forensics and operates as a law enforcement and counterintelligence support activity pursuant to the authorities vested in the Secretary of Defense by Title 10 of the United States Code, sections 125 and 376. IAW AFPD 71-1 and DoDD 5505.13E, *DoD Executive Agent (EA) for the DC3*, AFOSI will provide DC3, to the maximum extent possible, copies of digital media and logs and investigative and technical data associated with CI cyber intrusion incidents, investigations, and operations. DoD agencies should consider consulting the Executive Director, DC3, on DoD CI cyber investigations involving critical infrastructures and impacting the global information grid (GIG), as well as for digital forensic support.

4.6. Classifying Counterintelligence Information. Except for information subject to the Atomic Energy Act of 1954 (as amended), AFOSI assigns classification markings to counterintelligence information according to the guidelines in AFI 31-401, *Information Security Management* and DoD 5200.1-R, *Information Security Program*, DoDI 5240.8, *Security Classification Guide for Information Concerning the DoD Counterintelligence Program*, and Executive Order 13526. These publications and executive order provide the only basis for application of security classification to counterintelligence information within the DoD and Air Force.

4.7. Acquiring Intelligence Information about US Persons.

4.7.1. The Air Force General Counsel (SAF/GC) is the primary legal counsel for all Air Force intelligence oversight issues. SAF/GC provides advice to intelligence components on questions of legality and propriety, as required.

4.7.1.1. Reporting Questionable Intelligence Activities. In accordance with DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*, or its successor guidance, all AF personnel are required to report questionable intelligence activities and significant or highly sensitive matters involving intelligence activities which may have serious implications for the execution of DoD missions. 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.

4.7.2. Information about a U.S. person, as defined in DoD Directive 5240.1-R, may be collected by AFOSI in its role as a designated CI component only if it is necessary to perform its assigned mission.

4.7.3. The collection must meet the standard of information that can be collected as defined by Procedures 2 of DoD 5240.1-R, which are incorporated by reference. The fact that a collection category exists does not convey authorization to collect. There must be a link between the U.S. person information to be collected and the AFOSI mission and function.

4.7.3.1. 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. See paragraph C2.4.2. of DoD 5240.1-R.

4.7.3.2. Information acquired incidentally to an otherwise authorized collection may be retained if (a) the information is collected under the provisions of Procedure 2, DoD 5240.1-R; (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) the information is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

4.7.4. The collection, retention, and dissemination must be in accordance with Procedure 3 and Procedure 4 of DoD 5240.1-R, which are incorporated by reference.

4.7.4.1. Information about U.S. persons may be retained temporarily, for a period not to exceed 90 days, 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 IAW DoD 5240.1-R, and Air Force regulations.

4.8. 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, as defined by Procedures 5 through 10, in DoD 5240.1-R. This same definition applies if AFOSI requests other agencies to conduct these techniques in support of the Air Force. For the purposes of this paragraph, AFOSI is a DoD intelligence component as defined in DoD 5240.1-R. The authority to conduct specialized techniques resides solely with the Commander, AFOSI. The Commander, AFOSI, may delegate this authority in writing under specified circumstances to a headquarters-level senior official who exercises direct oversight authority of criminal 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 DOD 5240.1-R available to AFOSI for CI activities. In all cases, AFOSI must comply with the specific requirements of DOD 5240.1-R and AFI 14-104 which implements it.

4.8.1. 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. AFOSI/CC 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.

4.8.2. 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*, will apply.

4.8.3. Procedure 5, Electronic Surveillance, implements the Foreign Intelligence Surveillance Act (FISA) (Title 50, U.S.C. §1801). AFOSI may conduct electronic surveillance against persons within the United States pursuant to an order issued by the Foreign Intelligence Surveillance Court (FISC) or upon Attorney General authorization.

4.8.4. Procedure 6, Concealed Monitoring, applies to targeting by electronic, optical, or mechanical devices of a particular person or group of persons, without their consent, in a surreptitious and continuous manner. This technique is conducted for foreign intelligence and CI purposes. Concealed monitoring applies both within the United States or whenever targeting U.S. persons outside the United States. The subject must not have a reasonable expectation of privacy and under circumstances where no warrant would be required if the

monitoring was undertaken for law enforcement purposes. Concealed monitoring operations must be approved by the Commander, AFOSI, in accordance with DoD 5240.1-R.

4.8.4.1. Under 18 U.S.C. §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 will be relevant to the investigation; and (d) the interception does not acquire communications other than those transmitted to or from the computer trespasser.

4.8.4.2. GPS trackers, beacons (beepers), and transponders are considered concealed monitoring whenever affixed in a public place, such as on a vehicle in a public parking lot; no warrant would be required for law enforcement purposes; and the monitoring stops when the target acquires an expectation of privacy.

4.8.5. Under Procedure 7, Physical Search, AFOSI is authorized to conduct nonconsensual physical searches of active duty military personnel or their property within the United States 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.

4.8.6. Procedure 8, Mail Searches and Examination, applies to mail covers and the opening of mail within United States postal channels for foreign intelligence and counterintelligence purposes. It also applies to the opening of mail to or from U.S. persons where the mail is not in U.S. postal channels and the mail opening occurs outside the United States. AFOSI may request that United States 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 Status of Forces Agreements (SOFAs.)

4.8.7. 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 a training exercise in which the surveillance subjects are exercise participants. AFOSI may only conduct nonconsensual physical surveillance of U.S. persons who are military personnel on active duty status; present or former intelligence component employees; present or former intelligence component contractors and their present or former employees; applicants for such employment or contracting; 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 conducted outside a DoD installation must be coordinated with the FBI and other law enforcement agencies as appropriate.

4.8.8. Procedure 10, Undisclosed Participation, applies to AFOSI personnel participating in any organization within the United States, or a U.S. person organization outside the United States, 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. It will not apply to cooperating sources who volunteer information obtained as a result of their participation in an organization.

4.8.9. Unless otherwise proscribed by law, specialized techniques may be authorized by the appropriate approving authority for a period of 180 days (with the exception of cyber operations which are addressed in paragraph 4.8.9.1. below). 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.

4.8.9.1. Cyber counterintelligence investigations utilizing Procedure 6, Concealed Monitoring, DoD 5240.1-R and the computer trespasser exception may be authorized by the Commander, AFOSI for up to 365 days. 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. The Commander, AFOSI, may authorize extensions for cyber counterintelligence investigations with appropriate justification annually. All active monitoring sites must be included in the overall operations plan for AFOSI Commander extensions.

4.8.10. The Commander, AFOSI, will publish internal instructions directing the conduct and approval process for all specialized and operational techniques. AFOSI will document the approvals, the specific techniques utilized, the identity of persons monitored, and the disposition of the products of such techniques in internal documentation. The Commander will ensure a copy of the approval and legal review for activities under Procedure 10 are provided to SAF/GC as soon as possible.

4.8.11. In joint investigations, AFOSI may utilize specialized techniques under the approval authority of another authorized U.S. federal agency (normally FBI) after consultation with AFOSI/JA.

4.8.12. 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.

4.8.13. Procedures requiring approval outside AFOSI will be staffed through HQ AFOSI to SAF/GC. The request will be reviewed by SAF/GC who will ensure approval is obtained from the appropriate authority.

4.9. Other Operational Techniques targeting U. S. Persons. AFOSI also utilizes other techniques for counterintelligence purposes in accordance with DoD 5240.1-R. For the purposes of this paragraph, AFOSI is a DoD intelligence component as defined in DoD 5240.1-R. The Commander, AFOSI, or delegated authority, must approve the following operational techniques prior to initiation:

4.9.1. Consensual Acquisition of Stored Communications for computer hard drives and network records & information.

4.9.2. Trash cover.

4.9.3. National Security Letters.

4.9.4. DoD Subpoena.

4.9.5. AFOSI/JA is the 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.

4.10. Interceptions of Wire, Oral, or Electronic Communications. The Commander, AFOSI must approve the consensual acquisition of nonpublic wire, oral or electronic communications where at least one party to the communication consents to such interception. AFOSI Commander authority encompasses 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. The Commander, AFOSI, will ensure a copy of this approval and legal review is provided to SAF/GC as soon as possible.

4.10.1. Nonconsensual interceptions of nonpublic wire, oral, or electronic communications will be conducted in accordance with Procedure 5, Electronic Surveillance, DoD 5240.1-R, and this instruction. The request will be reviewed by SAF/GC who will ensure approval is obtained from the appropriate authority.

4.10.2. The Commander, AFOSI, or delegated authority, must approve all interceptions of Wire, Oral, or Electronic Communications targeting Non-U.S. persons overseas. All U.S. persons involved must be aware of the operation and consent to the monitoring.

4.11. 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.

4.12. Operations targeting Non-U. S. persons within the U.S. AFOSI may collect information about Non-U.S. persons within AFOSI 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.

4.12.1. Within the United States, when the individual has a reasonable expectation of privacy and under circumstances where a warrant would be required for law enforcement purposes, concealed monitoring will be treated and processed as electronic surveillance. Monitoring is considered within the United States if the monitoring device, or the monitored target, is located within the United States.

4.13. Operations targeting Non-US persons outside the United States. 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.

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

4.13.2. When conducting CI activities overseas, coordinate with the CIA in accordance with the Director Central Intelligence Annex 3 to the Memorandum of Agreement between the Central Intelligence Agency (previously DCID 5/1) and the Department of Defense.

4.13.3. In the deployed area of responsibility, the Combined Air Operations Center SJA or deployed SJA will review the application of each technique to ensure compliance with Intelligence Oversight policy and/or the Law of Armed Conflict (LOAC) and approve their use. This approval must be provided to AFOSI/JA.

4.14. Sources. CI sources will be selected based on suitability, placement, and access to required information, and need not be DoD-affiliated.

4.14.1. CI sources may be U.S. or foreign nationals and may be trained, tasked, recruited, and controlled.

4.15. Using Emergency and Extraordinary Expense Funds (E-Funds). Subject to the availability of appropriations, Title 10, U.S.C., Part I, Chapter 3, §127 provides the SECAF authority for any emergency or extraordinary expenses which cannot be anticipated or classified. AFOSI uses E-Funds for any authorized requirement that contributes to counterintelligence and investigative missions or aids in acquiring counterintelligence or criminal investigative information.

4.15.1. Congress annually specifies the amount of appropriated funds the SECAF can use as E-Funds. SECAF has delegated authority for expenditure of E-Funds to the Administrative Assistant to SECAF (SAF/AA). SAF/AA sets the annual E-Fund expenditure limitation and reports E-Funds expenditures to the Office of the Secretary of Defense.

4.15.2. SAF/AA annually allocates a specific portion of the E-Fund expenditure authority to the Inspector General (SAF/IG). SAF/IG oversees the Air Force E-Funds for counterintelligence and criminal investigative programs and delegates to the Commander, AFOSI, the authority to approve counterintelligence and investigative expenditures.

4.15.3. In accordance with AFD 71-1, AFI 71-101, Volume 1, *Criminal Investigations Program*, and AFOSII 71-111, *Use of Emergency and Extraordinary Expense Funds (E-Funds)*, Commander, AFOSI, manages and implements the E-Funds for the CI and criminal investigative programs and ensures that expenditures are proper. The Commander, AFOSI, or a designee, must approve the use of E-Funds for the extension of modest liaison event courtesies to representatives of foreign law enforcement and intelligence agencies and key representatives of U.S. Federal, state, county, or local law enforcement and intelligence agencies.

4.15.4. Air Force Audit Agency (AFAA) audits the E-Funds program annually to ensure compliance with this Instruction and internal AFOSI Instructions.

4.15.5. The E-Funds Custodian at each field unit is responsible for the working fund. Cash on hand must be stored in a General Services Administration (GSA)-approved container with a three-position combination lock.

MARC E. ROGERS, Lieutenant General, USAF
The Inspector General

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Executive Order 12333, *United States Intelligence Activities*, December 4, 1981

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

AF Instruction 14-104, *Conduct of Intelligence Activities of DoD Intelligence Components that Affect United States Persons*, April 16, 2007

AFI 31-401, *Information Security Management*, November 1, 2005

AF Instruction 33-332, *Privacy Act Program*, May 16, 2011

AF Instruction 71-101, Volume 1, *Criminal Investigations*, April 8, 2011

AF Policy Directive (AFPD) 71-1, *Criminal Investigations and Counterintelligence*, 6 January 2010 – Incorporating Change 1, October 26, 2010

DoD 5200.1-R, *Information Security Program*, January 14, 1997

DoD Directive 5200.2, *DoD Personnel Security Program*, April 9, 1999

DoD Directive 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, December 1982

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

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

DoD Directive O-5240.02, *Counterintelligence*, December 20, 2007 - Incorporating Change 1, December 30, 2010

DoD Instruction 3305.11, *DoD Counterintelligence (CI) Training*, March 19, 2007 – Incorporating Change 1, January 28, 2011

DoD Instruction 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 16, 2008 – Incorporating Change 1, December 28, 2010

DoD Instruction 5240.04, *Counterintelligence (CI) Investigations*, February 2, 2009

DoD Instruction 5240.10, *Counterintelligence Support to the Combatant Commands and the Defense*, May 14, 2004

DoD Instruction S-5240.15, *Force Protection Response Group (FPRG) (U)*, October 20, 2010

DoD Instruction S-5240.17, *Counterintelligence Collection (U)*, January 12, 2009

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

DoD Instruction 5240.19, *Counterintelligence Support to the Defense Critical Infrastructure Program*, August 27, 2007 – Incorporating Change 1, December 28, 2010

DoD Instruction O-5240.21, *Counterintelligence (CI) Inquires (U)*, May 14, 2009 – Incorporating Change 1, November 19, 2010

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

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

DoD Instruction 5240.6, *Counterintelligence (CI) Awareness, Briefing, and Reporting Programs*, August 7, 2004

DoD Instruction C-5240.8, *Counterintelligence Security Classification Guide (U)*, December 7, 2005

Directive Type Memorandum (DTM) 08-011, *Intelligence Oversight Policy Guidance*, March 26, 2008 – Incorporating Change 1, September 8, 2010

DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*, June 17, 2009 – Incorporating Change 1, September 10, 2010

Director of Central Intelligence Instruction (DCID) 1/20, *Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI)*, December 29, 1991

DCID 5/1, *Espionage and Counterintelligence Abroad*, December 19, 1984

Director Central Intelligence Annex 3 to the Memorandum of Agreement between the Central Intelligence Agency and the Department of Defense

Intelligence Community Directive (ICD) Number 203, *Analytic Standards*, June 21, 2007

ICD Number 206, *Sourcing Requirements For Disseminated Analytic Products*, October 17, 2007

Manual for Courts Martial

Public Law 95-511, *Foreign Intelligence Surveillance Act of 1978*

Revision 1 to the DoD Overprint to the National Industrial Security Program Operating Manual Supplement, April 1, 2004

Title 10, U.S.C. §801-940

Title 10, U.S.C. Part 1, Chapter 3, §127

Title 18, U.S.C. §2511(2)(i)

Title 28, U.S.C. §533

Title 50, U.S.C. §402, 1805

Uniform Code of Military Justice

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, September 22, 2009

AF Form 3985, *Interview Record*, July 9, 2008

AF Form 3986, *Case File Documents Outer Envelope*, September 1, 1996

AF Form 3987, *Case File Documents Inner Envelope*, September 1, 1996

Terms

Anomalies— Foreign power activity or knowledge 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.

Collections Management— The process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and re-tasking, as required.

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.

Counterintelligence (CI)— Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

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

CI awareness products— Analysis of a CI topic, event, situation, issue, or development. These products differ from an assessment in that they are often time sensitive, are published as needed or annually, and normally do not require extensive research to produce. Products of this nature ensure a consistent flow of appropriately classified or categorized threat information is available to the community to increase awareness and action as appropriate.

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 Cyber Investigation— A counterintelligence investigation targeting threats to DoD information systems by an insider or by an external entity. These investigations may involve unauthorized access/intrusions, exceeding authorized network privileges, denial of service attacks, or the introduction of malicious code.

Counterintelligence Investigations— Conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions, provide a basis for CI operations, or validate the suitability of personnel for access to classified information. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow Defense Agency and Military Department directives governing reporting contacts with foreign citizens and out-of-

channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve the security posture of threatened interests.

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

Defense 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 Forensics— In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - 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 now support the range of military operations and courses of action (e.g., computer network operations as well as CI objectives).

E-Funds— Emergency and Extraordinary (E&E) 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 United States 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 United States 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 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 United States, or its possessions and trust territories; and any person who is not a citizen or national of the United States.

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

Military Department CI Agency 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 United States.

Organic CI— Assigned and trained personnel having CI missions, functions, and responsibilities in a designated organizational CI element in support of the DoD Component.

Portico— A program managed by the DCHC to provide automation support, through web-enabled software hosted on a robust infrastructure, to the DoD CI Community. Portico enables CI enterprise business processes, facilitates information sharing, and coordination across DoD Services and Agencies. It provides management tools for each CI functional area, as well as supporting tools and services for managing the CI process in the functional areas of Collection; Counterintelligence Investigations; Analysis and Production; Operations; and CI Functional Services.

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 United States, 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 United States.

Technology Transfer— The export of controlled technical information, data, and/or material to a foreign interest pursuant to 50 App. U.S.C. §2401 and 22 U.S.C §2751.

Terrorism— The calculated use of violence or threat of violence to inculcate 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 United States, levies war against them or adheres to their enemies, giving them aid and comfort with the United States or elsewhere, is guilty of treason (see Title 18, U.S.C. §2831)

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

Unclassified Controlled Information— Information other than classified information that requires application of controls and protective measures because the information is exempt from release under the Freedom of Information Act. Examples include “For Official Use Only” information, “Sensitive but Unclassified” (Formerly “Limited Official Use”) information, “DEA Sensitive Information,” “DoD Unclassified Controlled Nuclear Information,” or “Sensitive Information” as defined in the Computer Security Act of 1987, and information contained in Technical Documents.

Unofficial Contact— Contact not specifically required in accordance with job responsibilities.