Headquarters
Department of the Army
Washington, DC
13 June 2025

***Army Regulation 381–12**

Effective 13 July 2025

Military Intelligence

Counterintelligence Awareness and Reporting

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision. The portions affected by this major revision are listed in the summary of change.

Authorities. This regulation implements 10 USC 7013, Executive Order 12333, DoDD 5240.01, DoDD 5240.02, and DoDD 5240.06.

Applicability. This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific requirements.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix D).

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to usarmy.pentagon.hqda-dcs-g-2.list.dami-cdc@army.mil.

Distribution. This regulation is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

*This regulation supersedes AR 381-12, dated 1 June 2016.

Summary of Change

AR 381–12
Counterintelligence Awareness and Reporting

This major revision, dated 13 June 2025—

- Changes the title of this regulation from Threat Awareness and Reporting Program to Counterintelligence Awareness and Reporting (cover).

- Updates responsibilities of Deputy Chief of Staff, G–2; Commanding General, U.S. Army Intelligence and Security Command, Commanding General, U.S. Army Forces Command, Commanding General, U.S. Army Training and Doctrine Command, Chief, Army Reserve, all Army commanders/directors, and contracting officers; and transfers responsibilities from the Army Counterintelligence Coordinating Authority to the Commanding General, U.S. Army Counterintelligence Command (paras 2–1, 2–1*d*, 2–1*e*, 2–3, 2–5, 2–6, 2–7, 2–8).

- Adds requirement to designate "counterintelligence-experienced persons" to U.S. Army Counterintelligence Command (para 2–1*e*(8)).

- Adds requirement to develop and maintain a public domain internet U.S. Army Counterintelligence Command page (para 2–1*e*(9)).

- Adds requirement to appoint a U.S. Army Counterintelligence eGuardian Program Manager and assigns responsibilities (para 2–1*e*(10)).

- Adds requirement to appoint an Army Counterintelligence Awareness and Reporting Program Manager who will serve as the representative to the Defense Intelligence Agency Counterintelligence Awareness and Reporting Council (para 2–1*e*(11)).

- Adds requirement for budgeting and sustainment of Counterintelligence Awareness and Reporting marketing and training materials (paras 2–1*e*(12) and 2–1*e*(13)).

- Adds requirement for completion of an annual Counterintelligence Awareness and Reporting program report to Army G–2X (para 2–1*e*(14)).

- Adds requirement for the development of a Counterintelligence Awareness and Reporting engagement strategy to U.S. Army Counterintelligence Command (para 2–1*e*(15)).

- Adds requirements for Deputy Chief of Staff, G–3/5/7 (para 2–2).

- Updates Counterintelligence Awareness and Reporting training requirement and removes train-the-trainer certification and standard briefing tool requirements (chap 3).

- Updates Counterintelligence Awareness and Reporting training policy in accordance with DoDD 5240.06 (para 3–1).

- Adds requirement for Department of the Army personnel to complete Counterintelligence Awareness and Reporting for DoD Employees - CI116.16 for annual training requirement (para 3–2*b*).

- Adds requirement for specific categories of Department of the Army personnel to receive specialized Counterintelligence Awareness and Reporting briefing (para 3–2*c*).

- Updates Counterintelligence Awareness and Reporting trainer requirement, and replaces it with "Counterintelligence-experienced person" (paras 3–2*c*, 3–3, and 5–1*b*).

- Specifies training requirement for Soldiers attending Basic Combat Training and One Station Unit Training (para 3–2*d*).

- Adds Counterintelligence Awareness and Reporting annual training exemption for current U.S. Army Counterintelligence Special Agents (para 3–2*f*).

- Incorporates Army Directive 2013–18, Army Insider Threat Program (para 4–6).

- Consolidates "reportable counterintelligence incidents" and "additional matters of counterintelligence interest" (table 4–1).

- Updates and consolidates incidents, activities, indicators, and behaviors found in DoDD 5240.06 (tables 4–2, 4–3, and 4–4).

- Adds listing of "technical activities, indicators, and incidents" (table 4–5).

- Updates reporting procedures for prohibited activities in accordance with DoDI 1325.06, Army Directive 2025-03, and AR 600–20 (para 4–12*f*).

- Adds Counterintelligence Awareness and Reporting special briefing requirements and listing for specific Department of the Army personnel, positions, and programs (chap 5).

- Adds Counterintelligence Awareness and Reporting support availability for current and former Department of the Army personnel seeking foreign government employment (para 5–8).

- Adds reporting procedures for Unauthorized Installation Access, Unmanned Aircraft Systems, and Controlled Turn Around incidents (para 6–5).

- Adds reporting procedures for threats to individuals under the protection of the U.S. Secret Service (para 6–6).

- Incorporates Army Directive 2025–03, Reporting Prohibited Activities (RPA) (throughout).

Contents (Listed by chapter and page number)

Chapter 1
Introduction

1–1. Purpose
This regulation implements DoDD 5240.06, establishes policy, assigns responsibilities, and establishes requirements for the Army's Counterintelligence Awareness and Reporting (CIAR) program; it establishes the reporting responsibilities for DA personnel and the potential punitive actions for those who violate reporting responsibilities.

1–2. References, forms, and explanation of abbreviations
See appendix A. The abbreviations, brevity codes, and acronyms (ABCAs) used in this electronic publication are defined when you hover over them. All ABCAs are listed in the ABCA directory located at https://armypubs.army.mil/.

1–3. Associated publications
This section contains no entries.

1–4. Responsibilities
Responsibilities are listed in chapter 2.

1–5. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in the Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

Chapter 2
Responsibilities

2–1. Deputy Chief of Staff, G–2
a. The DCS, G–2 is the principal military adviser to the Secretary of the Army (SECARMY) and Chief of Staff of the Army on intelligence and counterintelligence (CI), the Army's Senior Intelligence Officer, and the Army's Intelligence Community Head. The DCS, G–2 will—

(1) Establish and oversee the implementation of the Army CIAR program as the senior intelligence officer of the Army.

(2) Assess CIAR program effectiveness as an element of the Army's overall CI effort.

(3) Establish policy for the reporting and processing of CI incidents.

(4) Ensure Army leadership is aware of significant CI threats and other CI related incidents.

b. Ensure the Director, Army G–2X—

(1) Ensures that CIAR is implemented as a priority program of the Army Intelligence and Security Enterprise.

(2) Conducts annual assessments of the effectiveness of the Army CIAR program.

(3) Provides oversight and approval for the development of Army CIAR training content.

(4) Provides oversight and approval of Army wide CIAR engagement strategy.

c. Ensure the Commander, 650th Military Intelligence Group will implement CIAR in support of organizations, personnel, and installations of the North Atlantic Treaty Organization (NATO) alliance in accordance with NATO directives, regulations, and policies.

d. Ensure the Commanding General (CG), U.S. Army Intelligence and Security Command mans, equips, and resources U.S. Army Counterintelligence Command (ACIC) to update and maintain CIAR materials, modules, and systems.

e. Ensure the CG, ACIC—

(1) Executes responsibilities of the Army Counterintelligence Coordinating Authority (ACICA) as delineated in AR 381–20.

(2) Coordinates, deconflicts, and centrally manages CIAR reporting across the Army.

(3) Monitors incident reporting systems, outlined in paragraph 6–2 or any successor system, and develops policy and procedures for their use.

(4) Submits all Army CIAR referrals to the Federal Bureau of Investigation (FBI) for any indications classified national security information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power pursuant to 50 USC 3381.

(5) Coordinates, manages, and approves the release of all Army CIAR-related information to external entities (for example, Federal agencies, State, local, foreign governments).

(6) Serves as the approval authority for the release of information from closed CI investigations for use in developing revisions to CIAR training materials.

(7) Assists those DoD Component Headquarters, Defense Agency Headquarters, and DoD Field Activity Headquarters in the development and implementation of their CIAR program pursuant to DoDI O-5240.10, when ACI has been identified as the supporting Military Department Counterintelligence Organization (MDCO).

(8) Designates CI-experienced persons, based on their cumulative knowledge, skills, and abilities, to conduct specialized CIAR briefings.

(9) Develops and maintains a public domain internet ACIC website to promote the mission of the ACIC, CIAR, and provides a listing of all ACI field offices and resident agencies.

(10) Appoints an ACI eGuardian Program Manager in the minimum grade of GS–14, E–7, W–3, or O–4.

(a) Serves as the ACI representative to the eGuardian Working Group per DoDI 2000.26.

(b) Ensures suspicious activity reports and information received within the reports are managed, processed, and shared appropriately through local and higher authorities per the policy requirements of DoDI 2000.26 and DoDI 5400.11.

(11) Appoints an Army CIAR Program Manager in the minimum grade of GS–14, E–7, W–3, or O–4; who will serve as the ACI representative with the Defense Intelligence Agency CIAR Council per DoDD 5240.06.

(12) Develops special CIAR briefings and training materials to support the categories identified in chapter 5 of this publication and ensures they are current, relevant, and meet the standards set by the Army G–2X.

(13) Plans, programs, and budgets for the procurement, maintenance, and periodic updates to CIAR marketing materials, training modules, and incident reporting systems.

(14) Provides Army G–2X with an annual CIAR program report pursuant to appendix B.

(15) Develops a proactive Armywide CIAR engagement strategy pursuant to appendix C, in coordination with Army G–2X.

2–2. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will—

a. Publish training requirements outlined in paragraphs 3–2 and 3–3 of this regulation and require tracking of completion of training in the Digital Training Management System (DTMS) or other systems of record.

b. Provide DTMS statistical information to Army CIAR Program Manager.

2–3. Principal officials of Headquarters, Department of the Army and commanders of Army commands, Army service component commands, and direct reporting units

Principal officials of HQDA and commanders of ACOMs, ASCCs, and DRUs will—

a. Cooperate with and assist U.S. Army Counterintelligence (ACI) Special Agents with the execution of the CIAR program.

b. Ensure that those CI incidents, behavioral indicators, and suspicious activities as defined in chapter 4 are reported to ACI pursuant to paragraph 6–2 of this publication.

c. Track completion of CIAR training for all DA personnel under their authority in accordance with this regulation.

d. Produce a quarterly report that consolidates input from subordinate commands, as appropriate, to be provided to the Army CIAR Program Manager. This report will include a list of those supported units to

which CIAR briefings were provided, event dates, estimated number of attendees, and any problems or issues that are assessed as hindering the CIAR program.

e. Include the training and reporting requirements of this regulation in command inspection programs.

f. Post a link to the iSalute online CI incident tipline on all Army public domain websites hosted by the organization.

g. Oversee compliance and execution of the CIAR program, for ASCCs with an assigned Military Intelligence Brigade-Theater.

h. Identify and refer those personnel referenced in chapter 5, who should receive special CIAR briefings and debriefings to the local ACI office.

i. Exclude the details of CI reported incidents to preserve potential for SECARMY controlled CI activities unless authorized by the ACICA. Any command briefings or notifications that may be required will be accomplished by the ACI office executing SECARMY authorities. This requirement does not preclude Army personnel from reporting the details of any intelligence oversight issue that is reportable to the Inspector General as required by AR 381–10.

2–4. Chief, National Guard Bureau and Chief of Army Reserve

In addition to requirements in paragraph 2–3, the CNGB and CAR will—

a. Ensure CIAR training is provided to Army National Guard (ARNG) and U.S. Army Reserve (USAR) personnel prior to mobilization, and as required by this regulation.

b. Coordinate with ACIC to incorporate assigned CI personnel into CIAR coverage plan.

c. Ensure ARNG and USAR units will report matters or incidents defined in chapter 4 in compliance with procedures identified in paragraph 6–2.

2–5. Commanding General, U.S. Army Forces Command

In addition to requirements in paragraph 2–3, the CG, U.S. Army Forces Command (FORSCOM) will coordinate with ACIC to develop a CIAR coverage plan throughout regions, using assigned ACI Special Agents.

2–6. Commanding General, U.S. Army Training and Doctrine Command

In addition to requirements in paragraph 2–3, the CG, TRADOC will—

a. Ensure CIAR is incorporated into Basic Combat Training One Station Unit Training, and other Initial Entry Training for all new soldiers within the first 30 days of active duty to familiarize them with command and individual reporting responsibilities and the role of the supporting ACI office.

b. Coordinate with ACIC to incorporate assigned CI personnel into CIAR coverage plan.

2–7. All Army commanders/directors of Army organizations

In addition to requirements in paragraph 2–3, Army commanders/directors of Army organizations will—

a. Inspect compliance with the CIAR requirements of this regulation in unit command inspection programs in accordance with appendix D.

b. Administer judicial or administrative action if appropriate, pursuant to applicable law or policy, when personnel fail to report information as described in chapter 4.

c. Record completion of CIAR training in the DTMS or other systems of record used to track training for other DA personnel. Upon request, provide all records to ACIC and the Army CIAR Program Manager.

d. Report CIAR training metrics to senior commanders and their threat working groups in support of antiterrorism, force protection, and counter-insider threat programs in accordance with Installation Status Report (ISR 603) requirements.

2–8. Contracting officers

Ensure the CIAR training and reporting requirements of this regulation are incorporated into Army contracts as appropriate and made applicable to associated personnel.

Chapter 3
Counterintelligence Awareness and Reporting Education

3–1. Training policy
Per DoDD 5240.06, CIAR training will include instruction on—

a. The threat from foreign intelligence entities (FIEs), a term that includes international terrorists.

b. The methods, also known as "modus operandi," of FIEs.

c. FIEs' use of the Internet and other communications including social networking services.

d. The CI insider threat.

e. The early detection of espionage and other intelligence activities through identification and referral of anomalies.

f. Reporting responsibilities regarding foreign travel and foreign contacts.

g. The reporting requirements for CI incidents and indicators.

3–2. Army training requirement
a. DA personnel will complete CIAR training within 30 days of assignment or employment to an organization, and every 12 months thereafter pursuant to DoDD 5240.06.

b. DA personnel will complete "Counterintelligence Awareness and Reporting for DoD Employees" – CI116.16, located at https://www.cdse.edu/, to satisfy Army annual training requirements.

c. DA personnel identified in chapter 5 of this publication will receive a special CIAR briefing directly (for example, in person, via DoD communications systems) from an ACI Special Agent or a CI-experienced person in addition to their annual training requirement.

d. Personnel attending Initial Military Training, including Basic Combat Training and One Station Unit Training, will receive CIAR training via HQDA-approved multimedia presentation.

e. Failure to receive training does not relieve individuals from their reporting responsibilities in chapter 4 of this regulation.

f. Current ACI Special Agents are exempt from the annual CIAR training requirements.

3–3. Counterintelligence support to training
Organizational CI elements and ACIC elements will—

a. Provide their supported organizations with assistance to establish and maintain CIAR training.

b. Provide their supported organizations with a CI-experienced person to conduct supplemental CIAR training upon request and when possible.

c. Review supported organization CIAR training materials for accuracy and completeness when unable to provide a CI-experienced person to conduct training.

3–4. Supplemental training
Units may conduct supplemental CI awareness training using live training by a CI-experienced person or through DoD or Army authorized web-based, video, or other media. This is optional and should be tailored to the specific mission, deployment, operation, or activity.

Chapter 4
Reporting Requirements
All provisions of chapter 4 are punitive, with the exception of paragraph 4–5. Violations of the punitive provisions of chapter 4 may subject offenders to criminal prosecution, disciplinary action under the Uniform Code of Military Justice (UCMJ), adverse administrative action pursuant to AR 690–752, or other adverse action authorized by applicable provisions of law.

4–1. Responsibility to report incidents
The following persons are required to report incidents as defined in paragraph 4–6 to ACI within 24 hours; all other persons associated with Army activities but not listed below should report CI incidents to their servicing MDCO as soon as possible—

a. Regular Army personnel and Army civilian employees.

b. USAR personnel while in active status and reservists on inactive duty for training status.

c. ARNG personnel when performing or supporting a federal mission.

d. Foreign national employees of the DoD in foreign areas, as stipulated in command directives and status of forces agreements.

e. Army contractor employees.

f. Military, DoD civilian, and DoD contactor personnel of U.S. defense agencies for which ACI provides CI support in accordance with DoDI O-5240.10 and employees of the U.S. Government in foreign nations for whom the Army provides support.

4–2. Failure to report

DA personnel who fail to report information, as required in chapter 4 of this regulation, that identifies reportable contacts, activities, indicators, and behaviors may be subject to judicial or administrative action, or both, pursuant to applicable law and regulations.

a. Persons subject to the UCMJ who violate the punitive provisions of this regulation may be subject to punitive action under Article 92, UCMJ, as well as to adverse administrative or other adverse action authorized by applicable provisions of the USC or Federal regulations.

b. Civilian employees who violate the punitive provisions of this regulation may be subject to appropriate disciplinary actions in accordance with AR 690–752.

c. Contractor personnel who violate punitive provisions of this regulation may be subject to appropriate disciplinary action under the provisions of the associated contract and statement of work.

4–3. Fabricated reporting

Persons who report CI-related incidents, suspicious activity, or CI matters which are intentionally false or fabricated are subject to disciplinary or administrative action under Article 107, UCMJ and/or 18 USC 1001.

4–4. Obstruction

Any DA personnel who obstruct (or attempt to impede) others from reporting a CI-related incident, suspicious activity, or other CI matter are subject to disciplinary or administrative action under Article 131b, UCMJ and/or 18 USC Chapter 73.

4–5. Rewards

If a reported incident helps stop a case of espionage or terrorism, the originator of the reported information may be eligible for a reward. The reward is authorized by 18 USC 3071, which authorizes the Attorney General to make payment for information on espionage or terrorist activity in any country, which leads to the arrest or conviction of any person(s); for commission, conspiring, or attempting to commit an act of espionage or terrorism against the United States, or for the prevention, frustration, or favorable resolution of an act of terrorism against a United States person or property.

4–6. Reportable incidents, behaviors, and indicators

a. For the purpose of this paragraph, “contact” means any communication directed to an individual including solicited or unsolicited telephone calls, text messages, interaction via social media and networking websites, email, 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.

b. Tables 4–1 through 4–5 contain reportable incidents, contacts, activities, indicators, behaviors, and cyber threats associated with FIEs, international terrorism, and cyberspace.

c. These tables are not all inclusive and do not limit what may be considered a CI incident, anomaly, or a potential threat to national security.

Table 4–1
Reportable counterintelligence incidents

First Amendment-protected activities should not be reported as suspicious activity absent articulable facts and circumstances that support the source agency’s suspicion that the behavior observed is not innocent, but rather reasonably indicative of illicit activity associated with international terrorism, espionage, and other national security crimes including evidence of pre-operational planning

Table 4–1
Reportable counterintelligence incidents—Continued

related to international terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion.

1.	Espionage. The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to 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 in time of war or peace.
2.	Spying. In time of war, the act of clandestinely or under false pretenses collecting or attempting to collect information with the intent to convey it to a hostile party.
3.	Sabotage. Damaging, manipulating, or defacing part of a facility/infrastructure or protected site to injure or interfere with, or obstruct, the national defense by willfully injuring, destroying, or attempting to destroy any national defense or war material, premises, or utilities, to include human and natural resources.
4.	Sedition. Advocating, engaging in, or supporting the overthrow of the government of the United States, or any political subdivision thereof, including that of any State, Commonwealth, Territory, or the District of Columbia, by force or violence; or seeking to alter the form of these governments by unconstitutional or other unlawful means.
5.	Subversion. Advocating or encouraging military, civilian, or contractor personnel within the DoD or United States Coast Guard to violate the laws of the United States, or any political subdivision thereof, including that of any State, Commonwealth, Territory, or the District of Columbia, or to disobey lawful orders or regulations, for the purpose of disrupting military activities, or personally undertaking the same (for example, Mutiny).
6.	Treason. Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere.
7.	Assassination/Incapacitation. The assassination or incapacitation (including anomalous health incidents) of DoD personnel by FIEs or suspected agents of a foreign power.
8.	Anomalies. Foreign power activities or knowledge, inconsistent with the expected norms, that suggest prior foreign knowledge of U.S. national security information, processes, or capabilities.
9.	Extortion/Coercion. Any situation involving threats, compulsion, intimidation, influence, or pressure brought to bear on DoD personnel by FIEs directly or through a third party. Such as family members or friends residing in foreign countries.
10.	Unauthorized Disclosure. Any known or suspected incidents of communication, be it physical or digital, in which there is a transfer of national defense information (classified or unclassified) to any unauthorized recipient, including public disclosure.
11.	Deliberate Security Compromise. Incidents in which DoD personnel deliberately violate policy or procedures in the processing of classified national security information using information systems or digital media.
12.	Cover Identity Compromise. Intentional compromise of the identity of DoD personnel operating as a covert agent (for example, cover status).
13.	Elicitation. Questioning individuals at a level beyond mere curiosity about particular facets of an organization's mission, facilities, purpose, operations, security procedures, and so forth, that would arouse suspicion in a reasonable person.
14.	Suspicious contact. When any person exhibits undue interest, requests information, offers financial enticement or employment associated with the production of publications (for example, information papers, white papers, consulting) derived from critical technology fields or national defense information.
15.	Foreign Travel Incident. DoD personnel or their family members traveling in foreign countries are contacted or detained by persons who represent a foreign law enforcement, security, or intelligence organization.
16.	Theft/Loss/Diversion. Stealing or diverting DoD critical technology or weapon systems by anyone on behalf of or for the benefit of a foreign power or any unauthorized entity.
17.	Critical Infrastructure Incident. Actions associated with a characteristic of unique concern to specific critical infrastructure with regard to their personnel, facilities, systems, or functions (for example, the unexplained failure of critical assets, systems, or mission essential vulnerable areas).
18.	Cyber Attack. Compromising, or attempting to compromise or disrupt an organization's information technology infrastructure.
19.	Expressed or Implied Threat. Communicating a spoken or written threat to damage or compromise DoD facilities, infrastructure, missions, or personnel.
20.	Aviation Activity. Operation of aircraft, drones, unmanned aircraft systems/vehicles (UAS/UAV), or similar technology, including those of unknown origin/technology such as those associated with unidentified anomalous phenomenon, in a manner that

Table 4–1
Reportable counterintelligence incidents—Continued

	reasonably may be interpreted as suspicious, such as the likely unauthorized observation/surveillance of sensitive or classified DoD installations or activities, or posing a threat to DoD personnel or installations.
21.	Breach/Attempted Intrusion. Unauthorized personnel attempting to or actually entering a restricted area or protected site, including the impersonation of authorized personnel (for example, police/security, janitor).
22.	Testing or Probing of Security. Deliberate interactions with, or challenges to, DoD installations, personnel, systems, or attempted intrusion that reveal physical, personnel, or cyber security capabilities or vulnerabilities.
23.	Misrepresentation. Misusing or presenting false insignia, documents, access cards, and/or identification, to misrepresent or impersonate one's affiliation to cover possible illicit activity (for example, the unlawful possession or use of Army intelligence identification).
24.	Photography. Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), and so forth.
25.	Observation/Surveillance. Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (for example, engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, use of specialized observation equipment, and so forth.
26.	Materials Acquisition/Storage. Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible illicit activity.
27.	Acquisition of Expertise. Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities that would arouse suspicion in a reasonable person.
28.	Weapons Discovery. Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
29.	Special Category Absentee. Unauthorized or unexplained absence of DoD personnel who had access within the 5 years preceding their absence to TOP SECRET, sensitive compartmented information, special access programs, and critical nuclear weapons design information; personnel who were assigned to a special mission unit; and personnel in the DoD Cryptographic Access program. Included in this category are defectors, absentee DoD personnel who travel to a country other than the one in which they are stationed, and in which there is evidence that the individual may be involved with a foreign intelligence service or terrorist organization; absentees who have been found to be in possession of classified national security information; and cases where there is information that indicates that the Soldier is a potential terrorist or espionage associated insider threat or that he may leak classified national security information to unauthorized persons.
30.	Special Category Suicide. Actual or attempted suicide (including suicidal ideation) of DoD personnel who had access within the 5 years preceding their absence to TOP SECRET, sensitive compartmented information, special access programs, and critical nuclear weapons design information; personnel who were assigned to a special mission unit; and personnel in the DoD Cryptographic Access program.

Table 4–2
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 4–2 of this regulation. The activities in items 23 and 24 are reportable, but failure to report these activities may not alone serve as the basis for punitive action under Article 92, UCMJ.	
1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through social networking services that is not related to official duties.
2.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
3.	Visits or contact with foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
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.

Table 4–2
Reportable foreign intelligence contacts, activities, indicators, and behaviors—Continued

6.	Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
7.	Attempting to expand access to classified national security 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 national security information is handled or stored.
10.	Discussions of classified national security information over a non-secure communication device (disregard for security practices).
11.	Reading or discussing classified or sensitive information in a location where such activity is not permitted.
12.	Transmitting or transporting classified national security 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, emailing, or transmitting classified material.
16.	Improperly removing classification markings from documents or improperly changing classification markings on documents (disregard for security practices).
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 national security information when the witness did not observe the destruction (disregard for security practices).
22.	Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or social networking service.
23.	Trips to foreign countries that are— a. Short trips inconsistent with logical vacation travel or not part of official duties. b. 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. c. Sudden reversal of a bad financial situation or repayment of large debts.

Table 4–3
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 4–2 of this regulation. The activity in item 10 is reportable, but failure to report this activity may not alone serve as the basis for punitive action under Article 92, UCMJ. Extremism allegations related to DA personnel engaging in or suspected of engaging in the following behaviors; if there is a nexus to foreign powers, agents, or international terrorist activities, are reportable to ACI.
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 organizations or objectives.
3. Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.

Table 4–3
Reportable international terrorism contacts, activities, indicators, and behaviors—Continued

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, email, 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 United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.
11.	Expressing a hatred of American society, culture, government, or principles of the U.S. Constitution that implies support for or connection to an international terrorist organization.

Note: Extremism allegations related to DA personnel having engaged in prohibited activities as defined in DoDI 1325.06 (for example, domestic extremism, domestic terrorism, criminal gangs, protests), are reportable to the chain-of-command or law enforcement per AR 600–20.

Table 4–4
Reportable foreign intelligence entity-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 4–2 of this regulation. The indicators in items 11 through 19 are reportable, but failure to report these indicators may not alone serve as the basis for punitive action under Article 92, UCMJ. Known or suspected automated information system intrusions will also be reported as instructed in AR 25–2.

1.	Actual or attempted unauthorized access into U.S. automated information systems or, 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, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized email 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.

Table 4–4
Reportable foreign intelligence entity-associated cyberspace contacts, activities, indicators, and behaviors—Continued

17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, email 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.

Table 4–5
Reportable technical activities, indicators, and incidents

1.	Technology used by FIE to track the location of DA personnel or assets. Indicators may include, but are not limited to— a. Unidentified electronics discovered in a vehicle, shipping container, baggage, and so forth. b. Unexplainable conditions with government owned electronics such as a change in state in location services applications, additional applications installed on the system without knowledge of the owner. c. Messages on a government owned or personal cell phone that a commercial off-the-shelf tracking device may be in use. d. Sudden significant loss in battery life in cell phones, tablets, or laptops, and so forth. e. Sudden changes in network connection (for example, unexplained changing from 5G to 3G).
2.	Equipment destined for use in a secure space or for a sensitive mission was compromised during the purchase/logistical process. Indicators may include, but are not limited to— a. Equipment shipped from a country not identified as the manufacturer of origin. b. Equipment transited through or held in unnecessary countries as a part of the shipping process. c. Damage or removal of tamper proof seals prior to delivery. d. Indications that equipment was turned on prior to arriving at its destination.
3.	Loss of control of U.S. Government equipment during official travel. Indicators may include, but are not limited to— a. Equipment separation from owner during the customs/immigration process upon arrival. b. Equipment cases lost or held at customs prior to introduction into the country. c. Equipment separated from travelers for security or tariff inspection during exit procedures at the airport. d. Suspected tampering of laptop computers or other portable electronic devices.
4.	Deliberate introduction of prohibited technology into a secure space. Indicators may include, but are not limited to— a. Cleared personnel bringing prohibited electronics into the workspace without submitting the electronics to an inspections or approval process. b. Uncleared personnel deliberately attempting to bring prohibited technology into a controlled area during an escorted visit or meeting or attempting to bring in bags without going through the security screening process. c. Maintenance/vendors/janitorial staff claiming prohibited technology is required as part of their duties, and so forth.
5.	Discovery of a suspected listening device or other technical surveillance devices.

Chapter 5
Special Counterintelligence Briefings and Debriefings

5–1. Conduct of special counterintelligence briefings and debriefings

a. Special CIAR briefings and debriefings will be conducted either one-on-one with the individual concerned, or in small groups.

b. Briefings will be conducted by ACI Special Agents or a CI-experienced person.

c. The briefer will tailor the briefing to the particular risk or threat involved, including methods the person may use to minimize the risk, and will place special emphasis on reporting responsibilities.

d. Debriefings will be conducted as soon as feasible following completion of travel, duty, or visit to a foreign country, or attendance at a conference with foreign personnel by an ACI Special Agent.

5–2. Foreign travel

a. DA personnel scheduled to travel (official, unofficial, permanent change of station) to or through countries with a high foreign intelligence or terrorist threat level as identified by Defense Intelligence Agency or the Department of State, will receive a special CIAR briefing prior to the travel and will be debriefed upon return.

b. DA personnel who have security clearances travelling to foreign locations in any duty status must fulfill pre-and-post travel security briefing and debriefing requirements in accordance with the DoD Foreign Clearance Guide and DoDD 4500.54E.

c. DA personnel deploying in support of military exercises or contingency operations will receive a special CIAR briefing prior to departure.

d. DA personnel taking part in bilateral or multilateral engagements with foreign governments or international organizations will receive a CIAR briefing prior to the event.

5–3. Foreign visitors, personnel, and personal connections

Commanders will coordinate with unit security managers to identify personnel potentially vulnerable to FIE exploitation and ensure they are referred to ACI to receive specialized CIAR briefing. Examples include—

a. Participation in training, education, commercial ventures, technical information sharing, or exchange programs with foreign governments or organizations.

b. Meetings with foreign visitors, foreign exchange personnel, foreign liaison officers, and foreign students.

c. Personnel with close and continuing relationships with relatives or others residing in foreign countries, having foreign business connections or financial interests, or who have other significant ties to foreign countries.

5–4. Army modernization

DA personnel working in critical emerging science and technology (S&T) and projects pursuant to DoDI 5000.83, DoDI O-5240.24, and AR 70–77 will receive in-person special CIAR briefings on an annual basis and notify the supporting ACI office of all projected foreign travel prior to departure. Such personnel will receive foreign intelligence threat briefings prior to foreign travel or event. Upon completion of travel, personnel will contact their supporting ACI office to schedule a debriefing. Examples of personnel or activities include—

a. Attendance of scientific, technical, engineering, or other professional meetings, trade shows, or symposia that representatives from foreign countries sponsor or attend, whether in the U.S. or abroad.

b. Research, development, testing, and evaluation.

c. Project managers and S&T managers who engage with foreign partners and/or foreign officials.

d. Personnel at initial fielding locations.

e. Trade shows where Army technologies are exhibited.

5–5. Critical program information

Acquisition program personnel working with organic or inherited Critical Program Information as defined in the DoD Critical Programs and Technologies List, DoDI 5000.83, DoDI 5200.39, DoDI 5200.44, DoDI O-5240.24, and AR 70–77*,* and identified through Army Research and Technology Protection Center assessment process, will receive an in-person annual CIAR briefing and notify ACI of all projected foreign travel prior to departure. Such personnel will receive foreign intelligence threat briefings prior to foreign travel. Upon completion of travel, personnel will contact ACI to schedule a debriefing.

5–6. Personnel with access to Sensitive Compartmented Information and Special Access Programs

a. Pursuant to Intelligence Community Directive 703, and other applicable policies, personnel with access to Sensitive Compartmented Information, Special Access Programs (SAPs), Alternative Compensatory Control Measures (ACCM), or assigned to a special mission unit will receive an in-person special CIAR briefing on an annual basis. These personnel also 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 ACI to schedule a debriefing. Personnel with special access should contact their servicing ACI office, in accordance with DoDI 5205.11 and AR 380–381.

b. ACI Special Agents will be provided access to SAP or ACCM programs which require CI coverage or support.

5–7. Defense critical infrastructure

a. Personnel assigned to or supporting defense critical infrastructure or associated assets, pursuant to DoDD 3020.40 and DoDI 5240.19, will receive an in-person special CIAR briefing on an annual basis. Such personnel will notify their local ACI office of all projected foreign travel or foreign visits per paragraphs 5–1 and 5–2 of this regulation.

b. ACI will coordinate CIAR support with the Cybersecurity & Infrastructure Security Agency when critical infrastructure sector assets, systems, and networks are under the purview of the Department of Homeland Security.

5–8. Foreign government employment

Current and retired DA personnel seeking employment with foreign government entities will have CIAR training and support made available. Personnel should consult AR 600–291 and Intelligence Community Directive 712 as appropriate.

5–9. Information technology professionals

System administrators, privileged users, and those with privileged access that provides an individual capability to alter the properties, behavior, or control of a DoD information system will receive in-person special CIAR briefings on an annual basis. This personnel group includes, but is not limited to, any of the following types of access—

a. "Super user," "root," or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth.

b. Access to change control parameters (for example, routing tables, path priorities, and addresses) of routers, multiplexers, and other key information systems or network equipment or software.

c. Ability and authority to control and change program files, and other users' access to data.

d. Direct access (also called unmediated access) to functions at the operating system level that would permit system controls to be bypassed or changed.

e. Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers, intrusion detection software, and firewalls) or in performance of cyber or network defense operations.

5–10. Professional and educational exchange programs with foreign governments

a. DA personnel and contracted cadets attending foreign universities, foreign military education courses, or assigned as a liaison to a foreign government or international organization will receive a special CIAR briefing prior to departure.

b. Recipients of scholarships, fellowships, and grants (for example, David L. Boren Scholarships and Fellowships, Project Global Officer) from the National Security Education Program will have CIAR training and support made available.

Chapter 6
Reporting Procedures

6–1. Individual response

DA personnel will report threats related to FIE, international terrorists, and cyberspace to their supporting ACI office within 24 hours. DA personnel must report unauthorized disclosures of classified national security information to the appropriate security authorities in accordance with DoDM 5200.01, Volume 3. Additionally, in accordance with DoDD 5148.13 and AR 381–10, DA personnel must report questionable intelligence activities and significant or highly sensitive matters involving intelligence activities that may have serious implications for the execution of DoD missions.

6–2. Reporting the incident

a. DA personnel will report suspicious activity referenced in this publication to an ACI office within 24 hours after learning of the incident.

b. If a report cannot be made directly to an ACI office, personnel may utilize the following incident reporting systems—

(1) The iSalute online CI incident tipline located at https://www.usainscom.army.mil/.

(2) The 1–800–CALL–SPY tipline (1–800–225–5779) if located in the United States.

c. When using the CALL SPY tipline or iSalute, provide only that information which the ACI Special Agent will need in order to contact you. Do not provide any classified details of the incident or matter over the telephone or online.

d. When ACI support is unavailable, DA personnel will report the incident within 24 hours to their security officer, supervisor, or commander, who will refer the incident to ACI within 48 hours of receipt.

6–3. Imminent threats

If the incident presents an imminent threat to life or property, call 911 or the local Military Police station. If outside the United States, contact the appropriate local law enforcement entity, Military Police station, or U.S. Embassy or Consulate Regional Security Office.

6–4. Prohibited activities

a. ACI will ensure all allegations (and related information) of DA personnel having engaged in a prohibited activity, as defined in DoDI 1325.06 and AR 600–20, are referred to the appropriate chain-of-command or entity.

b. ACI will report allegations to the Army Inspector General in accordance with PL 116–283.

6–5. Unauthorized Installation Access, Unmanned Aircraft Systems, and Controlled Turn Around incidents

DA personnel will—

a. Ensure all Army Unauthorized Installation Access, UAS, and Controlled Turn Around incidents are captured within the Commander's Critical Information Requirement, Command and Control Information Environment (C2IE), and eGuardian.

b. Ensure incidents reported in the eGuardian "Counterintelligence" program are provided to ACIC within 72 hours of receipt.

6–6. Threats to individuals under U.S. Secret Service protection

DA personnel will immediately report threats to or about persons and events under the protection of the U.S. Secret Service (USSS) to the nearest USSS field office (https://www.secretservice.gov/).

6–7. Anomalous Health Incidents

DA personnel who have experienced a suspected anomalous health incident (AHI) should—

a. Immediately contact a health care provider to seek treatment. The health care provider will conduct a comprehensive medical assessment and look for red flags that could suggest a medical emergency unrelated to AHI. Some symptoms may dissipate rapidly, and immediate medical treatment is imperative.

b. Report the incident to their security officer, supervisor, or commander.

c. Security officers, supervisors, commanders, and medical professionals are required to report medically assessed AHI to ACI.

Chapter 7
Assessment of Counterintelligence Awareness and Reporting

7–1. Purpose

Using data furnished by CI elements and collated by ACIC, the Director, Army G–2X will maintain statistical data on CIAR for use by DCS, G–2 to monitor and evaluate its effectiveness.

7–2. Counterintelligence element responsibility

CI elements at echelons below corps will produce annual reports on CIAR generated activity. This report will be transmitted to ACIC no later than 20 days after the end of each fiscal year (20th of October). Report the following:

a. The number of Counterintelligence Incident Reports which resulted from CIAR training.

b. The number of leads generated from CIAR training.

c. Number and description of any significant reporting resulting from CIAR training.

d. A description of any other action taken on reports, such as leads referred to other agencies or organizations.

Appendix A

References

Section I

Required Publications

Unless otherwise stated, Department of the Army publications are available on the Army Publishing Directorate website at https://armypubs.army.mil/. DoD issuances are available on the Washington Headquarters Services website at https://www.esd.whs.mil/. The USC is available at https://uscode.house.gov/. The Uniform Code of Military Justice is available at https://jsc.defense.gov/. Intelligence Community Directives are available at https://www.dni.gov/.

AR 70–77
Technology and Program Protection (Cited in para 5–4.)

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities (Cited in para 5–6*a*.)

AR 381–10
The Conduct and Oversight of U.S. Army Intelligence Activities (Cited in para 2–3*i*.)

AR 381–20
The Army Counterintelligence Program (U) (Available by contacting the proponent.) (Cited in para 2–1*e*(1).)

AR 600–20
Army Command Policy (Cited in summary of change.)

AR 600–291
Foreign Government Employment (Cited in para 5–8.)

AR 690–752
Disciplinary and Adverse Actions (Cited in chap 4.)

Article 92, UCMJ
Failure to obey order or regulation (Cited in para 4–2*a*.)

Article 107, UCMJ
False Official Statements; False Swearing (Cited in para 4–3.)

Article 131b, UCMJ
Obstructing Justice (Cited in para 4–4.)

DA Pam 25–403
Army Guide to Recordkeeping (Cited in para 1–5.)

DoDD 3020.40
Mission Assurance (MA) (Cited in para 5–7*a*.)

DoDD 4500.54E
DoD Foreign Clearance Program (Cited in para 5–2*b*.)

DoDD 5148.13
Intelligence Oversight (Cited in para 6–1.)

DoDD 5240.01
DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities (Cited in title page.)

DoDD 5240.02
Counterintelligence (CI) (Cited in title page.)

DoDD 5240.06
Counterintelligence Awareness and Reporting (CIAR) (Cited in title page.)

DoDI 1325.06
Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces (Cited in summary of change.)

DoDI 2000.26
DoD Use of the Federal Bureau of Investigation (FBI) eGuardian System (Cited in para 2–1*e*(10)(*a*).)

DoDI 5000.83
Technology and Program Protection to Maintain Technological Advantage (Cited in para 5–4.)

DoDI 5200.39
Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E) (Cited in para 5–5.)

DoDI 5200.44
Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (Cited in para 5–5.)

DoDI 5205.11
Management, Administration, and Oversight of DoD Special Access Programs (Cited in para 5–6*a*.)

DoDI 5240.19
Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP) (Cited in para 5–7*a*.)

DoDI O-5240.10
Counterintelligence (CI) in the DoD Components (Cited in para 2–1*e*(7).)

DoDI O-5240.24
Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA) (Cited in para 5–4.)

DoDI 5400.11
DoD Privacy and Civil Liberties Programs (Cited in para 2–1*e*(10)(*b*).)

DoDM 5200.01, Volume 3
DoD Information Security Program: Protection of Classified Information (Cited in para 6–1.)

EO 12333
United States Intelligence Activities (Cited in title page.) (Available at https://dpcld.defense.gov/.)

Intelligence Community Directive 703
Protection of Classified National Intelligence, Including Sensitive Compartmented Information (Cited in para 5–6*a*.)

Intelligence Community Directive 712
Requirements for Certain Employment Activities by Former Intelligence Community Employees (Cited in para 5–8.)

PL 116–283
William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Cited in para 6–4*b*.) (Available at https://www.congress.gov/.)

10 USC 7013
Secretary of the Army (Cited in title page.)

18 USC 1001
Statements or entries generally (Cited in para 4–3.)

18 USC Chapter 73
Obstruction of Justice (Cited in para 4–4.)

18 USC 3071
Information for which rewards authorized (Cited in para 4–5.)

50 USC 3381
Coordination of counterintelligence activities (Cited in para 2–1*e*(4).)

Section II

Prescribed Forms

This section contains no entries.

Appendix B

Annual Counterintelligence Awareness and Reporting Program Report

B–1. Purpose

The purpose of the annual CIAR program report is to assist the DCS, G–2 in evaluating the effectiveness of the Army CIAR program using qualitative and quantitative analytical methods. It is intended as a guide and may not cover all possible report requirements. In accordance with paragraph 2–1*e,* the CG, ACIC is assigned responsibility to produce this report.

B–2. Annual report format

a. Date of report (updated annually each fiscal year).
b. Executive Summary describing the state of Army CIAR Program.
c. Organization breakdown of the Army CIAR Program and their associated enabling functions.
d. Briefings and debriefings by the personnel categories listed in chapter 5 of this publication.
e. CIAR information leads, reporting, and referrals by ACI including the following statistics—
(1) Counterintelligence Incident Reports.
(2) eGuardian Suspicious Activity Reports.
(3) Intelligence Information Reports.
(4) Spot Reports.
(5) iSalute leads.
(6) Call Spy leads.
(7) Prohibited Activities.
(8) A description of any other significant action taken such as leads referred to other agencies.
(9) A description of any significant CI activities generated from the CIAR program.
f. CIAR program trends. Trends and new information will include, but not be limited to—
(1) Targets of foreign collection.
(2) FIE modus operandi.
(3) Cyberspace trends.
(4) CI Insider Threat.
g. Required external coordination.
h. Plan of action and milestones.
i. Measures of performance and effectiveness.
j. Gaps and Risks.
k. Recommendations.
l. Unfunded Requirements.
m. Approving signature of commander or senior leader.

B–3. Annual report submission

a. The annual report is due 1 November of each year.
b. The finalized CIAR annual report will be submitted to DCS, G–2, Counterintelligence Division (DAMI–CD).

Appendix C

Army Counterintelligence Awareness and Reporting Engagement Strategy

C–1. Purpose

The purpose of the CIAR engagement strategy is to more effectively reach Soldiers, Civilians, and families of the U.S. Army. This strategy should cover all of the channels ACI intends to employ to engage the greater Army community. In accordance with paragraph 2–1*e,* the CG, ACIC is assigned responsibility to produce this strategy.

C–2. Engagement strategy considerations

At a minimum, the CIAR engagement strategy will address—

a. Engagement. Develop comprehensive engagement strategies informed by thoughtful research and aligned with the Army's CIAR objectives, target audience, and trends. Identification of opportunities for growth and recommend initiatives to enhance awareness and marketing positioning and the development of creative dissemination strategies.

b. Content creation. Creation of compelling and persuasive content for various platforms, including but not limited to official website, blogs, social media, email campaigns, press releases, and physical marketing materials. Tailor content to resonate with different target audiences and ensure brand consistency in all communications.

c. Marketing. Manage and optimize digital marketing campaigns, including search engine optimization, search engine marketing, and the dissemination of CIAR marketing materials to ACI offices for local use, generation, and conversions.

d. Research. Conduct research to understand CIAR program needs, preferences, and trends.

e. Analytics and reporting. Identification of various analytics tools to track and measure the performance of CIAR marketing campaigns and communication efforts.

f. Budget requirements. The projected budget to implement the strategy and any unfunded requirements.

C–3. Engagement strategy format

a. Date of report (updated annually each fiscal year).

b. Executive summary describing the objectives of the strategy.

c. Prior fiscal year performance.

d. Upcoming fiscal year strategy to address engagement budget requirements, priorities, approach, anticipated challenges, and goals.

e. Required external coordination.

f. Plan of action and milestones.

g. Measures of performance and effectiveness.

h. Gaps and risks.

i. Recommendations.

j. Unfunded requirements.

k. Approving signature of commander or senior leader.

C–4. Strategy submission

a. The strategy is due 1 November of each year.

b. The finalized engagement strategy will be submitted to DCS, G–2, Counterintelligence Division (DAMI–CD).

Appendix D

Internal Control Evaluation

D–1. Function

The function covered by this evaluation is to ensure effective implementation of the Army's CIAR training.

D–2. Purpose

The purpose of this evaluation is to assist unit commanders in evaluating the key internal controls listed. It is intended as a guide and does not cover all controls.

D–3. Instructions

Answers must be based on the actual testing of key internal controls by utilizing one of four test methods which are Inquiry, Observations, Examination, or Re-performance. Inquiry regarding a control's effectiveness does not, by itself, provide sufficient evidence of whether a control is operating effectively and generally is corroborated through other types of control tests (observation or inspection). Answers that indicate deficiencies must be explained and corrective action identified in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that the evaluation has been conducted must be accomplished on a DA Form 11–2 (Internal Control Evaluation Certification).

D–4. Key control questions

a. Have Army commanders—

(1) Established procedures to ensure that CIAR training is scheduled for members of their unit?

(2) Included the requirements of this regulation as a mandatory subject in the organizational inspection program?

(3) Established a process to track CIAR training in their units?

(4) Established a process to track CIAR training on their installation, if appropriate?

(5) Maintained contact information for the supporting ACI office (identity of office, names of ACI Special Agents, phone numbers, and email addresses)?

(6) Has the installation identified and communicated all critical facilities and assets with their local supporting ACI Special Agent for prioritization of CI support?

(7) Is information regarding incidents of suspicious activity, sabotage, or potential surveillance shared between Installation law enforcement, CI and security?

b. Army senior commanders—

(1) Does the installation place emphasis on the importance of prompt threat reporting to ensure threat incidents, behavioral indicators, and other matters of CI interest are reported to the supporting ACI office?

(2) Does the installation have a process for tracking completion of CIAR training on the installation?

(3) Has the installation coordinated with a local supporting ACI Special Agent to provide opportunities for initial and annual CIAR training?

(4) Have all unit commanders reported their compliance with initial and annual CIAR training to the installation?

(5) Are CIAR requirements incorporated into installation contracts via a statement of work or on the DD Form 254 (Department of Defense Contract Security Classification Specification), as appropriate?

(6) Does the Installation have a process for ensuring contractors attend CIAR training at least annually?

(7) Does the Installation's public domain and Intranet website include a link to the iSalute online CI reporting portal?

(8) Does the Installation's public domain and Intranet website include contact information for their local supporting ACI office?

(9) Does the installation have an established relationship with a supporting ACI office for coordinating CI support to the installation?

(10) Is the supporting ACI office providing CI updates on FIE threats, to include terrorist threats, during semi-annual Installation antiterrorism working group meetings?

(11) Has the installation identified and communicated all critical facilities and assets with their supporting ACI office for prioritization of CI support?

(12) Is information regarding attempts to gain unauthorized access to installations, facilities, critical technology or equipment shared between installation law enforcement, CI, and security?

(13) Is information regarding incidents of sabotage or potential surveillance activities shared between installation law enforcement, CI and security?

(14) Does the installation antiterrorism working group consider FIE threats and vulnerabilities when developing vulnerability countermeasures or mitigation strategies?

c. Have ACI element commanders—

(1) Established procedures for supporting CIAR?

(2) Ensured assigned ACI Special Agents responded within 48 hours to reported incidents?

(3) Included CIAR in the Organizational Inspection Program?

(4) Include CIAR training, and special CIAR briefings and debriefings as a component of the Covering Agent Program?

(5) Maintained records of activity generated by CIAR training?

(6) Submitted a quarterly report on the unit's CIAR program as required by paragraph 6–2?

(7) Submitted CI Incident Reports (via ACOP) or Suspicious Activity Reports (via eGuardian) within 3 business days after the interview of appropriate complainant/witness who provides best source of information?

(8) Evaluated the effectiveness of CIAR public messaging in their local area?

D–5. Supersession

This evaluation replaces the evaluation previously published in AR 381–12, dated 1 June 2016.

D–6. Comments

Help to make this a better tool for evaluating internal controls. Submit comments to DCS, G–2 at usarmy.pentagon.hqda-dcs-g-2.list.dami-cdc@army.mil.

Glossary of Terms

ACI office
An ACICA-validated ACI field office or resident agency assigned responsibility for a command, facility, program, installation, or geographic area. This includes offices sourced from across the ACI enterprise (for example, ACIC, Military Intelligence Brigade-Theater (MIB–T), FORSCOM, U.S. Army Special Operations Command, USAR, ARNG, and 650th Military Intelligence Group).

Anomalous Health Incidents
Sudden sensory events such as sounds, pressure, or heat concurrently or immediately preceding the sudden onset of symptoms such as headaches, pain, nausea, or disequilibrium (unsteadiness or vertigo). (see DoDD 5111.13 and Secretary of Defense memorandum (Anomalous Heath Incidents), dated 15 September 2021).

Anomaly
Defined in DoDD 5240.06.

Army Counterintelligence Coordinating Authority
The ACICA is an Army level office responsible for the worldwide mission management and technical control of all controlled ACI activities conducted under the SECARMY's Authorities. The ACICA has the authority to task, direct, control, and prioritize all CI activities. The activities include CI investigations, CI operations, special collection procedures, CI projects, CI support to research, technology, and acquisitions, and CI Cyber. The ACICA exercises direct control of all CI investigations including direct tasking of CI field or resident offices. The ACICA is not responsible for CI activities conducted by the 650th MI Group; collection; analysis and production; CI technical services; CI support to force protection, technology, and critical infrastructure; and CI cyber activities. (see AR 381–20).

CI awareness
Defined in DoDD 5240.06.

CI element
Defined in DoDD 5240.02.

CI incident assessment
The collection and examination of information of CI interest to determine if a CI investigation is warranted.

CI insider threat
Defined in DoDD 5240.02.

CI investigations
Defined in DoDD 5240.02.

CI-experienced person
An individual designated by ACIC, based on their cumulative knowledge, skills, and abilities, to conduct specialized CIAR briefings.

Classified national security information
Defined in DoDM 5200.01, Volume 1 and EO 13526.

Collection
Defined in DoDM 5240.01.

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.

Contracted cadet
The military status of a cadet is a member of the Individual Ready Reserve or a member of the Selected Reserve in the Simultaneous Membership Program, unless activated for military training at which time a cadet is placed on orders (see DoDI 1215.08) and is in contrast to a "Reserve Officers' Training Corps (ROTC) student" who may be taking ROTC courses but is not formally enrolled in the program.

Contractor
Defined in DoDD 5240.02.

Controlled unclassified information
Defined in 32 CFR 2002.4.

Counterintelligence
Defined in EO 12333, as amended.

Critical program information
Defined in DoDI 5200.39.

Debriefing
a. Interviewing, under other than hostile conditions, of an individual who has completed an intelligence assignment or who has, through observation, participation, or personal knowledge, information of intelligence or CI value or significance.
b. The process of using direct questions to elicit intelligence information from a cooperative party to satisfy intelligence requirements.

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 (see DoDM 5105.21, Volume 3).

Department of the Army personnel
Persons employed by the Army. It includes all military, civilian, contractors, and foreign nationals.

Espionage
See UCMJ, Article 103a (10 USC 903a).

Field office, ACI
A field office is normally a subordinate element of an MIB–T or ACIC Region. It provides CI support within a specified portion of a geographic area of responsibility and typically provides administrative supervision over multiple resident agency offices.

Force protection
Defined in the DoD Dictionary of Military and Associated Terms.

Foreign diplomatic establishment
Any embassy, consulate, or interest section representing a foreign country.

Foreign intelligence entity
Defined in DoDD 5240.06.

Foreign power
Defined in DoDM 5240.01.

Insider threat
A threat presented by a person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the department; and wittingly, or unwittingly, commits an act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or a destructive act, which may include physical harm to another in the workplace (see Public Law 114–328).

Leak
The unauthorized disclosure of classified or sensitive information, as to the news media.

Military Department Counterintelligence Organization
Elements of the Military Departments authorized to conduct CI investigations (for example, U.S. Army Counterintelligence, Naval Criminal Investigative Service, and the Air Force Office of Special Investigations) (see DoDD 5240.06).

National Security Education Program
The National Security Education Program (NSEP) is a U.S. federal government initiative to enhance U.S. national security and economic competitiveness by increasing “critical need” foreign language skills, cultural understanding, and regional expertise within the U.S. federal workforce. NSEP oversees eight initiatives designed to support and expand language and cultural skills within the federal workforce. NSEP Programs provide pathways to careers in federal government, and select programs include a year-long federal service requirement upon completion of academic study. NSEP oversees eight programs: David L. Boren Scholarships and Fellowships, The Language Flagship, English for Heritage Language Speakers, National Language Service Corps, Project Global Officer, Language Training Centers, and Regional Flagship Language Initiatives (see DoDI 1025.02).

Resident agency, ACI
A resident agency is normally a subordinate element of an ACI field office. It provides ACI support within a specified portion of a geographic area of responsibility.

Sabotage
See 18 USC Chapter 105.

Sedition
See UCMJ, Article 94 (10 USC 894).

Self-radicalization
Significant steps an individual takes in advocating or adopting an extremist belief system for the purpose of facilitating ideologically based violence to advance political, religious, or social change. The self-radicalized individual has not been recruited by and has no direct, personal influence or tasking from other violent extremists. The self-radicalized individual may seek out direct or indirect (through the Internet for example) contact with other violent extremists for moral support and to enhance his or her extremist beliefs.

Special Agent, ACI
An individual (military or civilian) who has been accepted, accredited, and successfully completed Counterintelligence Agent Course or equivalent approved course, and is authorized to investigate national security crimes and support prosecution under UCMJ and federal laws (PMOS MOS 35L, 351L, 35A2E; Office of Professional Management Occupational Series 0132).

Special Agent-In-Charge, ACI
An ACI Special Agent appointed as the supervisor of an ACI field office, resident agency, or ACIC Region.

Spying
See UCMJ, Article 103 (10 USC 903).

Subversion
See 18 USC Chapter 115.

Suspicious activity
Any behavior or incident that is indicative of criminal activities, intelligence gathering, or other preoperational planning related to a security threat to DoD interests.

Terrorism
See 18 USC Chapter 113B.

Treason
See 18 USC 2381.

Unauthorized disclosure
Defined in DoDM 5200.01, Volume 3.

Unsolicited correspondence
Requests for information from a person which may range from direct inquiries by phone, email, fax, or letter in which the recipient is asked to provide seemingly innocuous data. Typical requests include solicitation of research papers, requests for additional information after a public presentation, suggestions for mutual research, requests for survey participation, and so forth; correspondence where the actual

purpose may be to identify by name and position any individual who might be targeted later by a foreign intelligence service, and to elicit targeted information not readily obtainable by other means.