Department of the Army Pamphlet 381–20

Military Intelligence

Counterintelligence Investigative Procedures

Headquarters
Department of the Army
Washington, DC
15 April 2020

UNCLASSIFIED

SUMMARY

DA PAM 381–20
Counterintelligence Investigative Procedures

This new publication, dated 15 April 2020—

- Supports the guidance in AR 381–20 (throughout).
- Provides reference for counterintelligence investigative procedures and processes (throughout).

Headquarters
Department of the Army
Washington, DC
15 April 2020

Department of the Army Pamphlet 381–20

Military Intelligence

Counterintelligence Investigative Procedures

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet complements AR 381–20 (classified) and is the counterintelligence reference for counterintelligence investigative procedures and processes based on U.S. law, Department of the Army policy, Army Counterintelligence Coordinating Authority policy, and U.S. Army Intelligence Center of Excellence doctrine. AR 381–20 will take precedence whenever this publication is in conflict with AR 381–20.

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

Proponent and exception authority. The proponent of this pamphlet is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions or waivers to this pamphlet 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 pamphlet 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 guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–2 (DAMI–CDC), 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. This publication 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 and for the Marine Corps.

Contents (Listed by paragraph and page number)

Table List

Glossary

Chapter 1
Introduction

1–1. Purpose
This pamphlet is the counterintelligence (CI) reference for CI investigative procedures and processes based on U.S. law, Department of the Army (DA) policy, Army Counterintelligence Coordinating Authority (ACICA) policy, and U.S. Army Intelligence Center of Excellence doctrine. Army Regulation (AR) 381–20 will take precedence whenever this publication is in conflict with AR 381–20.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Counterintelligence investigative principles
Army counterintelligence (ACI) special agents (SAs) are responsible for investigating national security crimes and related incidents that affect Army equities. CI investigations are sensitive and legally complex. Understanding CI investigative principles ensures that ACI investigations be conducted in a way that protects the civil liberties of all persons associated with an ACI investigation, resolves identified allegations, and protects the prosecutorial integrity of the investigation.

1–5. Counterintelligence investigative mission and authorities
All SAs assigned to a unit or organization with an investigative mission require a thorough understanding of the ACI investigative mission, techniques, procedures, and legal authorities for conducting ACI investigations. This ensures ACI investigations are conducted in a lawful manner and preserves the prosecutorial integrity of ACI investigations.

a. Tenets of counterintelligence investigations. ACI investigations identify persons, organizations, and other entities engaged in national security crimes against the Army, Department of Defense (DOD), and the U.S.; determine the full nature and extent of their activities; and neutralize their effectiveness through apprehension, prosecution, expulsion, or exposure. The most significant objectives of CI investigations are to minimize or prevent the loss of sensitive and classified defense information to foreign governments and to prevent, preempt, or disrupt foreign terrorist attacks against Army and DOD interests. While it is Army policy that all national security investigations are conducted in a manner that preserves the potential for prosecution, this purpose is secondary to the ACI mission of detecting, identifying, fully determining the extent of, and neutralizing national security threats to the Army, DOD, and the U.S. The primary tenets of CI are as follows:

(1) CI is an intelligence function. Although CI is a fusion of security, law enforcement, and intelligence, the primary objective of CI is to exploit the situation by identifying the larger foreign intelligence entity (FIE) network and to affect their perception and targeting of Army personnel, operations, resources, technology, and information.

(2) CI investigations are about discovering the facts and conveying them to decision makers while maintaining the ability to negate, mitigate, or exploit the FIE threat.

b. Army Counterintelligence Coordinating Authority.

(1) The ACICA, on behalf of the DA G–2X, is accountable for the worldwide management of ACI activities conducted under Secretary of the Army authorities. Investigation management functions include—

(a) Technical authority and control of ACI investigations.

(b) Reviewing, staffing, and coordinating CI investigation procedures.

(c) Opening all ACI investigations.

(d) Providing oversight of all ACI investigations and investigative activities.

(e) Coordinating national-level records checks.

(f) Coordinating with other U.S. Government and military CI agencies to assist in the conduct of investigations.

(2) In accordance with AR 381–20, specific functions of the ACICA include—

(a) Informing the DA G–2 and Army leadership of significant ACI investigations.

(b) Providing periodic reports and briefings to the combatant commanders, DA G–2, and Army and DOD leadership concerning significant ACI investigations and operations.

(c) Conducting direct tasking of ACI unit-level elements when operational necessity dictates immediate action. In these situations, the ACICA will inform appropriate commanders of such tasking.

(d) Acting as the sole authority to open, initiate, close, and terminate investigations worldwide, except those involving North Atlantic Treaty Organization elements, for which the 650th Military Intelligence (MI) Group has authority.

(e) Assigning case control numbers and maintain a tracking system for all ACI investigations.

(f) Serving as the approval authority for all ACI investigative referrals to or operational coordination at the national level with intelligence, CI, security, and law enforcement agencies.

(g) Serving as the single conduit through which all CI investigative tasking external to the Army is coordinated.

(h) Representing ACI investigative policy, planning, and programming issues at U.S. Government and military security, intelligence, and CI agencies and working groups.

(i) Providing technical authority and oversight of Army cyber CI investigative activities.

(j) Notifying the Federal Bureau of Investigation (FBI) of cases in which the Army is investigating allegations of espionage.

(k) Referring information which is not under ACI investigative jurisdiction and which does not involve Army personnel, technology, or security to appropriate security, intelligence, or law enforcement agencies.

(l) Reviewing ACI investigative and operational reports and the activities they represent for quality assurance and to ensure compliance with intelligence oversight policy and provide feedback to the appropriate investigative element.

(m) Ensuring investigations conducted in two or more theaters are properly coordinated.

(n) Reviewing requests for release of ACI information in intelligence files under the provisions of the Freedom of Information Act (FOIA) (see Section 552, Title 5, United States Code (5 USC 552)), the Privacy Act of 1974 (see 5 USC 552a), and discovery motions.

(o) Ensuring case files, project files, source dossiers, records, and reports are properly processed, classified or declassified, and retired to the U.S. Army Investigative Records Repository (USAIRR) when ACI activities are concluded.

(p) Referring CI investigative procedures specified in AR 381–10 to the proper officials for staffing, coordination, and approval.

(q) Ensuring information derived from active and terminated ACI investigations that meets intelligence or CI collection requirements is properly submitted using intelligence information reporting.

(r) Referring questionable CI activity or any activity that presents intelligence oversight concerns to the appropriate command legal and intelligence oversight officers for review.

(s) Conducting name trace and national agency checks (NACs) with appropriate U.S. Government and military agencies.

(t) Maintaining a database for ACI reports and ACI investigations (currently called Army Counterintelligence Operations Portal (ACOP)).

(3) See AR 381–20 for more information concerning ACICA responsibilities and functions.

c. Army theater counterintelligence coordinating authority responsibilities. The Army theater CI coordinating authority serves as the Army service component command focal point for coordinating and deconflicting CI activities within the respective area of operations (AO).

d. Counterintelligence investigative authorities. Investigative authority is the execution of CI investigative mission and activities based upon DOD and DA policy, applicable Executive orders (EOs), and U.S. law. SAs assigned to a unit with an investigative mission execute their investigative authority based on regulatory and other authorities.

e. Regulatory authorities. The basic investigative authority for ACI is codified in directives, regulations, and policy. The primary ARs that address ACI investigative authority are—

(1) AR 381–10. In some instances, the guidance provided in both AR 381–10 and DODM 5240.01 applies. There is no change to Army approval authorities for Procedures 5, 6, and 9 (see DODM 5240.01 for more information on the procedures). The regulation serves as a fundamental authority document governing the conduct of all intelligence activities by the DA, to include CI activities. It provides policy and procedures for the collection, retention, and dissemination of information concerning U.S. persons. SAs will be knowledgeable of the chapter that describes the kind of information about U.S. persons that can be collected. SAs assigned to an organization with an investigative mission should be knowledgeable of the chapters that provide detailed information on the use and approvals for special investigative techniques.

(2) AR 381–12. This regulation establishes the Army's CI awareness program that serves as basis for many ACI investigations and lead development programs. AR 381–12 establishes the requirement for the threat awareness training program and authority for tailored small-group and one-on-one briefings for persons with special vulnerability. It mandates the requirement for personnel to report threat-related incidents. AR 381–12 is a punitive regulation in that

failure to report incidents in compliance with the regulation is an offense punishable under the Uniform Code of Military Justice (UCMJ).

(3) AR 381–20. This regulation provides details of the ACI Program. It contains most of the regulatory authorities used by SAs during the execution of their CI mission, to include investigations. It describes the ACICA responsibilities and authorities for management and oversight of ACI investigations. It provides details on the roles, responsibilities, techniques, and methods for the ACI investigative program. AR 381–20 specifically provides details on the SA's standing investigative authority (SIA) as it pertains to limited counterintelligence assessments (LCAs), preliminary investigations (PIs), and full-field investigations (FFs). Finally, it further clarifies SIA as it pertains to cyber CI investigations.

(4) DODM 5240.01. The manual serves as a fundamental authority document governing the conduct of all intelligence activities by the DA, to include CI activities. It provides policy and procedures for the collection, retention, and dissemination of information concerning U.S. persons. SAs should be knowledgeable of the section that describes the kind of information about U.S. persons that can be collected. SAs assigned to an organization with an investigative mission should be knowledgeable of the sections that provide detailed information on the use and approvals for special investigative techniques.

f. External authorities. In some investigative circumstances, the SA can use external authorities that may exist in support of ACI investigative activities. For example, the commander of an active duty Soldier may authorize the SA to search a Soldier's room or workplace. However, this requires the SA to gain the cooperation of the commander to allow this activity. If the SA assesses that this type of external authority might be useful, they will consult with their responsible operations management element and legal advisor prior to approaching the commander.

1–6. Covering agent program philosophy

a. Proactive covering agent program. The success of ACI hinges on a proactive and aggressive covering agent program (CAP). An aggressive, well-planned CAP routinely leads to successful investigations and should be the initial focus of any ACI professional. CAP builds relationships and provides supported commanders and unit personnel a focal point for FIE threat education and reporting incidents of CI interest. A successful CAP requires the SA to be—

(1) Professional.

(2) Technically competent.

(3) Proactive.

b. Professionalism. The SA conducting CAP is normally going to be the CI community's single point of reference for the supported commander and unit personnel. Today's company and battalion commanders will be the senior Army leaders in the future. The SA's persona and demeanor can affect the trust and reliance of these leaders and a large population of the Army for years to come. Being a professional means—

(1) Being prepared.

(2) Creating a positive image of the ACI.

(3) Following through on products and deliverables.

c. Preparedness. The success of any CAP meeting is dependent on the preparation of the SA. Develop a discussion plan to use the amount of time allocated to meet with the commander or designated unit representative. Being prepared includes, but is not limited to, preparing products for the commander and their staff and being ready to provide one-on-one threat updates and foreign travel, foreign contact, and Threat Awareness and Reporting Program (TARP) briefings tailored to the unit or individual. During the CAP meeting, the SA should explain the following:

(1) ACI mission.

(2) CAP meeting objectives.

(3) What is known and unknown about the FIE threat in the AO.

(4) Threat reporting that affects the supported commander and unit's mission.

(5) Recommended CI support strategy for the commander and unit.

d. Creating a positive image. First impressions last a lifetime. The SA should present a professional appearance to represent their command and ACI. Creating a positive image for the commander and supported unit will help establish the SA's credibility. The SA should—

(1) Be in the right place at the right time and in the right uniform.

(2) Make a brief phone call to verify meeting times. Doing so demonstrates the importance, interest, and concern the SA has in conducting the meeting.

(3) Know their topics, briefly discuss each one, and avoid using intelligence jargon and acronyms.

(4) Know what support can and cannot be provided to the supported commander or unit.

(5) The SA should be familiar with the criteria that must be met for each level of support a commander or unit may request, as it will allow both parties to meet the goals of the CAP. This strengthens the working relationship because

the SA says “this is how we can do it” rather than “the support cannot be obtained” (for example, getting technical surveillance countermeasure support).

e. Following through. CAP is not about only obtaining information from the supported commander or unit. CAP is also about supporting the commander and the unit. This includes—

(1) Providing a product or deliverable (for example, a tailored threat briefing or threat reporting) when offered during a CAP meeting.

(2) Explaining that the SA should be contacted about any information concerning any foreign interest or threat to a person, unit, operation, program, technology, or information. It should be emphasized that regardless of how minor the information or implication might be, it must be reported immediately.

(3) Finding other resources that may satisfy the commander’s or unit’s request.

(4) Documenting what was agreed to be provided to the unit in a CI support plan, memorandum of agreement, or memorandum for record (MFR) and deliver a copy to the unit in person if possible.

(5) Assisting the unit when asked and within the authorities of the SA. Future investigative activities become much easier to accomplish when the unit trusts and respects the SA as their covering agent.

(6) Maintaining accurate CAP files within ACOP.

f. Technical competence. The success of CAP is largely dependent upon the SA selling the program to the supported commander and unit personnel. While interpersonal skills greatly assist in accomplishing this, the most important selling point is the SA demonstrating their technical competence. Technical competence means the SA has an in-depth knowledge of the—

(1) ACI collection requirements and FIE threat data. The SA executing a CAP must also have a thorough understanding of the CI collection requirements, supported commander’s information requirements, and FIE threat data in the supported unit’s AO, areas adjacent to the unit’s AO, and theaters and AOs where the unit will be conducting operations. The SA should have an in-depth knowledge of the following:

(a) Standing CI collection requirements.

(b) The supported commander’s critical information requirements.

(c) FIE threats to the supported unit’s personnel, operations, facilities, and installation, to include, but not limited to—

1. Methods of operations.
2. Key personnel.
3. Targeting (collection and operations).
4. Historical information.
5. FIE threats in other theaters or AOs where the supported unit may be conducting operations.
6. Current ACI collection requirements regarding the FIE threat in the AO.
7. Other intelligence or national organizations, foreign liaison elements, multinational organizations, assets, and resources within the AO that can provide information to satisfy collection requirements, corroborate threat reporting, or answer the supported commander’s information requirements.

(2) Supported unit characteristics. A good CAP also requires the SA to have intimate knowledge of the supported unit. It allows the SA to tailor the CAP specifically to support the unit’s organization and mission. This aids the supporting SA in developing a bond of inclusiveness with the commander and unit personnel. The commander, staff, and unit personnel may proactively reach out to and include the supporting SA in discussions involving security, force protection, threat issues, and unit predeployment or pre-mission planning for exercises and operations. The SA should know the following unit characteristics:

(a) Names and contact information for key leaders within the organization and subordinate elements.

(b) Unit’s mission.

(c) Subordinate commands and functions.

(d) Higher commands and functions.

(e) Theater and AOs the unit trains for deployment to.

(f) Key technologies and capabilities of the unit.

(g) Presence of cleared defense contractors supporting Army programs within the unit’s AO and name and contact information for the supporting Defense Counterintelligence and Security Agency (DCSA) CI representative.

(h) Whether or not the unit supports any Army programs in its AO, if the programs contain critical program information, and if there is a CI support plan for the programs.

(i) Whether or not the supported unit hosts foreign visits or visitors.

(j) Whether or not unit personnel conduct foreign travel or frequently attend conferences or presentations where foreigners are present.

(k) Known or suspected FIE threats to or FIE interest in specific technologies, programs, or units.

(l) Means by which the unit disseminates information to dependents of unit members.

(3) ACI mission, objectives, authorities, and jurisdiction. SAs supporting CAP should have an encyclopedic knowledge of their CI mission, objectives, authorities, and jurisdiction. They should also be able to talk and discuss these topics in an articulate and confident manner. This includes, but is not limited—

(a) ACI office, element, and unit missions.

(b) Authorities the SA has to support the command (CI support to security, force protection, AR 15–6 investigations, and other).

(c) CI advice and assistance that can be provided to the supported commander and unit.

(d) TARP and specially tailored training the SA can provide to the unit.

(e) Detailed CI threat information that can be provided to the unit leadership and to the intelligence or security officer.

g. Proactivity. CAP requires the supporting SA to be motivated and take the initiative. CAP also requires the supporting SA to be proactive in interacting with the supported unit in a manner that does not appear to be forcing the commander, staff, or unit personnel to have to contact the SA when they need support or something must be reported. Key elements that allow the SA to be proactive in their CAP support include researching, reading, and tracking.

h. Researching. Researching is critical in developing the technical competence of the SA conducting CAP. Technical competence and subject matter expertise is developed through research and use of tools that allow a rapid and efficient absorption of information from the large volume of data available to the SA. Researching includes—

(1) Establishing lanes of communication and other automated tools that automatically identify threat reporting and intelligence products associated with the supported unit's AO or mission.

(2) Including the web addresses for knowledge centers (for example, the Army Counterintelligence Center) and other websites that post daily intelligence products.

(3) Understanding current and emerging threats and FIE organization, leadership, tactics, methods of operation, targeting and collection focus, and historical activities.

(4) Identifying and routinely monitoring changes to FIE trends and patterns based on regional conflict, response to U.S. and multinational partner policies, and media focus.

i. Reading. It is imperative to mission success that every SA is knowledgeable of Army and DOD CI policy and doctrine. The supported commander and unit will probably not understand the ACI mission nor how it can support their unit. It is the supporting SA's responsibility to educate them. The SA should read as many CI-related policy, doctrine, concepts, and articles to maintain current awareness of potential changes to CI doctrine, policy, mission sets, enablers, organization, and force structure. These items will be found in the ACOP Library, through the special-agent-in-charge (SAC), or operations officer. Reading should include EO 12333; AR 381–10; AR 381–12; AR 381–20; ATP 2–22.2–1; ATP 2–22.2–2; ATP 2–22.2–3; ATP 2–22.33; JP 2–01.2; DODD 5240.02; DODM 5240.01; all DOD policy letters, instructions, and directives related to CI; and all DA policy letters, pamphlets, regulations related to CI.

j. Tracking. Keeping track of vital information is important to sustaining a successful CAP once established. A record should be kept for all CAP meetings (date, time, and location) and include any actions required prior to (for example, briefing slides or threat reporting summaries) or after the meeting (followup deliverables). All CAP reporting will be maintained in the ACOP. The supporting SA should also keep an updated CAP point of contact list for all units and organizations within their AO. The SAC or operations officer is responsible for prioritizing the ACI element's operational effort; however, the SA is responsible for explaining the importance of their assigned CAP units and organizations to the decision makers. A particular unit may not seem to be a valid target for a FIE based solely on their mission; however, the unit may have capability, technology, or persons who are especially vulnerable to targeting that may designate the unit as a potentially lucrative target. These are all factors that must be tracked by the supporting SA to keep their operational managers informed and to maintain a successful CAP.

k. Summary. The overall success of ACI begins and ends with an effective CAP. Every SA must know the threat, unit, and mission. They must be professional, technically competent, and proactive to maintain a successful CAP and provide dedicated support to their CAP customers. ACI is the primary and sometimes only defense for protecting units, installations, and individuals from FIE targeting and collection. SAs must be dedicated to integrating CAP into their unit's mission to prevent a compromise, identify espionage, or more importantly, save a life. SAs must be diligent in their CAP duties, aggressive in their efforts to identify FIE and insider threat indicators, and proactive in executing the CI mission. Successful ACI investigations and operations are not accomplished by waiting for someone to walk in and report an incident or information to ACI. SAs have to go out and get it. SAs often believe that all they need to do is brief a unit and then wait by the phone or wait for someone to walk in. That is not how it works. SAs must always be out and about, establishing themselves as a known quantity in their AO. In this way, they are much more likely to be approached by someone who has a question, who saw something, or otherwise is aware of something of possible CI interest. There is no passive CI. After a CAP meeting, SAs will maintain a record of the meeting in ACOP and will

cover who was briefed, to include numbers, any issues, what came up, and plans for later CAP meetings to be scheduled.

1–7. Counterintelligence investigative activities

a. Purpose of counterintelligence investigations. SAs need to have a thorough understanding of all investigative techniques and planning, approval processes, and legal requirements before requesting and initiating any type of CI investigative activity. A lack of understanding in any one of these areas may potentially invalidate an investigation from a prosecutorial standard and may jeopardize the ability to exploit a national security threat to the United States. ACI investigations are conducted to develop leads and gather information to—

(1) Detect espionage and other threats to national security.

(2) Detect and identify foreign intelligence collection.

(3) Determine the plans and intentions of FIE threats and other foreign adversaries that pose a threat to lives, property, or security of Army forces and technology.

(4) Neutralize foreign terrorist operations against U.S. forces.

(5) Detect and identify the insider threat.

(6) Develop information that may support a subsequent prosecution related to incidents that may constitute a national security crime as defined in AR 381–20.

(7) Determine the scope and extent of damage to national security and sensitive Army operations.

(8) Identify systemic security vulnerabilities.

b. Counterintelligence investigative objectives. CI investigations are conducted to—

(1) Identify people, organizations, and other entities engaging in incidents of CI interest or who engage in national security crimes that affect Army equities.

(2) Determine the full nature of incidents of CI interest and national security crimes within the authority and jurisdiction of ACI.

(3) Prove or disprove allegations or indications that a person or persons are engaged in national security crimes or incidents of CI interest.

(4) Prevent the loss, control, or compromise of sensitive or classified defense information and technology.

(5) Protect the security of Army personnel, information, operations, installations, networks, materiel, and technology.

(6) Acquire and preserve evidence used to support exploitation, prosecution, or any other legal proceedings or punitive measures resulting from ACI investigations.

(7) Detect and identify FIE and terrorist activities that may present a threat to Army, DOD, and national security.

c. Types of Army counterintelligence investigative activities. There are three levels of ACI investigative activities: LCAs, PIs, and FFs. ACI LCAs, PIs, and FFs are solely approved by the ACICA. Table 1–1 is a quick reference sheet for the basis of initiation, oversight, and actions associated with the different types of ACI investigative activities. ACI investigations must conform to applicable U.S. laws and DOD and DA regulations. All ACI investigative activity will be documented in ACOP. Only those with a need to know will have access to the ACOP investigative files. CI investigations must be conducted in a discreet manner, ensuring the rights and privacy of individuals involved, as well as the preservation of all investigative prerogatives. This is required to protect the rights of individuals and to preserve the security of investigative techniques.

d. Limited counterintelligence assessments. LCAs are designed to provide the ACI SA the ability to conduct limited investigative activity to explore and develop situations that do not meet the threshold for submission of a counterintelligence incident report (CIR) or when there are insufficient CI indicators to justify opening a formal ACI investigation. LCAs are intended to be short-duration efforts that quickly determine CI interest in a potential FIE threat. LCAs are relatively nonintrusive investigative techniques that allow proactive collection of information. Normally, LCAs will be conducted until a CI incident is resolved or enough information has been collected to upgrade to a PI or FF. The LCA will not be used as a basis for delaying or not submitting a local threat report in accordance with local threat reporting procedures contained in AR 381–20 or a CIR when the information is clearly reportable under AR 381–12. All reporting for the LCA will be done within ACOP.

(1) *Objectives of limited counterintelligence assessments.* The objectives of the LCA are to—

(a) Further develop information to a point where a determination can be made to open a formal investigation.

(b) Resolve the allegation or incident.

(c) Determine if there is or is not enough substantiated information to continue CI investigative activities.

(d) Joint LCAs with other agencies are unauthorized and any investigative activity will only be conducted as a joint PI or FF.

(2) *Approval and extension of limited counterintelligence assessments.* The ACICA must approve any LCA extending beyond 60 days.

(3) *Authorized activities under a limited counterintelligence assessment.* An ACI SA may conduct any investigative activities authorized under their SIA. Any investigative activity that exceeds 72 hours may be conducted as the LCA. ACI investigative elements consistent with their assigned investigative jurisdiction, mission, and function may engage in the following investigative activities when conducting the LCA:

(a) Interview of the source or sources of the report and other knowledgeable persons to establish the facts of the incident, identify all associated personnel, and identify additional leads.

(b) Records checks of local, state, and Federal law enforcement and intelligence agencies; local Army personnel, finance, security, and unit records; host nation law enforcement and intelligence files; and reviews of ACI and intelligence files and databases to fully identify any potential subject for an investigation.

(c) Collection and retention of physical evidence not requiring approval under the provisions of AR 381–10.

(d) Collection of publicly available information, if appropriate.

(e) Providing assistance to inquiries of supported commands conducted in accordance with AR 380–5 and AR 15–6 when related to matters of possible CI interest and only upon specific request from the command investigating officer.

(f) Forensic examination of Army or personally-owned computer systems, digital media, and devices with system owner's consent and ACICA approval.

(g) A subject interview (SI) can only be authorized by the ACICA. The interview of a subject under the LCA is usually approved when it appears there is no solid allegation against subject, yet there is not enough information available from LCA investigative efforts to come to a resolution of the incident without talking to subject. ACICA approves such interviews on a specific case-by-case basis.

(4) *Reporting and documentation for limited counterintelligence assessments.* Investigative activities conducted under LCA will be reported in an ACOP report of investigation (ROI) entry in ACOP using the activity generator under the running ROI as soon as possible, but no later than 5 working days after the completion of the activity. The LCA will be assigned a local case control number (LCCN) based on the ACICA numbering policy guidance. Once the LCA investigation is complete, it will be forwarded to ACICA and retired to the USAIRR.

e. Preliminary investigation. A PI is a limited investigation to determine whether a basis exists for the FF. PIs are limited in both duration and scope of investigative activity. A PI is designed to gather information and identify or verify the credibility of potential sources and subjects of CI interest. PIs will be initiated after a CIR has been submitted or a report from another agency has been received and will be opened by the ACICA.

(1) *Approval and extension of preliminary investigations.*

(a) All PIs will require an investigative plan. If the PI is a joint investigation with another agency, that agency's concurrence must be included in the investigative plan. The investigative plan aids the SA or element in maintaining the focus of a PI, ensures approved investigative activities are executed within the identified timeline, and allows for the oversight by the responsible operations management element and ACICA. Investigative plans are living documents and require review and updates throughout the course of the investigation.

(b) PIs are initially authorized for up to 180 days and may be extended for up to an additional 180 days upon approval by the ACICA. A PI continuation requires the SA or element to submit a field office (FO) continuation request to the ACICA. Continuation requests must address—

1. Reasons why the PI could not or did not address the original allegations during the first 6 months (for example, delay in another agency's investigative activities, unavailability of subject or source due to deployment, resource limitations, or a higher priority case).
2. Specific investigative actions anticipated or planned and the purpose (for example, interview of former supervisor who may provide information corroborating subject's placement and access, interview of critical Source previously unavailable due to deployment, or other).
3. Details of significant investigative results obtained up to the submission of the continuation request.
4. Anticipated timeline and end-state of the investigation.

(c) The investigating SA or element will submit requests for PI continuations no later than 30 days prior to the scheduled expiration of the PI.

(2) *Authorized activities under a preliminary investigation.* PIs may include any of those actions authorized by SIA, as well as SIs and pretext SIs (with prior approval of the ACICA) and bank letters for financial institutions. The following special investigative techniques are authorized during PIs in accordance with DODM 5240.01, AR 381–10, and AR 381–20:

(a) Procedure 5 (electronic surveillance, but only when requesting the trespasser exception, as outlined in DODM 5240.01 and AR 381–10).

(b) Procedure 6 (concealed monitoring).
(c) Procedure 9 (physical surveillance, including support to FBI-approved surveillance).
(d) Special techniques, as specified in AR 381–20.

Note. Certain other investigative techniques may be authorized, such as an exception to Procedure 5 to support CI cyber PIs.

(3) *Reporting and documentation for preliminary investigations.* All investigative activities will be documented in the current automated ACI investigative program of record, ACOP (see chap 5 for more information on CI reporting).

f. Full-field investigation. FF is authorized when there are specific and distinct facts giving reason to believe that persons who ACI has jurisdiction over are involved in an act that may constitute a threat to national security.

(1) *Approval and extension of full-field investigations.* The ACICA is the authority for opening or terminating FFs. All FFs require an investigative plan.

(2) *Authorized activities under a full-field investigation.* SAs conducting the FF may incorporate all lawful investigative techniques available to ACI authorized for PIs. The following additional special investigative techniques are authorized under FFs with appropriate approvals:

(a) Procedure 5 (electronic surveillance).
(b) Procedure 7 (physical searches).
(c) Procedure 8 (mail searches and examination).

(3) *Reporting and documentation for full-field investigations.* The FF may be initiated by the ACICA, usually after the submission of a CIR or supporting information indicative of the need for the FF. All investigative activities will be documented in ACOP.

Table 1–1
Counterintelligence investigations quick reference sheet

	Limited counterintelligence assessment	**Preliminary investigation**	**Full-field investigation**
Predication	Receipt of information indicating a potential CI threat to the Army or DOD	CIR, report from another agency, or other information with specific facts giving reason to believe a CI threat involving a FIE may exist	CIR, report from another agency, or other information with specific facts giving reason to believe a CI threat incident involving a FIE has occurred
Purpose	To facilitate proactive collection of information concerning potential threats to the Army, DOD, and national security; the objective is to collect information or matters of CI interest in accordance with AR 381–12	To determine if an incident under ACI investigative authority as specified in AR 381–12 may have occurred	To determine if an incident under ACI investigative authority as specified in AR 381–12 has occurred
Authority to open	ACICA	ACICA	ACICA
Oversight	ACICA	ACICA	ACICA
Duration	60 days, investigative activity upon submission of CIR and disposition determination	6 months	No limitations
Extension	Up to 60 days with written justification and ACICA approval	Up to 180 days upon ACICA approval	No limitations
Investigative activities	1. Interview of the source or sources of the report and other knowledgeable persons to establish the facts of the incident, identify all associated personnel, and identify additional leads	Investigative activities listed under LCA and SIs and bank letters for financial institutions The following additional special investigative techniques	All lawful investigative techniques available to ACI listed under LCA and PI may be used

Table 1–1
Counterintelligence investigations quick reference sheet—Continued

	2. Records checks of local, state, and Federal law enforcement and intelligence agencies; local Army personnel, finance, security, and unit records; host nation law enforcement and intelligence files; and reviews of ACI and intelligence files and databases to fully identify any potential subject for an investigation 3. Collection and retention of physical evidence not requiring approval under the provisions of AR 381–10 4. Collection of publicly available information, if appropriate 5. Providing assistance to inquiries of supported commands conducted in accordance with AR 380–5 and AR 15–6 when related to matters of possible CI interest and only upon specific request from the command investigating officer 6. Forensic examination of Army or personally-owned computer systems, digital media, and devices with system owner's consent and ACICA approval 7. SIs, which require legal review and ACICA approval	are authorized with the required approval: Procedure 5 (electronic surveillance, but only when requesting the trespasser exception, as outlined in DODM 5240.01 and AR 381–10) Procedure 6 (concealed monitoring) Procedure 9 (physical surveillance, including support to FBI-approved surveillance) Special techniques, as specified in AR 381–20	The following additional special investigative techniques are authorized with the required approval: Procedure 5 (electronic surveillance) Procedure 7 (physical searches) Procedure 8 (mail searches and examination)

g. Personal subject versus incident investigations. A personal subject investigation occurs when an allegation is made that an identifiable person has committed a known or suspected act. An incident investigation occurs when there is evidence that a known or suspected act has occurred, but the perpetrators cannot be initially identified. When the subject is not known, an Army incident investigation will be conducted, in coordination with other CI investigative agencies as appropriate, until the subject is identified. If the subject is under ACI jurisdiction, it will continue as a personal subject investigation. If not, the investigation will be referred to the appropriate agency.

h. Joint investigations. In cases where there is joint, parallel, or concurrent jurisdiction and valid ACI equities are evident, every effort will be made to pursue a joint investigation with the other agency or agencies involved. ACI may conduct joint investigations with other DOD, U.S. Government, or host nation investigative agencies. Regardless of which organization is designated as the lead investigating agency, ACI will always participate to support Army equities. A joint investigation only applies to PI and FF and is only authorized by the ACICA.

i. Joint investigations with U.S. Army Criminal Investigation Command. Because the Army divides investigative responsibility for CI matters from general criminal investigations, there are a number of special circumstances involving parallel and joint jurisdiction of crimes with national security implications.

(1) ACI and U.S. Army Criminal Investigation Command (USACIDC) will jointly investigate crimes and incidents listed in paragraphs 1–8*i*(1)(*a*) through 1–8*i*(1)(*l*), with USACIDC as the lead agency until FIE involvement is indicated, at which point ACI will assume the role of lead investigating agency.

(2) ACI and USACIDC will conduct parallel investigations of computer intrusions. USACIDC will be the lead agency until FIE involvement is indicated, at which point ACI will assume the role of lead investigating agency.

Potential violations of the Intelligence Identities Protection Act of 1982 (see 50 USC Chapter 44) will be considered on a case-by-case basis with USACIDC usually taking the lead, unless FIE involvement is identified. The responsible operations management element and ACICA should be immediately notified of any potential jurisdictional disputes with the USACIDC. If required, the ACICA can assist in resolving jurisdictional disputes at the headquarters level.

j. Joint investigations with the Federal Bureau of Investigation. ACI should request to be a joint investigating partner for any FBI investigation containing ACI equities. This should occur at all levels to ensure ACI has an appropriate level of visibility and involvement in the investigations. These efforts begin at the local level where the SAs coordinate with their FBI counterparts to gain concurrence for a joint investigation when ACI equities exist. Preferably, concurrence for a joint investigation should be established by the FBI providing Army an FBI letterhead memorandum (LHM). If this is not possible, SAs can submit an MFR documenting the agreement through technical authority channels to the ACICA. The MFR must note the date, location, and identity of the FBI supervisor authorizing the joint investigation. The LHM or MFR will become part of the official case file in ACOP and become part of the ROI. If the FBI field element expresses reluctance to acknowledge Army equities in an investigation and refuses a joint investigation, the issue will be addressed by the ACICA.

k. Federal Bureau of Investigation release or declination of investigative jurisdiction. The FBI does not have the authority to release investigative jurisdiction on a civilian subject suspected of a national security crime to ACI. This authority resides with the Department of Justice and is rarely exercised. The FBI may open joint investigations with ACI on civilian subjects and then authorize Army agents to conduct the majority of the investigative acts with little oversight from the FBI. The FBI provides this authorization in an LHM; however, the SA will submit a MFR documenting the agreement through technical authority channels to the ACICA. The MFR will include the date, location, identity of the FBI supervisor authorizing ACI investigative activities. The MFR will also identify other persons present at the meeting who witnessed the granting of this authority. ACI investigative activities will be coordinated through technical channels to gain approval from the appropriate approval authority based upon the type of requested investigative activity. ACI will provide investigative updates to their FBI counterparts and immediately notify the FBI when significant information is developed. The memorandum of agreement between the U.S. Attorney General and the Secretary of Defense, "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation," dated 5 April 1979 (also called the Delimitations Agreement, available in the ACOP library), stipulates that in situations where the FBI declines to open an investigation, the DOD CI services can open and pursue a unilateral case to establish the factual basis for required or authorized administrative action and to protect the security of DOD personnel, information, activities, and installations.

l. Reporting in joint investigations. U.S. Government agencies are independent of one another and operate under different statutory authority, EOs, and procedures; however, in court, the U.S. Government is viewed as a single entity. Reports and case files of all investigative agencies involved in an investigation are subject to discovery and use in court. Because of this, only one report of an investigative activity is generated. Multiple or duplicate reports, especially if they conflict in any way can undermine the prosecution's efforts. Reporting procedures and agreements should be addressed in the initial joint investigative plan.

1–8. Standing investigative authority and jurisdiction

CI SIA provides ACI the mission to conduct limited investigative activities prior to the submission of a CIR. Jurisdiction defines those persons, incidents, and national security crimes that fall under ACI authority and are subject to ACI investigative activities.

a. Standing investigative authority.

(1) SIA is a tool that enhances the SA's ability to respond to initial source reporting and develop the details of reportable incidents. SIA extends beyond the basic collection of the minimal facts needed to articulate a reportable incident in a CIR. When fully executed within the parameters established by the ACICA, SIA allows the SA to collect and clearly articulate relevant facts pertaining to an incident of CI interest. AR 381–20 provides the authority for SAs to develop as much of the reported incident as possible within 72 hours of receipt of the reportable information. SIA includes—

(a) Identifying indicators of espionage or terrorism involvement.

(b) Reviewing computer and network system logs to conduct local, military, and host nation records checks.

(c) Putting allegations into context.

(d) Fully identifying subjects.

(2) The appropriate implementation of SIA and accurately communicating those findings can often be the difference between simply submitting a CIR in ACOP and the opportunity to conduct a larger CI investigation or exploit a situation operationally. SIA should focus on—

(a) Developing a methodical approach.

(b) Collecting detailed information.
(c) Identifying the best source.
(d) Producing the best report.
(e) Requesting extended SIA when needed.

b. Developing a methodical approach. Upon receipt of initial source reporting and initiating activities under SIA, SAs should immediately begin analyzing the information to determine if they have a reportable incident. This process does not need to be formalized as it is when developing an investigative plan. SAs should develop a methodical approach to gathering facts and conducting only the interviews and records checks necessary to accurately capture the details of an allegation or incident. Developing a methodical approach early in the process not only helps identify logical leads under SIA, it also helps keep the SA focused. Deliberate planning and logical sequencing of investigative activities serves as the framework for more comprehensive investigative planning when an investigation is opened.

c. Collecting detailed information. One of the most important factors for the ACICA to consider in making case determinations is the context of the reported allegations. More details assist in the case determination process. Case determinations are made considering a number of factors, but ultimately all stem from the clarity, details, and context of the information that is initially reported.

d. Identifying the best source. SAs can and should use SIA to identify and interview the best source or sources of information when time permits and as often as logistically practical. Interviewing best sources is still the best way to put what was observed, overheard, understood, or believed to be true into an accurate context. It helps SAs stay focused on gathering facts and reduces opportunities for other persons with indirect knowledge of an incident from reporting opinions and speculation. This is especially important when the initial allegations involve an individual under Army jurisdiction that is reportedly involved in terrorism or is in direct contact with a FIE.

e. Producing the best report. SIA is more than just conducting records checks necessary to identify subjects and other persons involved. SIA is the authority that provides the legal justification to conduct preliminary activities for gathering enough pertinent information to also put the incidents into relevant context. While all CI professionals recognize the need for rapid reporting, SIA should be fully utilized to submit the best report within the 72-hour parameter.

f. Requesting extended standing investigative authority.

(1) In some cases, the SA may recognize the need for additional records checks, interviews, or database checks by analysts to confirm multiple indicators or establish probability that the incident or allegation is of CI interest. These situations highlight the importance of utilizing SIA to allow ACI to respond appropriately and fully develop information that allows the ACICA to make informed decisions using the best information available. However, due to a lack of time to execute further SIA, the SA submits the report within the 72-hour requirement. Instead of submitting an incomplete report, the SA can request extended SIA from the ACICA. The extension request should include the facts that are known and the plan for obtaining additional details. The ACICA will consider the totality of the situation and extend SIA and reporting requirements, provide investigative direction, or direct reporting based on available information. If the ACICA extends SIA, any such extension is annotated in the subsequent CIR, if written.

(2) AR 381–20 establishes the ACICA as the final authority on determining whether the circumstances of a CI incident merit the initiation of investigative activity. Fully exercising SIA allows SAs to make sound and informed recommendations and ultimately serves as the cornerstone for ACICA case determinations and the CI community's collective ability to protect Army equities.

g. Jurisdiction.

(1) ACI jurisdiction includes both the investigation of known or suspected criminal acts (defined in the USC and UCMJ) and incidents identified in AR 381–20 or a person or persons suspected of being involved in those acts or incidents. To establish jurisdiction, the SA must determine whether the incident, the subject, or both are under ACI investigative jurisdiction. The answers to these questions will determine what kind of investigative jurisdiction ACI has concerning the matter and determine if an investigation is conducted unilaterally, jointly, with other agencies, or if it must be passed to another agency for resolution.

(2) Jurisdiction over the person refers to the persons known, alleged, or suspected of involvement in an incident of CI interest or committing a national security crime. ACI can then focus investigative efforts to confirm or deny their involvement.

(3) Table 1–2 identifies persons under ACI jurisdiction. If investigative activity is necessary to develop evidence to determine whether the act of a retired or reserve component subject occurred while the person was on active duty, ACI may review existing Army records and interview persons who knew or had contact with the subject while they were on active duty. This investigative activity must be coordinated with the FBI in writing before it is undertaken.

Table 1–2
Persons under counterintelligence jurisdiction

Within the United States[1]	Outside the United States[2]
U.S. Army personnel on active duty.	U.S. Army personnel on active duty and their Family members.
Retired U.S. Army military personnel when the acts under investigation took place while the individual was on active duty.	Current DA civilian employees and their Family members.
Active and inactive members of the U.S. Army Reserve Components (U.S. Army Reserve and U.S. Army National Guard) when the acts under investigation took place while the individual was in active duty status.	U.S. Army contractors and their family members, subject to coordination with the FBI, Central Intelligence Agency (CIA), and host government agencies, as required.
Active, retired, and reserve personnel of the other Services when DOD has assigned CI investigative responsibility to ACI.	Retired U.S. Army personnel, U.S. Army Reserve and U.S. Army National Guard personnel, and other U.S. persons who permanently reside overseas, subject to coordination with the FBI, CIA, and host government agencies.
	Foreign nationals who are applicants for U.S. Army employment, current U.S. Army employees and their Family members, and former U.S. Army employees.
	Foreign nationals not affiliated with the U.S. Army in a country in which agreements preexist, subject to coordination with the CIA and agreements with the FBI, other DOD intelligence components, and host nation governments. These investigations are under the auspices of international and multinational agreements and are bilateral investigations.
	Foreign nationals not affiliated with the U.S. Army in geographic areas where U.S. Army is conducting contingency operations and there is no functioning government, subject to coordination with the CIA and agreements with the FBI and other DOD intelligence components.
	Active, retired, and reserve personnel of the other services, DOD civilian employees and their Family members, and DOD foreign national employees and their family members, where DOD has assigned CI investigative responsibility to U.S. Army.

Notes.
[1] ACI jurisdiction within the United States and its territories and protectorates.
[2] ACI jurisdiction outside the United States, unless responsibility is otherwise assigned by U.S. law, EO, or agreement with the host government.

h. Counterintelligence jurisdiction for incidents and crimes. In accordance with EO 12333, DOD 5240.01–R, DODD 5240.02, and AR 381–20, ACI has investigative authority concerning criminal statutes under 18 USC and corresponding criminal articles in the UCMJ or incidents of CI interest, if the subject or potential subject meets the CI investigative jurisdiction (see para 1–7*i* for CI jurisdiction of crimes and incidents).

i. Types of counterintelligence jurisdiction. There are various categories of jurisdiction for ACI that depend on the legal status of the subject and the type of crime or incident involved. The categories of jurisdiction dictate the level of CI participation in the investigation. The categories of CI jurisdiction are primary, parallel, and joint.

(1) *Primary jurisdiction.* When both the subject and the incident or crime fall under the purview of an investigative agency, that agency has primary jurisdiction and the authority to pursue the investigation unilaterally. When ACI has primary jurisdiction, the investigation may be conducted jointly with other agencies, when and if appropriate; however, ACI will be the lead agency in planning and conducting the investigation. ACI is the primary authority for investigating national security crimes and incidents of CI interest for—

(a) Sedition.
(b) Aiding the enemy by providing intelligence to the enemy.
(c) Spying.
(d) Espionage.
(e) Subversion.

(f) Treason.

(g) International terrorist organization activities or materiel support to international terrorist organizations and associated organizations or persons. Terrorist organizations are specified in the Operational Planning List published annually by the DA G–2.

(h) Unreported contact with foreign government personnel or groups involved in intelligence activities against the U.S., international terrorism, or those making unauthorized requests for classified or sensitive unclassified information.

(i) Unauthorized or intentional disclosure of classified information or material, especially when other indicators of espionage are identified or there are acts which are consistent with known foreign intelligence or terrorist methods. Investigations are conducted to determine if the incident involves foreign intelligence activity or international terrorism. SAs may also act to secure classified material and to determine if the actions of the subject were an act of omission or commission.

(j) Matters developed as a result of intelligence polygraph examination that require inquiry as specified in AR 381–20.

(k) Military personnel in any location or DA civilian employees employed overseas who perform unofficial travel to those countries designated on the Operational Planning List, who have unauthorized contact with official representatives of foreign countries, or who contact or visit foreign diplomatic facilities without authorization.

(l) Attempts by authorized users of classified information systems to gain access to information or data for which they are not authorized access (also referred to as insider threat).

(2) *Parallel jurisdiction.* ACI may investigate the following incidents simultaneously with other agencies, organizations, or commands whose investigative objectives may differ from the objectives of ACI:

(a) Sabotage conducted by or on behalf of a foreign entity or an international terrorist organization.

(b) Unauthorized removal of classified material or possession of classified material in unauthorized places.

(c) Known, suspected, or attempted intrusions into classified or unclassified information systems when foreign involvement has not been ruled out.

(d) Special category absentees. Personnel in this category include those absent without leave, deserters, defectors, and military absentees known to have gone to a foreign country. SAs will conduct investigations of the circumstances surrounding the absences of special category absentees using the guidelines in AR 381–20.

(e) DA military and civilian personnel who are detained or captured by a government, group, or adversary with interests inimical to those of the U.S. When directed by proper authority, such personnel will be debriefed upon return to U.S. control in accordance with AR 381–20.

(f) Attempted or actual suicide or suspicious death of a DA member if they have an intelligence background, were assigned to a special mission unit, or had access to classified information within the year preceding the incident; or where there are indications of foreign intelligence, foreign adversary, or terrorist involvement.

Note. As an example of parallel jurisdiction, ACI may investigate for the presence of threats to national security, the involvement of a foreign power, or the involvement of a person under ACI investigative jurisdiction, while other organizations may focus on the criminal aspects of an incident.

(3) *Joint jurisdiction.* ACI may investigate the following activities with other agencies or organizations, with their agreement, for the purpose of detecting and identifying national security issues within ACI investigative jurisdiction:

(a) Joint jurisdiction for crimes and incidents.

(b) Incidents associated with the national security crimes listed in table 1–2, involving other disaffiliated U.S. persons when there is a reasonable belief of a threat to the Army. ACI elements will forward requests for joint investigations to the ACICA for appropriate legal review and validation.

(c) Suspected or actual unauthorized acquisition or illegal diversion of militarily critical technology, research and development information, or information concerning an Army acquisition program. If appropriate, CI will ensure that those Federal agencies with law enforcement jurisdiction identified in AR 381–20 are notified. CI personnel will ensure that these agencies are fully knowledgeable of DOD critical technologies and the imperative to protect them from foreign exploitation. CI will either monitor the progress of the case, provide assistance to the investigating agency, or participate in joint investigations at the invitation of the investigating agency.

(4) *Joint jurisdiction when Army counterintelligence is not the lead agency.* Joint jurisdiction may exist in situations where ACI is not the lead investigative agency. This most often occurs when the lead investigative agency has primary jurisdiction over both the subject and the incident and ACI only has jurisdiction over the incident. ACI is involved in investigating these incidents when the subject's activities represent a potential threat to Army equities that involves DA Civilians, contractors, and Reservists. However, the lead investigative agency or ACI can request a joint investigation to protect threats against Army equities.

Chapter 2
Counterintelligence Investigations

Section I

Counterintelligence Investigative Process

The CI investigative process is a logical and methodical approach to conducting CI investigations. The CI investigative process is not cyclic. The process has a beginning and an end. However, during the CI investigative process other operational branches may be identified that lead to or initiate other CI activities. For example, information developed during a CI investigation may initiate a CI collection activity or operation.

2–1. Phases of the counterintelligence investigative process

a. The CI investigative process has four phases that generally occur sequentially. The four phases of the CI investigative process are—

(1) Lead development.
(2) Planning and approval.
(3) Investigative activities.
(4) Case disposition.

b. Although the CI investigative process has four phases, the phases may be repeated due to developments that occur during the investigation. For example, additional leads may be identified during the investigative activities phase, which may require the SA to seek additional approvals to conduct additional investigative activities.

2–2. Lead development

Lead development is the most important part of the CI investigative process. All CI investigations are initiated from a lead. CI leads normally come from someone seeing or hearing something or as a referral from another investigative agency. However, personnel often do not understand what types of incidents are of interest to CI nor are they fully aware of their reporting obligations under the provisions of AR 381–12. Lead development requires the SA to be proactive in educating Soldiers, civilians, and contractors on incidents of CI interest, as well as indicators of espionage and insider and other threats.

a. Lead development sources. ACI investigations are based upon leads developed by SAs. The CAP is the primary lead generation tool available to SAs since it helps to inform military members and employees of the CI mission, as well as what and where to report CI incidents. Other military and civilian security, law enforcement, and intelligence agencies may also provide leads to SAs. The primary sources of lead development are walk-in sources, TARP, referrals and sensitive reporting, polygraph failures or refusals, and SA knowledge of a reportable incident.

b. Walk-in sources. A walk-in source is the most typical lead for reportable incidents of CI interest. A walk-in source is an individual who contacts ACI to volunteer information that is believed to be of intelligence value. Many CIRs come from walk-in sources that have no previous relationship or reporting history with ACI. SAs have the authority to interview any individual who potentially possesses information of an intelligence or CI nature (see chap 4 for more information on walk-in source interviews).

Note. A walk-in source will never be turned away. If the initial contact is made by a phone or web-based message, all efforts will be made to meet the source in person within 24 hours of receipt of message.

c. Threat Awareness and Reporting Program. CI relies on the TARP to identify systemic or personnel issues and to identify other anomalies or inconsistencies that may indicate a vulnerability or incident of CI interest. CI operations identify vulnerabilities to U.S. forces resulting in countermeasure recommendations that negate, mitigate, neutralize, or exploit FIE targeting and collection activities and disrupt their ability to target and collect against U.S. forces. Proactive and aggressive CI operations generally cause threat collection elements to shift targeting priorities resulting in degraded threat operations and decreased threat activities directed towards U.S. and multinational forces.

(1) AR 381–12 TARP provisions require all Army personnel, both civilian and military, to report potential incidents of CI interest to their supporting or closest CI element. This program mandates annual threat awareness training. CI training of all personnel is subject to inspection under both the Inspector General's office and the command inspection program.

(2) The TARP helps identify potential incidents of CI interest and is a lead development enabler for CI investigations in response to suspected national security crimes under ACI jurisdiction. Threat awareness briefings should be given by qualified SAs whenever possible and, at a minimum, contain—

(a) FIE collection methods of operation.

(b) National security crimes under CI authority.

(c) Types of situations and incidents considered matters of CI interest that should be reported (see AR 381–12 for specific guidance).

(d) Indicators of espionage and insider threats.

(3) Many TARP walk-in sources report information because they received a TARP brief that educated them on techniques and methods used by FIEs and other threats. SAs conducting CAP should be the focal point for providing TARP briefings; however, the unit G–2/S–2 or G–2X/S–2X (brigade and above) may do so when there are no SAs available. The G–3/S–3 is responsible for the supported unit's training mission and must coordinate with the G–2/S–2 or G–2X/S–2X to ensure TARP is incorporated into the unit's training schedule.

(4) TARP briefings should be tailored to the operational environment and unit's mission. Information obtained during CAP meetings should be used to tailor TARP training to a specific unit. TARP briefings should also include issues, such as—

(a) Identifying and presenting potential threats from local employee persons in contingency and combat operations.

(b) Identifying and presenting potential threats from local personnel employed or contracted in support of regular or predeployment training exercises.

(c) Lessons learned from threat and vulnerability assessments, CI activities (investigations, operations, and collection), analytical products, and previously reported threat information.

d. Referrals and sensitive reporting. Investigative leads may also be developed from sensitive reporting and referrals from other agencies (for example, the FBI and USACIDC). These leads may come from local (SA counterparts) or agency headquarters level. Information of CI interest that is obtained at the local level can be either verbal or in writing. If the information provided requires the submission of a CIR, it is preferable to obtain the information in the form of an LHM or official report. Sensitive reporting at the headquarters level may include the following:

(1) FBI—Section 811 of the Intelligence Authorization Act of 1995 (Public Law (PL) 103–359) requires notification and coordination between the FBI and other executive departments, to include DOD, of investigations of espionage.

(2) Other agency referrals—SAs or elements may receive information from other Government agencies concerning an allegation or incident that is within the jurisdiction of ACI.

(3) Financial Crimes Enforcement Network (FinCEN), Department of the Treasury—generates suspicious activity reports (SARs) when they become aware of known and suspected criminal offenses at specified thresholds under the Bank Secrecy Act (BSA) of 1970 (see PL 91–508).

e. Polygraph failures or refusals. Investigative leads may also result from unresolved or failure or refusal of counterintelligence scope polygraph examinations (CSPEs). The Army Intelligence Polygraph Program (AIPP) will review all forms, documentation, and results concerning inconclusive results, failures, or refusals of CSPEs. AIPP Branch will provide a referral letter with pertinent information and results to the appropriate authorities. The results of all unresolved CSPEs of Army members, DA Civilians, and contractors will be referred to the ACICA. These referrals pertain to individuals who refuse to undergo a CSPE or fail to complete a CSPE and test results evaluated as "significant response" or "no opinion." A "no significant response" CSPE may be referred when significant admissions concerning CI issues are made by the examinee. Investigations resulting from CSPEs have special considerations especially in investigative planning (see para 2–13 for additional guidance).

(1) Individuals who require a CSPE for indoctrination into special access programs (SAPs) or for entry or duty at National Security Agency (NSA) facilities are not suspected of wrongdoing. Inconclusive results, failures, or refusals are not the sole basis for adverse action. Generally, there are three primary reasons for someone to fail or refuse an exam—

(a) Failure due to security violations—improper handling of classified information (for example, took it home and told or gave it to family, friends, and so forth).

(b) Refusal—a legitimate desire (due to health and so forth) not to take the examination.

(c) Refusal—a bad experience with the examination or the examiner.

(2) The objective of the investigation is to determine if the subject's inconclusive result or failure or refusal of the CSPE is related to any CI issues. If sufficient CI indicators are identified, the ACICA will assign the appropriate category to the investigation. This determination is made by the ACICA.

(3) Investigations resulting from CSPEs have special considerations especially in investigative planning. Results of all uncompleted and unsuccessfully completed CSPEs of Army members, DA Civilians, and DA civilian contractors will be referred to the ACICA. These referrals pertain to individuals who refuse to undergo a CSPE or fail to complete a CSPE and those test results are evaluated as "deception indicated" or "inconclusive." The ACICA may

also refer a CSPE where the subject's examination was evaluated "no deception indicated; however, significant admissions concerning CI issues were made by the SUBJECT." In accordance with DA policy, ACI will not investigate an individual based solely on inconclusive CSPE results (see para 2–13 for additional guidance).

f. Special agent knowledge of a reportable incident. During official and nonofficial contact with other Army service members or employees, SAs may also gain knowledge concerning an allegation or incident of CI interest. Army service members or employees may observe or hear something that does not seem suspicious or out of the ordinary to them and may relay that information to the SA during a conversation. Information that initially seems innocuous may develop into an indicator or lead that may require further investigation. SAs may also observe or overhear discussions during assistance or liaison meetings that may be the basis for submitting a CIR. This could include identification of indicators of espionage, insider threats, or systemic procedures and vulnerabilities that violate regulations for protecting, handling, or safeguarding sensitive or classified information.

2–3. Initial reporting

a. Initial reports are entered into ACOP and forwarded concurrently to the ACICA, responsible Army theater CI coordinating authority (for situational awareness only), and appropriate members of the CI chain of command. If the SA is unsure if the reported incident meets the criteria of reportable matters as specified in AR 381–12, a report will be submitted to the ACICA for a determination.

b. The investigating SA obtains as much information as possible from the initial source, including—

(1) Date.

(2) Time and duration of incident.

(3) Locations.

(4) Suspected acts.

(5) Conversational details.

(6) Any further pertinent information.

(7) Personal information (such as a first and last name and unit of assignment or employment location) concerning—

(a) Known additional sources of the reported incident.

(b) Witnesses to the incident.

(c) Subjects or potential subjects involved in the incident.

(d) The source of the information.

(e) Physical descriptions of unidentified witnesses to the incident or subjects or potential subjects involved in the incident.

2–4. Field adjudication

Absent of directive or other guidance from higher, the SA will not "field adjudicate." The SA should first determine if the incident is reportable in accordance with AR 381–12. If the incident meets a threshold for a reportable incident, CI agents will produce a CIR in ACOP and provide recommendations for further investigative activities in the agent notes section of the report. If the SA is not sure if the incident meets a threshold for a reportable incident, a CIR should be submitted to the ACICA for a case determination.

2–5. Counterintelligence incident reports

a. Purpose. CIRs are used to report specific allegations that individuals have committed, are committing, or plan to commit national security crimes, to include terrorism. CIRs should be submitted no later than 72 hours after receipt of reportable information from a complainant or source. In combat or contingency operations environments or other exigent circumstances when it is not possible to meet the 72-hour requirement, SAs will inform the ACICA the report will be late and the reasons why. Exceptions to the time limit for SIA can be provided by the ACICA, if applicable.

b. Timeliness. SAs will make every reasonable attempt to fully identify and interview the original or best source of information within the allotted 72 hours. If additional time is needed to obtain the minimum information required to properly adjudicate the reported incident, ACI SAs will request extended SIA from the ACICA. A timely but incomplete report is more useful than a complete report may lead ACICA to mistakenly open or terminate a reported incident when an investigation is appropriate or open an investigation when one isn't warranted. Request for extended SIA should be submitted as soon as the responsible ACI SA realizes more time may be required.

2–6. Local threat reporting

Reported information, which may be indicative of a potential terrorist threat to DOD, will be immediately shared with agencies with a counterterrorism or force protection mission. In these instances, ACI elements will use local threat

reporting to immediately notify the supported unit, command, or installation to negate or mitigate the threat and follow through with the submission of the CIR within the 72-hour requirement. See chapter 5 for more information on CI reporting requirements and chapter 6 for the CIR format. See AR 381–20 for more information on local threat reporting.

Section II

Counterintelligence Incident Report Dispositions

Once a CIR is submitted, it will be reviewed by the ACICA. CIRs are the primary basis for initiating a CI investigative activity; however, the CIR may also result in no investigative activity or delay an investigative case status determination due to incomplete information or coordination with other agencies. Examples of CIR dispositions are delayed case determination, returned with guidance or comment, open (with different subcategories), merged, or no case.

2–7. Delayed case determination

a. Delayed case determination will be used with CIRs when coordination is required with other investigative agencies to determine if a joint investigation will be pursued. It is not used as a venue to conduct investigative activities.

b. The term "abeyance" has been utilized incorrectly in the past to allow subordinate CI field elements to coordinate CIR-related actions or conduct specific investigative activities to help in making a case determination. Abeyance, as applicable to CIRs, has been replaced with delayed case determination. Abeyance will only be used with open CI investigations and it means all investigative activity is temporarily suspended by the directing authority for a specified time period.

2–8. Returned with guidance or comment

Returned with guidance or comment is a CIR disposition for CIRs that do not contain enough relevant facts to make a case determination. This term is used when further analysis or specific investigative activity is required to facilitate a case determination. A CIR returned with guidance or comment will include ACICA guidance for additional interviews or records checks. A CIR returned with guidance or comment will include an agreed upon suspense, not to exceed 10 calendar days. A revised or corrected CIR will be provided upon completion of the directed investigative activity or activities.

2–9. Foreign counterintelligence activity operational interest

CIRs which identify probable espionage indicators or FIE involvement maybe fall under the purview of the foreign counterintelligence activity for operational interest. In this case, the CIR will be categorized as delayed case disposition, special circumstances.

2–10. Open

A CIR is the primary basis for opening an ACI investigation. A CIR may be designated as open if it contains information that a credible allegation or other information of CI interest has occurred and ACI has unilateral jurisdiction over both the potential crime and the person. An ACI investigation may also be opened when ACI has jurisdiction over the person or crime or where an identifiable Army equity is present and ACI should pursue a joint investigation with another agency that has or shares jurisdiction. There are several subcategories for an open CIR, including—

a. Open FF—the CIR is the basis for approving the conduct of a CI FF. The ACICA can designate a CIR as open/FF.

b. Open LCA—the CIR is the basis for approving the conduct of the LCA. The ACICA can designate a CIR as a CIR as open/LCA.

c. Open PI—the CIR is the basis for approving the conduct of a CI PI. The ACICA can designate a CIR as open/PI.

d. Open/terminated—a CIR is designated open/terminated after SAs pursue logical investigative activities authorized under SIA and the ACICA determines that the allegations are resolved or that the incident is not under ACI jurisdiction. To qualify as open/terminated the information presented in the CIR must be reportable in accordance with AR 381–12, but the expectation is that no further investigative activity will be required or authorized. If the subject or incident is not under ACI jurisdiction, the SA will recommend open/terminated with a summary of information (LHM) and letter of transmittal transmitted to the relevant investigative agency. In joint investigations with the FBI, the FBI may terminate the investigation. If there are still unresolved U.S. Army equities, the responsible ACICA will request that the FBI permit the ACI element to continue a unilateral investigation of the incident.

2–11. Merged
If an incident reported in a CIR is related to a similar incident in an open investigation, the CIR can be merged with the open LCA or above investigation based on concurrence with the ACICA. Merging CIRs is very rare.

2–12. No case
The term "no case" is utilized when a CIR of no reporting relevance has been submitted. In many cases, this issue can be mitigated and better resolved by the ACICA authorizing extended SIA to further acquire the initial information required for possible CIR publication. A CIR that is eventually no-cased will include a memorandum from the ACICA, outlining the reasons for the returned CIR (usually lack of reportable information, as outlined in AR 381–12).

Section III

Planning and Approval
Due to the legal complexities involved in CI investigations, investigative planning has to be meticulous to maintain the legal integrity of the case or to compartmentalize the knowledge of the incident allowing for potential exploitation of the incident.

2–13. Investigative planning
Investigative planning is critical to the overall conduct of the investigation. Planning ensures a CI investigation is conducted in a logical and methodical manner and within the guidelines of applicable U.S. laws and DA and DOD regulations. CI investigative planning considerations include identifying the following:

a. Investigative objectives. Investigative objectives should be targeted towards confirming, refuting, or mitigating allegations and suspicions regarding the subject's potential involvement with a FIE.

b. Elements of the crime. Understanding and staying focused on the elements of the crime originally alleged can avoid distraction. Periodically reviewing the elements of the crime and ensuring that all investigative actions are tied to establishing one or more of them is a good technique. If the SA cannot articulate how an investigative act will help prove one of the elements of the crime, the investigative act may not be required. During the course of a CI investigation, derogatory information may be developed that affects the subject's suitability to hold a security clearance; however, not all suitability information necessarily satisfies an element of the crime.

c. Identifying the best sources. SAs should identify the persons who possess the greatest knowledge regarding the subjects or incident under investigation. For example, rarely is it necessary to interview all of the subject's coworkers to establish a daily routine, behavior, office layout, or other pertinent investigative details. The subject's supervisor may be able to identify coworkers who work or socialize closely with the subject that may be the best sources to further develop information concerning an allegation, incident, or suspected crime or the subject.

d. Using the least intrusive to the most intrusive means. ACI investigative activities are conducted using the least intrusive means that will accomplish the objective. This protects the civil and privacy rights of those being investigated. Intrusive means are the most specialized and resource-intensive of the tactics and techniques available and should be used only when required. The more intrusive a required technique is, the more approval authority and oversight is required to conduct it. Information obtained through research, records checks, and overt interviews can help establish the probable cause required for approval of special investigative techniques and warrants. Most intrusive means are only employed when probable cause exists and it is determined that further, pertinent information cannot be discovered through the execution of other, less intrusive investigative activities.

e. Least visible to most visible. The selection and execution of investigative activities should follow a logical sequence and progress from least visible to most visible. The SA must employ effective risk management techniques while conducting investigative activities to mitigate circumstances that may expose the investigation. ACI investigations are initially conducted using the least visible means to maintain operations security (OPSEC) and to avoid prematurely alerting the subject. For example, checks of centralized records outside the unit of assignment, nonconsensual records checks, and interviews of former bosses and coworkers from previous assignments are all examples of investigative acts conducted outside the view and knowledge of the subject. More visible means are employed as the investigation progresses and more leads are developed (for example, source interviews of the subject's current coworkers or the execution of certain special procedures in the same geographic area as the subject). The most visible techniques include techniques that involve direct contact with subject (for example, consensual checks and searches and SI).

f. Linear versus concurrent investigative activities. Investigative plans are generally organized chronologically in the order which investigative activity is expected to occur. However, this does not mean some investigative activities cannot be done concurrently. There are times when actions must be pursued sequentially and there are times when

investigative activity can occur simultaneously. Investigative activities should occur concurrently whenever possible. This negates a protracted investigation.

2–14. Levels of concurrence and approval for investigative documents

Investigative plans are reviewed and approved by the local CI supervisor. After reviewing the investigative plan, ACICA will either concur or provide additional guidance. Investigative activity will not be delayed pending review or approval by the CI element's chain of command. Additionally other agencies participating in the investigation will be required to review investigative planning documents before the conduct of any investigating activity. Table 2–1 provides an overview of the concurrence and approval required for the different CI investigative planning documents.

a. Concurrence. Subject interview plan (SIP) and joint subject interview plan (JSIP) require review and approval by the ACICA. The ACICA can nonconcur and issue guidance on adjusting the document to ensure it is legally sound and in accordance with applicable ARs. The document must be adjusted in accordance with the higher authority's guidance, prior to approval.

b. Approval. Formal authorization from a higher echelon to proceed with the proposed investigative activities presented in the documents.

Table 2–1
Concurrence and approval for investigative documents

	Limited counterintelligence assessment	Preliminary investigation	Full-field investigation
Opening message approval	Operations officer	ACICA (Joint)	ACICA
Extension memorandum approval	Army theater CI coordinating authority ACICA	ACICA	ACICA
Investigative plan concurrence	Army theater CI coordinating authority	ACICA FBI (Joint)	ACICA FBI (Joint)
Investigative plan approval	Operations officer	ACICA	ACICA
Subject interview plan concurrence	Supporting staff judge advocate (SJA)	Supporting SJA	Supporting SJA
Subject interview plan approval	ACICA	ACICA	ACICA
Joint subject interview plan concurrence	Not applicable	FBI or host nation partner, supporting SJA	FBI or host nation partner, supporting SJA
Joint subject interview plan approval	Not applicable	ACICA	ACICA
Termination message approval	Operations officer	ACICA (Joint)	ACICA

2–15. Counterintelligence investigative plan

a. The investigative plan is used to outline and request approval for the conduct of investigative activities. The ACICA is the approval authority for the investigative plan.

b. As outlined in AR 381–20, the investigative plan or joint investigative plan is the blueprint for CI investigations and will be used as tools to describe the purpose and objectives of the investigation. The investigative plan provides a detailed road map on CI investigations including investigative participants, investigative activities required, resources and external support required, and interagency or legal coordination required to successfully resolve the incident. The investigative plan is a living document, subject to frequent changes based on the investigative process, and is a document that guides the investigation to a logical conclusion. The investigative plan integrates the activities of all the elements conducting investigative activity in furtherance of an investigation and ensures that investigative activity is conducted in a properly sequenced, coordinated, coherent, timely, and efficient manner. Although investigations tend to follow the general pattern reflected in the investigative process, investigative activities can and do occur in unpredictable patterns and frequently the investigating SA is confronted with multiple concurrent actions that

are occurring in different parts of the investigative process simultaneously. The nonstandard nature of CI investigations makes sound basic organization and planning critical. It is recommended that the investigative plan is updated every 45 days or when major changes have occurred concerning the focus of the investigative effort.

c. A joint investigative plan is required when other agencies besides ACI are involved with a given investigation. The most common would be investigations with the FBI, USACIDC, Air Force Office of Special Investigations, or Naval Criminal Investigative Service. In these cases, the joint investigative plan must clearly show the other agencies have agreed to the plan, as written. An investigative plan, joint or otherwise, is required for all PIs and FFs. The investigative plan is normally due to the ACICA no later than 7 working days after the date of the case opening message; however, the ACICA may approve exceptions to the 7-day rule. Again, investigative activity will not be delayed pending review, approval, or concurrence of an investigative plan.

d. The investigative plan is generally organized chronologically in the order which investigative activity is expected to occur. This does not mean, however, they should be pursued in a lock step (A then B then C) manner. There are times when actions must be pursued in careful sequence and there are times when investigative activity can occur simultaneously. Investigative activity should occur concurrently whenever possible. The projected actions of an investigation are often listed by phases, which help keep the logical flow and ensure the order of investigative activities are from the least intrusive to most intrusive actions. While not mandatory, separating the intended investigative activities into phases helps keep the investigation on track.

e. In concert with the intent of least intrusive to most intrusive investigative activity, it is important to maintain operational security during the investigation to prevent subject from being prematurely alerted to our investigative interest. The basic principle is risk versus gain: what is the risk of discovery versus the need for the information gained. Eventually, visible, higher risk investigative activity is required in most investigations. Sometimes that point comes early and sometimes later. The key is to always plan for and consider risk in each investigative step.

2–16. Investigative plan submission

a. The investigative plan is normally due no later than 7 working days after the date of the case opening message; however, the ACICA may approve exceptions to the 7-day rule. Investigative plans are living documents and may require revision due to information development and case direction. Before implementation, investigative plans should be updated, revised, and forwarded to the ACICA for approval. Investigative plans are required in all open PIs and FFs for investigative actions. The content of the investigative plan must include, at a minimum, the background, investigative objectives, and the investigative actions. The background includes a synopsis of the incident under investigation. The investigative objectives include—

(1) Identification of subjects and a potential or suspected FIE nexus.

(2) Confirming, mitigating, or refuting the suspected allegations concerning the subjects.

(3) The nature or extent of the compromise of classified information or technology.

(4) Assessing the damage to national security.

(5) Determining the involvement and methodologies of an FIE.

b. Investigative actions are the projected activities required to conduct the investigation and resolve the incident. They include—

(1) Local, military, and national agencies records checks.

(2) Interviews of all persons who may be able to provide details concerning the incident. This includes witness, others knowledgeable, and SIs.

(3) Procedures requests for special investigative techniques.

(4) Submission of final ROI.

(5) Joint investigative coordination. All activities conducted with or supported by external military, civilian, or host nation agencies during the course of the investigation.

(6) Intelligence contingency funds (ICF). The projected amount of funds required to support all investigative activities through the life of the investigation.

(7) Coordination required. All activities by external agencies required to support the investigation, which may include technical support for special investigative techniques, legal coordination before the SI, and coordination for apprehension, detention, and searches by the appropriate approval authority.

2–17. Updating investigative plans

a. An investigative plan will be updated when there is a change in focus of the investigation or a major occurrence that sheds new light on the evidence or shows a new direction for the investigation to follow. To avoid confusion and errors in communications, there can be only one investigative plan as the sole authority for all future investigative

activity in the affected case. SAs and the responsible desk officer will only work from one investigative plan. Therefore, an updated investigative plan must supersede all previous versions. The lead agent and the desk officer must assume that, in the natural course of an investigation, developed facts and information will dictate a revision to the investigative plan. An investigative plan may be revised at any time. It is not necessary to wait for ACICA to task an updated investigative plan.

b. At or near the transition from one phase to another, the entire case should be reviewed to ensure it remains focused, the investigative activity supports the objectives, and follow-on activities are appropriate. It is not necessary to finish every investigative action in the original approved investigative plan before submitting an updated investigative plan. It is not necessary to finish all investigative actions in the original investigative plan before starting the investigative actions requested and approved in the updated investigative plan. This same guidance applies to joint investigative plans.

2–18. Planning for special collection and other investigative techniques

The most intrusive investigative methods, commonly referred to as special investigative or collection techniques, are outlined and explained in DODM 5240.01 and AR 381–10. Each request for authorization requires designated standards of proof for the special investigative technique being considered. The special collection techniques outlined under the above chapters are more intrusive than ordinary records checks and interviews and thus require more stringent guidelines and higher levels of approval. Request for authorization must explain why less intrusive means cannot be used to gather the required information, that sufficient probable cause exists where required, and that a clear nexus to DOD has been established. Remember, special collection techniques are time- and resource-intensive and involve low-density, sometimes one-of-a-kind, capabilities and equipment. The requesting element should be prepared to justify the requirements and anticipate questions.

2–19. Procedures not authorized during preliminary investigations

Procedure 7 (physical searches) and Procedure 8 (mail searches and examination) will not be conducted during a PI. All other investigative techniques, with the exception of Procedure 5, may be employed with the proper approvals as specified in DODM 5240.01 and AR 381–10.

2–20. Intelligence oversight coordination

In all cases involving a procedure or special operational request, the official documentation will include a review by the U.S. Army Intelligence and Security Command (INSCOM) Intelligence Oversight Office.

2–21. Staff judge advocate coordination

In cases where prosecution is a possibility, CI investigative personnel should consult with the SJA throughout the investigation and after coordinating with the ACICA and obtaining command approval. Continuous legal consultation during the investigation supports the prosecution's case and provides insight to the investigating SA regarding case direction. SJA assistance to CI investigations can include—

a. Providing legal advice for unique situations, such as offenses rarely charged or pursued.

b. Helping to clarify or resolve multiagency jurisdiction disputes and questions.

c. Assisting with identifying specific criminal offenses for individual cases.

d. Coordinating with the SA to discuss interview legalities, rights warning waivers, and hostile interview courses of action.

e. Assisting with the legal coordination and approval for apprehension, detention, and search warrants with prior coordination and approval of the ACICA.

f. Preparing criminal proceedings.

g. Providing intelligence oversight review for proposed CI activities.

h. Providing advice and assistance in the preparation of proposals for special investigative techniques.

2–22. External support requirements

The investigative plan serves as the single guiding document for the conduct of a CI investigation. It is important that it be used to plan for and integrate all external support (for example, outside the resources of the investigating element) and resources required to pursue the investigation. Many of these requests will be staffed and coordinated by the ACICA based upon the type of external support required. The types of external support include, but are not limited to—

a. Polygraph.

b. Computer forensics.

c. CI activities online support.
d. Surveillance support (Army or other agency).
e. Technical support for surreptitious entry or search and seizure.
f. NACs.
g. Subject matter experts (psychologists, linguists, and technicians).

2–23. Case control
Case control is the investigative management activities conducted to determine whether to approve a CI investigation. Case control also includes the oversight and approvals required during an investigation to preserve prosecutorial prerogatives or potential for exploitation of a CI incident. Case control consists of case determination, case status, opening and closing messages, and the running ROI.

2–24. Case determination
The ACICA may direct the opening of the LCA based upon a CIR that is of CI interest. The ACICA may direct the opening of a PI based upon a CIR that meets the threshold of reportable information in accordance with AR 381–12. Only the ACICA can open the FF. Only the ACICA can close LCAs, PIs, or FFs. The ACICA is responsible for closing all unilateral, joint, and bilateral PIs and FFs.

2–25. Merged
If an incident reported in a CIR is related to a similar incident in an open investigation, the CIR can be merged with the open investigation, based on concurrence of the ACICA. However, this is a rare occurrence.

2–26. Open
A CI investigation may be opened concerning an allegation, suspected commission of a crime, or incident of CI interest which ACI has jurisdiction. This includes cases for which ACI has primary jurisdiction for both the allegation, crime, or incident and the person; or ACI has parallel jurisdiction, with another agency, over the allegation, crime, or incident and the person. If an identifiable Army equity is involved in the allegation, crime, or incident, then ACI should pursue a joint investigation with another agency that has or shares jurisdiction.

2–27. Abeyance
During an open CI investigation, circumstances may require investigative activity be temporarily suspended by the directing authority for a specified time period. This may occur if all witnesses or the subject is deployed or otherwise unavailable for interview and all other investigative leads and activities have been exhausted. The directing authority may place the investigation in abeyance until the witness or subject is available to be interviewed and further investigative activities pursued.

2–28. Reopened
The ACICA may direct a terminated CI investigation be reopened based upon the discovery of new information or leads that merit further investigative activity.

2–29. Terminated
a. A CI investigation will be terminated after all leads and investigative activities have been exhausted or the allegation, crime, or incident of CI interest is resolved. The ACICA will direct the investigating element to cease all investigative activity and the submission of an ROI. Only the ACICA is authorized to terminate investigations.

b. Upon completion of all logical investigative activity and prior to the termination of a U.S. CI investigation, the ACICA must provide a final disposition of resolved or unresolved.

c. When a CI investigation is terminated as resolved, the following resolution subcategories will be used to further define the nature and circumstance in which the investigation was assessed as resolved:

(1) Terminated as resolved and referred for prosecution.
(2) Terminated as resolved with referral for action.
(3) Terminated as resolved when allegations are unsubstantiated.
(4) Terminated as resolved with operational potential exploited.

d. Conversely, when terminating an ACI investigation as unresolved, the following resolution subcategories will be used to define the nature and circumstances in which the investigation was unresolved:

(1) Terminated as unresolved with no referral for action.
(2) Terminated as unresolved with referral for action.

2–30. Closed

An ACI investigation is only officially closed after ACICA reviews of the ROI and submission of the ROI to the USAIRR (see para 2–45*d* for more information concerning case termination determinations).

2–31. Opening message

The ACICA informs the reporting field element of the results of the case determination process in the case opening memorandum, referred to as the opening message. The opening message generally identifies what investigating element has been identified as lead investigative element and the case determination and status. In the case of open FFs, the opening message will task the reporting element with developing an investigative plan. While the customary suspense for an investigative plan is 7 working days, in joint and interagency investigations it can sometimes take longer to coordinate and obtain concurrence and approval for the investigative plan. Once the investigation is designated as open by the ACICA, there is no requirement to wait for an approved investigative plan. The investigation is authorized to proceed with all approved investigative activities. SIA authorizes some of these investigative activities, but the ACICA can approve other nonintrusive investigative activity either telephonically or via email. SAs need to document such authorizations and make them part of the investigative file. This allows the investigating element to get the investigation started quickly and obtain additional information that will support the development and submission of a more detailed and thorough investigative plan. This may include the conduct of records checks on witnesses and others knowledgeable, other records checks, and limited interview authority (for example, witnesses and the subject's commander). All activities conducted under initial investigative authority will be documented in appropriate ACOP ROI entries.

2–32. Running report of investigation

a. The running ROI in ACOP is a draft version of the final ROI and is developed as the investigation progresses. Every investigative action, whether investigative activity or coordination, is documented in ACOP under the running ROI.

b. Once an investigation is opened in ACOP, the investigating SA will begin documenting all their activity in the running ROI. The running ROI has an administrative portion located in the ROI header, an offenses section, an activities section, and an attachments section. Once the agent selects the reports to be included in the final ROI, ACOP will automatically generate the ROI.

c. Everyone within the unit hierarchy will have access to the running ROI and can add to the running ROI. Once the case is terminated, the final ROI will be reviewed by the ACICA prior to retirement to the USAIRR.

2–33. Investigative activities

The investigative activities phase of the investigative process includes the conduct of investigative techniques for the collection of information to support investigative objectives, documenting the results of investigative activities and the collection of evidence to support potential prosecutorial prerogatives. During the investigative activities phase, SAs will—

a. Conduct CI interviews.
b. Conduct files and records checks.
c. Conduct research.
d. Report investigative activity results.
e. Collect evidence.
f. Conduct special investigative techniques.

2–34. Conduct counterintelligence interviews

CI interviews are conducted to ascertain facts and details concerning a person or incident of CI interest. The types of CI interviews are walk-in interviews, pretext interviews, source interviews, and SIs.

2–35. Walk-in interviews

A walk-in is an individual who seeks out U.S. ACI to volunteer information that is believed to be of interest to CI. A significant number of CIRs come from a walk-in source that has no previous relationship or reporting history with ACI. Agents have the authority to interview any individual who potentially possesses information of an intelligence or CI nature. A walk-in source should never be turned away (see chap 4 for more information on conducting a walk-in interview).

2–36. Witness interview

Witness interviews are conducted for persons who may have observed, heard, or have knowledge of a national security crime or CI incident. Witnesses are not the target of the investigation. If information is developed to indicate they should be a target of an investigation, the source will be treated as a subject. During SIA, SAs should focus on developing the best source for providing details concerning a person or incident of CI interest. Types of witnesses include—

a. Primary (best) source. SAs should identify the best source under their SIA to establish the facts of the incident, identify all associated personnel, and identify additional leads for any incident of CI interest. The primary or best source is generally a person having direct personal knowledge of a fact or series of facts related to a CI incident or allegation. Primary source interviews are conducted to develop information for a CIR. Primary source interviews can develop direct evidence and additional case facts and leads. Primary or the initial source may not necessarily be the best source. A CIR can be returned with guidance to interview the best source who was identified by the initial source.

b. Witness. A person having direct but partial knowledge of an incident or allegation. A witness may be able to corroborate or augment the information provided by the primary source and provide direct evidence, but not to the same extent as the primary source.

c. Others knowledgeable. An interview of a person having indirect or hearsay knowledge of the incident or allegation. Others knowledgeable may be able to corroborate or amplify upon specific case facts. Others knowledgeable can be critical for verifying case facts and developing leads; however, they generally do not provide direct evidence to support the investigative activity.

d. Coworkers and supervisors. Interviews of coworkers and supervisors can reveal large amounts of information about a subject. These sources can provide details on a subject's personality, behavioral characteristics, and pattern of life due to their personal or professional proximity to the subject. Some areas that can be addressed include—

(1) Subject's access to classified information.

(2) What information the subject may have compromised.

(3) Subject's handling of classified information.

(4) Subject's adherence to security procedures in their work area.

(5) Subject's connections to foreign entities and related indicators of espionage (travel, tradecraft, collection, contact and communication, and motive).

(6) Subject's lifestyle and changes to it.

(7) Subject's personal problems (psychological, medical, financial, legal, or other.)

(8) Subject's normal behavior and activity in professional and social settings.

(9) Other cooperating witnesses. Other cooperating witnesses include any personal or professional associations who may be able to provide further information pertaining to the situation or circumstances that may have given the subject reasons to commit the alleged acts. These witnesses may include everyone from unit security managers who grant access to information and files, to medical experts that can interpret medical findings, to neighbors or family members who have knowledge of the subject's personal life.

2–37. Subject interview

a. SIs are only conducted with ACICA approval. An interview of the subject is often the only way to put all the information gathered during a CI investigation into context and resolve the allegations. The SI requires a review by competent legal authorities (for example, the supporting SJA), which must be provided to the ACICA; the ACICA makes the final determination for an interview (see para 2–39). The SI may be the single most important investigative action SAs conduct during a CI investigation. It is conducted to allow subject an opportunity to resolve, refute, explain, or mitigate allegations developed through the investigation.

b. Most investigations conclude with the SI, but additional investigative activities may be necessary, to include special investigative techniques. It is possible and sometimes even desirable to conduct multiple SIs during the course of an investigation to obtain all the details required to resolve an allegation.

c. SAs should ensure that the interview environment does not suggest confinement or restraint, either through the type of room used (for example, bars on windows, a locked door, seating arrangement, or statements made by the interviewing SA) or by the number of SAs participating in the interview.

d. The SI may be—

(1) Pretext interview. An interview of a source in a CI investigation or a person who is or may become the subject of the investigation for the purpose of refuting, explaining, clarifying, or mitigating their knowledge of or involvement in an incident of CI interest without informing them of the true nature of the interview. Pretext interviews may be used in circumstances when a case may be resolved by eliciting relevant information from a source or subject without the person being aware of the true nature of the interview. AR 381–20 provides guidance on the approval authority and employment of pretext interviews.

(2) Noncustodial interview. A noncustodial SI is conducted without depriving the subject of their freedom (for example, arrest or detention). The subject voluntarily consents to being interviewed and is advised that they may depart at any time.

(3) Custodial interview. A custodial SI is conducted following the formal arrest or detention of a subject. The subject is made fully aware of their deprivation of freedom and specifically that they are in custody.

2–38. Types of subjects

The types of subjects in ACI investigations include military, civilian, and contractor.

a. Military subjects. A rights warning is mandatory for all persons suspected of a crime who are subject to the provisions of the UCMJ. Military subjects of ACI investigations who are suspected of a crime must be advised of their legal rights under UCMJ, Article 31(b) (see Manual for Courts-Martial United States (2019 Edition)) prior to the onset of questioning. This includes interviews conducted as part of a polygraph examination, if the subject is suspected of a crime. SAs may not participate in or witness SIs conducted by other agencies of Servicemembers who are suspected of a crime under the UCMJ, unless a rights warning is administered.

b. Civilian subjects. There is no need for SAs to advise civilian subjects who are not in custody of their rights. The rights advisement requirement for civilians (see U.S. Reports: Miranda v. Arizona, 384 U.S. 436 (1966)) takes effect when and if the civilian is in custody. Since ACI has no legal authority to place a civilian in custody, there are no rights warning requirements during a unilateral interview. If the subject incriminates themselves during the course of an interview, questioning may continue without a rights advisement. Additionally, SAs may participate in a noncustodial interview of a civilian subject who is either under ACI investigative jurisdiction or is the focus of an approved joint investigation. When interviewing a civilian subject, SAs will ensure that the civilian subject is aware that they are free to leave at any time.

c. Contractor subjects.

(1) EO 12333 directs the Secretary of Defense to protect the security of DOD installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the DOD, as are necessary.

(2) The 1979 Delimitations Agreement establishes jurisdictional boundaries and operational procedures that govern the conduct of CI activities by the CI organizations of DOD in conjunction with the FBI. The agreement specifies FBI and DOD investigative jurisdictions in both the United States and overseas based on the status of the persons who are the focus of the investigation (military personnel, civilian employees, contractors, foreign national employees of DOD, or persons not affiliated with DOD).

(3) Interview of contractor subjects is no different from other civilians. Outside the United States, unless responsibility is otherwise assigned by U.S. law, EO, or agreement with the host government, ACI may investigate Army contractors and their family members, subject to coordination with the FBI, CIA, and host government agencies as appropriate. Within the United States, ACI may investigate Army contractors with the prior approval of the FBI, unless it is a joint investigation, in which case ACI would be participating with the FBI.

2–39. Approval authority

The SI is a legally complex event that requires significant legal and operational oversight to avoid jeopardizing prosecutorial objectives or potential for exploitation. Approval to conduct the SI requires—

a. Approval of the SIP in writing by the ACICA. Additionally, if the interview involves other agencies, the JSIP was be agreed to by all parties concerned (such as the FBI) and approved by the ACICA.

b. SAs to coordinate with the supporting SJA and possibly the INSCOM SJA prior to conducting an approved SI. The ACICA may direct INSCOM SJA involvement depending on the legal complexity, nature of the criminal allegations, and other elements associated with the investigation.

c. A subject's pretext interview to be approved by ACICA and the SIP.

2–40. Subject interview approval for joint investigations

The SI approvals are also required for ACI participation or support for SIs conducted by other agencies.

2–41. Subject interview plan

a. Once the ACICA has directed or granted approval for the SI, the interviewing SA will develop the SIP to—

(1) Ensure the agent is familiar with all information obtained during the course of the investigation and clearly understands the goals of the SI.

(2) Identify and coordinate outside support as required.

(3) Provide documented approval to schedule and conduct the SI.

(4) Facilitate legal review of the SI proposal.

(5) Identify the intended charges, as discussed with the SJA.

b. The ACICA will approve all SIPs in writing before execution. A properly completed SIP will include the background, which details a synopsis of the incident under investigation, and the investigation objectives. The investigation objectives should encompass a list of all the goals of the SI including, for example—

(1) Affording subjects the opportunity to refute, explain, clarify, or mitigate allegations of espionage, terrorism, and other acts that may constitute threats to national security.

(2) Determining if subject is wittingly or unwittingly affiliated with a FIE.

(3) Determining if subject committed a national security crime and identifying FIE methods of operation and potential damage to national security.

(4) Summarizing the results of the investigation to date. A brief synopsis of all investigative activities and the corresponding results preceding the SI.

(5) Describing the purpose of the interview. Identification of all persons involved in the suspected allegations, the extent of compromise, all the details concerning the suspected allegations, and assessment for potential exploitation.

(6) Documenting administrative information. All participants in the SI, date, location, and whether or not the interview will be audio or video recorded.

(7) Conduct of the interview. Introductions; identification; rights warning or waiver and other administrative procedures; topical areas of the interview or, if required by the ACICA, a line of questioning; and closure of the interview including assessment on subject disposition, such as released, released to the chain of command, detention, or apprehension by appropriate authorities.

(8) Identifying coordination required. Any type of external CI coordination required to support the interview, including the SJA for legal advice on charges, military police for possible custody assumption, and any joint participants, such as USACIDC or FBI.

(9) Identifying the lead agent. Name, title, and contact information for the investigating agent conducting the interview.

2–42. Conduct files and records checks

a. A record is any item, collection, or grouping of information, whatever the storage media (for example, paper, or electronic), about an individual that is maintained by a DOD component, including, but not limited to, their education, financial transactions, medical history, criminal or employment history, that contains their name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, a voice print, or a photograph (see DODI 5400.11).

b. Records checks are conducted with U.S. and host nation military, law enforcement, security, and intelligence agencies to develop information concerning a subject or person associated with a CI investigation or a person of CI interest. Records checks can be conducted to—

(1) Confirm or determine identity.

(2) Collect information relevant to or of value to the investigation.

(3) Fully identify the subject of an incident when exercising SIA.

(4) Fully identify the subject of an incident in support of an ongoing LCA, PI, or approved FF.

c. Files and records checks are requested from Government agencies or from specific organizations that may retain personal data concerning a person of CI interest. There are two types of records check categories—

(1) Government agency checks.

(2) Personal data checks.

2–43. Government agency checks

Government agency checks are differentiated by the type of agency from which the check is being requested. Types of Government agency checks include—

a. Local agency check.

b. Military agency check.

c. NAC.

2–44. Personal data checks

Personal data checks are usually categorized by the type of check being requested.

a. Records checks during standing investigation authority.

(1) During CI investigations, discreet local and military agency records checks may be conducted to fully identify subjects (for example, assignment data, level of access to classified information, or other). Local and military agency checks that can be conducted include—

(a) Defense person search.

(b) Reenlistment eligibility data display.

(c) Enlisted Distribution and Assignment System.

(d) Total Officer Personnel Management Information.

(e) Interactive Personnel Electronic Records Management System.

(f) Joint Personnel Adjudication System/Joint Clearance and Access Verification System.

(g) Defense Central Index of Investigations (DCII).

(h) Defense Manpower Data Center.

(2) Discrete open-source records checks that can be accomplished under SIA include—

(a) Consolidated Lead Evaluation and Reporting (CLEAR) National Comprehensive Report (NCR).

(b) LexisNexis.

(3) Discrete military agency checks to fully identify subjects who may be linguists include—

(a) Contract Linguist Information Program (CLIP).

(b) Army Knowledge Online (AKO) Linguist Database.

(c) Contractor Translator Interpreter Data Entry System.

(d) CI storage site.

(4) Records checks for foreign travel, to include—

(a) Airlines Reporting Corporation.

(b) TECS.

b. Gaining access to records. Various procedures are available to SAs to obtain access and copies of records of investigative interest. The type of information being requested, the privacy rights afforded that type of information, and the nature of the agency holding it impact the procedure required to gain access. Generally, Government records are easier to access since SAs represent a Government agency conducting an official Government mission. Records of commercial companies are more difficult to obtain and often require formal written requests especially where specific privacy rights have been established by law (for example, telecommunications and financial records). Records checks can be either consensual or nonconsensual. Nonconsensual records checks that have been afforded specific privacy rights under the USC are the most difficult to obtain. The types of access include—

(1) Informal requests.

(2) Formal requests.

(3) Access with consent.

(4) Access granted by military authority.

(5) Warrants, subpoenas, and court orders.

Note. It is important to determine if the request for a specific type of record is afforded specific privacy rights under U.S. law and any exceptions. For example, the disclosure of both financial and telecommunications records are generally prohibited with specific exceptions.

c. Informal request. SAs may make verbal or written requests to an agency for access to records of interest. This method is most often used for a military agency check or local agency check. SAs may pursue this type of access when using an existing liaison relationship and access to the records will not be questioned based upon that status (presentation of badge and credentials) and the authority provided by AR 381–20.

d. Formal written requests. A NAC and checks of a commercial company records are requested formally in writing. There are various types and forms used for NACs and commercial agency checks. For example, NACs are typically requested electronically or by memorandum, normally through the ACICA. Nonconsensual checks of commercial company records are requested by formal memorandum. Some requests for access are processed in accordance with procedures identified in the USC (sometimes incorrectly referred to as a national security letter, which is primarily an FBI term) or other mechanisms (for example, bank letters). These memoranda certify that the agency presenting them has the authority under a specific section of the USC to obtain the records and has met the legal threshold required to exercise that authority. These memoranda are strictly formatted and often require specific approval authorities and signatures depending on the language in the supporting section of the USC. Authorities differ depending on the type and subject matter of the record and the matters being investigated (for example, foreign CI versus terrorism). Other formal written requests are for voluntary cooperation with ACI from commercial companies. While the companies involved do not have to grant access, they are not prohibited by law from doing so.

e. Access with consent. In cases where a record is afforded formal privacy rights, a check can be conducted if the subject gives consent. Consent to access must be in writing and, depending on the type of record, may require a specific form to access the record. This type of records check should be considered in the latter stages of an investigation when the subject may be aware of the investigation. The subject may consent to a records check if the SA explains that the check may refute, explain, or mitigate the allegations against the subject.

f. Access granted by military authority. AR 381–20 provides regulatory authority for access to Army records and facilities in support of a CI investigation. Upon presentation of badge and credentials, SAs will be permitted access to Army records as required for the conduct of CI investigations or operations. Under these authorities, SAs are authorized to make extracts or transcripts of specific information obtained. The actual records will remain under the control of the records custodian, who will make the records, or legible certified copies of the records, available for judicial, nonjudicial, or administrative proceedings. Section 552a(b)(7), Title 5, USC authorizes access to records of other Federal agencies.

g. Warrants, subpoenas, and court orders. Records that cannot be obtained through the methods above may be obtained through a warrant, subpoena, or court order in support of a CI investigation. This is the most formal method of obtaining access and is a complex and time-consuming process. Warrants and court orders may be sought from military or Federal court, the Foreign Intelligence Surveillance Court, or a grand jury as appropriate. In bilateral or joint investigations, the Army will usually defer to the FBI to obtain a warrant or court order.

h. Conduct research.

(1) Research is information gathered by SAs from open and classified sources and databases and does not require a formal request to another agency. Research can be used to gather basic information about the people, places, and things that form the framework and context of an investigation. In many instances, research develops only background information to aid understanding of the case facts. In other instances, it will yield tangible information that furthers the investigation and the results must be captured in an ACOP ROI entry. Information obtained through basic research may include—

(a) Basic identifying data of sources and subjects.

(b) Employment information.

(c) The subject matter involved (for example, reading articles and publications concerning technology involved in a CI incident).

(d) The geographic locations where case events occurred.

(2) Open and restricted research methods include—

(a) Name checks and traces.

(b) Open-source research.

(c) Fee-based, open-source searches.

(d) Classified resources and intelligence databases.

i. Name checks and traces.

(1) The term name check is one of the most widely used and often misunderstood investigative terms. Name checks concerning information on personalities can be gathered using both research tools and through formal local and NACs. Entering a name into an open-source internet search engine is a form of name check and would be considered research. Requesting a name be run through national-level indices (for example, DCII) is also a form of name check; however, this is considered a formal records check. Research-based name checks are considered investigative activity and the information is required to be reported in an ACOP ROI entry.

(2) Name checks using open-source, fee-based and general intelligence databases are requested through submission of a request for information through the responsible operations management element. This ensures the requests are efficiently processed in a consistent manner and tracked to completion.

(3) Name traces requested from a national database are considered a NAC. All NACs not available through liaison with the local agency's office or representative are requested through the operations management element based upon unit standing operating procedures (SOPs).

j. U.S. person information. SAs should remember that any organization where the majority of the members are U.S. persons is also considered a U.S. person.

Note. In accordance with AR 381–10, a U.S. person is a U.S. citizen, an alien known by the intelligence component to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the United States that is not directed or controlled by a foreign government. A corporation or a subsidiary incorporated abroad is not a U.S. person even if partially or wholly owned by a corporation incorporated in the United States.

k. Open-source research. Open sources are those that are available, without restriction, to the general public. SAs may use open sources to locate and identify sources and subjects, as well as corroborate or refute information collected from other sources. Open sources can often provide context and background information for the investigative case. Reviews of open-source information that advance the investigation or yield specific case facts are considered investigative actions and results are recorded in an ACOP ROI entry. Some examples of open-source resources include—

(1) Internet search engines.

(2) Newspapers.

(3) Telephone directories.

(4) Chamber of Commerce.

(5) Better Business Bureau.

l. Computer attribution. Be aware that DOD computer systems are easily identifiable. SAs will use Managed Attribution Solutions to research information pertaining to an investigation.

m. Fee-based, open-source services. As internet accessible information has proliferated, a number of commercial services have developed to exploit those resources more efficiently. These for-profit services are not usually accessible from desktop of SAs. A support analyst, the Intelligence Operations Support Branch, or Army Counterintelligence Center library can conduct this type of research.

n. Classified resources and intelligence databases. SAs also have access to a number of classified research tools and resources. Secret Internet Protocol Router Network (SIPRNET) search engines can leverage intelligence websites and provide access to intelligence products and databases.

o. Reporting investigative activity results. CI investigative reporting serves to document the results of CI investigative activity conducted under SIA or an approved investigative activity. CI investigative reporting also allows operational management elements to conduct technical control and oversight of ongoing CI activities to ensure compliance with applicable U.S. laws, foreign agreements, DA and DOD policy, and unit SOPs (see chap 5 for more information concerning CI investigative reporting). CI investigative reporting and documentation consist of requests for assistance (RFAs) and MFRs.

p. Army Counterintelligence Operations Portal activity generator in the running report of investigation.

(1) All investigative activities are documented in the activity generator within the ACOP running ROI as an ROI entry. It serves as the SA's certified affidavit concerning investigative actions. All documentation may be used in a prosecution and is subject to discovery by a defense attorney and if incomplete or inaccurate information is reported, the defense may have pertinent information excluded from use in the prosecution of a subject. The exclusion of a poorly written ACOP ROI entry could result in the dismissal of criminal charges. Each ACOP ROI entry must be accurate, concise, impartial, and complete to preclude incorrect or arbitrary conclusions being drawn by the reviewing officials or other agencies.

(2) Many ACOP ROI entries will include associated exhibits. For example, the results of a records check with the local provost marshal will be documented in an ACOP ROI entry with the actual results attached to the report as an exhibit. ACOP ROI entries resulting from interviews will normally have a sworn statement attached as an exhibit.

(3) ACOP ROI entries are documented in ACOP with associated exhibits no later than 5 working days from completion of the investigative activity or receipt of results.

q. Requests for assistance.

(1) RFAs arise from two sources: the ACICA or another agency. In accordance with 381–20, RFAs are normally used for one-time or limited- or short-duration investigative assistance in the conduct of local or military agency checks. RFAs are tracked and managed within ACOP. Requests from other agencies for information or assistance not requiring investigative assistance (for example, facilitating introductions on a military installation or arranging for interview space) are not considered RFA. The ACICA disseminates the request in the form of an RFA with completion suspense date to the responsible FO. An RFA is used when another agency (most often the FBI) has exclusive jurisdiction in a national security investigative matter, but requires ACI assistance of a lesser scope than would warrant a joint investigation. An RFA will not be used to circumvent establishing a joint investigation where Army intelligence has jurisdiction or significant Army equities are involved. National agencies normally submit a formal request to the ACICA in the form of an LHM. However, requests can also occur at the FO level.

(2) RFAs in the form a lateral lead can also be passed laterally from one FO to another. This is most often done for interviews of sources who are not located in the requesting FO's AO or for technical assistance, such as conducting forensic examinations of digital media. The SA completing the RFA will prepare the ROI entry in ACOP documenting the investigative activity. RFAs may be passed by an outside agency at the field level. SAs may request that the outside agency prepare an LHM addressed to the ACICA. The SA receiving the request will communicate to higher using ACOP, documenting the type, duration, and scope of support requested, if the outside agency is unable to provide an LHM. The operations officer or SAC will send an ACOP comment to the ACICA to seek approval in supporting the

request. Certain investigative acts, such as participating or witnessing interviews, require ACICA approval. The FO will request approval from the ACICA for these types of investigative activity since the ACICA is the approving authority as outlined in AR 381–20.

(3) At times, other U.S. intelligence community members and U.S. Government agencies may have information that may be useful or provide additional investigative leads. ACI may submit an RFA or request for information to another agency to develop information and generate additional investigative leads; however, these requests should be submitted to the ACICA for review, approval, and coordination at the national level. This specific document is frequently referred to as a reverse LHM. The RFA or request for information should articulate relevant details supporting the request, as well as what information is needed from the U.S. intelligence community member or U.S. Government agency. This specific request is signed by the Chief, ACICA Investigations and Operations Branch and is submitted at the national agency headquarters level.

(4) See DODI 3025.21 for more information regarding defense support to civilian law enforcement agencies.

r. Collect evidence.

(1) Evidence is anything that helps to ascertain the truth of a matter or gives proof of a fact. Evidence may be physical or testimonial (see AR 195–5). CI investigations result in the collection of evidence to support conclusions or judgments concerning an incident of CI interest. Evidence is used to support prosecutorial activities in courts of law or to allow base commanders to make informed decisions regarding criminal liabilities or security considerations (for example, increasing protection measures, base access, custodial status, or other). Evidence consists of—

(a) Testimonial evidence, which includes verbal or written confessions or statements of participants, witnesses, sources, or subjects of an incident or suspected crime.

(b) Physical evidence, which includes materials or objects associated with an incident or suspected crime.

(2) Although exploitation may be an objective of a CI investigation, the investigation should be conducted to maintain legal integrity in the event of prosecutorial activities.

(3) Techniques and procedures for gathering evidence are dependent upon the type and scope of the authorized investigation or investigative activity. Investigative activities, to include evidence gathering, in response to CI incidents are also limited to that authorized under SIA. The scope of investigative activity will also vary depending on the type of authorized investigation, LCA, PI, or FF. SAs must be knowledgeable concerning how to collect, seal, preserve, store, and maintain custody of evidence. Evidence is processed in accordance with AR 195–5 and ATP 3–39.12.

s. Counterintelligence special operations concept staffing and approval. A counterintelligence special operations concept (CISOC) documents a proposed special operation, special investigative activity, or CI source operation and serves as the basis for the review and approval process. CI investigation activities that are proposed through the submission of a CISOC usually represent targeted, sensitive, complex, and intrusive activities that require close and continuing oversight and legal review. A CISOC serves as the vehicle to document an operation, but the CISOC is not the operation itself. It identifies to the approving authority what the investigative element wants to do. Proposals for CI investigative source operations must be documented in ACOP and coordinated and approved in the context of a CISOC. The CISOC serves as the basis for facilitating the review, intelligence oversight, and approval process.

t. Special collection techniques and special investigative activity approval authority. Any proposal for the use of special collection techniques specified in AR 381–20 must be documented in ACOP and approved separately from the CISOC. Proposals for the conduct of special investigative activity not defined in AR 381–20 or by AR 381–47 will be forwarded to the ACICA for review prior to being submitted for approval (see AR 381–20 for investigative source operations approval authorities).

u. Guidance on requesting counterintelligence special operations concept approval. See AR 381–20, for guidance on content that must be included when developing and requesting approval of a CISOC (see ATP 2–22.2–2 and ATP 2–22.33 for more information and example format for a CISOC).

2–45. Case disposition

The final phase of the investigative process is case disposition. During this phase, all investigative activity has been completed. The ACICA decides if the CI incident under investigation has been resolved and makes a determination on the status of the case.

a. Allegation resolution.

(1) The ultimate objective of a CI investigation is to determine the resolution of allegations of known or suspected acts that may constitute national security crimes under U.S. law or the UCMJ. During the case disposition phase of the investigative process, the ACICA must evaluate whether there is sufficient information and evidence to support—

(a) Exploitation of the incident.

(b) Neutralization of the threat through prosecutorial activities.

(c) Recommendations to the supported commander for nonjudicial punishment or changes to systemic procedures when an incident identifies a security risk or vulnerability, but there is no evidence to suggest FIE involvement.

(d) Dismissing the incident when no crime or FIE activity is identified.

(2) Upon completion of all logical investigative activity and prior to the termination of a CI investigation, the ACICA must provide a final disposition of resolved and unresolved allegations.

b. Resolved allegation. In addition, when terminating a CI investigation as resolved, the following resolution subcategories will be used to further define the nature and circumstance in which an investigation was assessed as resolved:

(1) Terminated as resolved and referred for prosecution. Those investigations wherein during the course of an investigation, sufficient evidence is discovered which leads to the investigation being referred to the U.S. Attorney's Office or Military Justice Division at the Office of the SJA for prosecution.

(2) Terminated as resolved with referral for action. Those investigations that are terminated, however additional matters exist that reside outside of ACI jurisdiction and are therefore referred to the appropriate agencies, commands, services, or other U.S. Army components for further action.

(3) Terminated as resolved with operational potential exploited. Those investigations that are terminated, however the circumstances surrounding the initial allegation are exploited in a controlled CI operation.

(4) Terminated as resolved when allegations are unsubstantiated. Those investigations where investigative activities either failed to yield information substantiating the allegations or failed to yield information that disproves the allegations.

c. Unresolved allegation.

(1) Conversely, when terminating an investigation as unresolved, the following resolution subcategories will be used to define the nature and circumstance in which an investigation was unresolved:

(a) Terminated as unresolved with no referral for action. Those investigations that are terminated, wherein the allegations cannot be resolved through continued CI investigation.

(b) Terminated as unresolved with referral for action. Those investigations that are terminated, wherein the allegations cannot be resolved, but are referred to other appropriate agencies, services, or commands for action.

(2) See AR 381–20 for policy on unresolved allegations.

d. Termination message.

(1) The ACICA can terminate the LCA, FF, joint PI, or ACICA-directed PI, except those involving North Atlantic Treaty Organization organizations, for which the 650th MI Group has requisite authority.

(2) Once the ACICA terminates an investigation, a case termination memorandum or message will be sent to the investigating CI element. The appropriate chain of command will receive information copies for administrative and suspense actions.

(3) The investigating CI element will request termination of an investigation from the ACICA. The ACICA will prepare a termination message. This document will cite the justification for case termination and will levy requirements for preparation and submission of an ROI, if required. No further investigative activity will be taken on a terminated case, unless directed by the ACICA. Investigative activity initiated prior to the termination date should be completed as ACOP ROI entries.

e. Reporting and documentation. Once an investigation is terminated, the investigating SA will prepare all final documentation in ACOP and forward the investigative case file through the operations management element to the ACICA. Generally, the final documentation will consist of an ROI and an LHM.

f. Report of investigation. An ROI will be prepared for all terminated PIs and FFs. The CI investigating element will only prepare an ROI for the LCA if significant investigative acts were conducted. The ROI is the executive summary (EXSUM) of all results of investigative activity conducted in an investigation. The ACICA processes and forwards investigative and operational records included in the ROI to the USAIRR at Fort Meade, Maryland. ROIs are required for all investigations that go beyond SIA. The ROI highlights investigative efforts to explain, refute, or support allegations or incidents that predicated the investigation (see chap 6 for more information concerning the format for the ROI).

g. Summary of information.

(1) The LHM is the document used to provide information about a CI investigation to other Government agencies or organizations with a vested interest in the information or those that have primary jurisdiction and responsibility for responding to the incident. The LHM will only provide a summary of information relevant to the release. The LHM will not include CI internal tasking or coordination information, CI investigative methods, case control information, or identifying data on sources. The LHM contains administrative data and a summary of the information obtained by ACI. The hand delivery of LHMs to the appropriate command or agency is recommended to ensure any questions or concerns are addressed by the SA.

(2) Any LHM going outside Army channels will be signed by the Director, ACICA. Any LHMs staying within Army channels can be signed by the investigative element once it is reviewed by the ACICA.

(3) The LHM serves a specific purpose and must be concise. It should not include information that is irrelevant or information that does not directly pertain to the allegation. The LHM is used to provide information, including results of any ACI investigative activities, to those agencies or organizations with a vested interest in the information or those that have primary jurisdiction and responsibility for responding to the incident. LHMs are intended for a specific organization and should be tailored to the receiving command or agency. Investigative findings and issues may not necessarily be relevant to another U.S. Government agency (for example, the FBI or USACIDC). However, the information may be more important for a command to take UCMJ or other administrative actions against a subject. U.S. Government agencies may include local- and national-level agencies, unit commanders and security officers, or law enforcement agencies. Additionally, the LHM can be used to inform an agency or command of the results of Army intelligence's investigation concerning a subject of interest to them or under their command. An LHM usually contains information from multiple investigative documents and is intended to articulate ACI's investigative activities and the relevant facts of the investigation. As such, the LHM will capture all pertinent information directly associated to the allegation. At a minimum, the LHM will fully identify the subject of the investigation, the initial allegation, pertinent or significant investigative results or findings, and the termination status (either resolved or unresolved). For joint investigations, the LHM will not include any post-ACI case termination activities or findings from another U.S. Government agency. An additional review and subsequent approval by AIPP for release of polygraph-oriented statements are required for LHMs containing information related to a polygraph administered by them. AIPP is the sole approving authority for the release of their polygraph examination results, findings, and activities. Under no circumstances will another U.S. Government agency's information be released via LHM without written consent and approval of that agency (for example, the FBI or Defense Intelligence Agency (DIA)). Once ACI passes an LHM to the responsible agency or element, ACI may have to follow-up and determine what actions were taken as the result of the LHM's passage.

h. Case file disposition.

(1) Upon receipt of a message from the ACICA terminating investigative activity, the CI investigating element will complete and forward an ROI and an LHM in ACOP along with all original, signed investigative documentation to the ACICA.

(2) OPSEC is a critical component for all U.S. Army operations including CI investigations. Once a CI investigation has been initiated, limiting knowledge and implementing OPSEC measures is critical to maintaining the legal integrity of the investigation. The more people become involved or associated with the investigation, the greater the risk of compromising the investigation. For CI investigations, OPSEC prevents compromise by limiting knowledgeability of the investigation, preserves the legal integrity of the investigation in anticipation of prosecutorial action, protects the reputation of a potential subject, and prevents the possibility of reprisals should the investigation disprove the allegations or their involvement in an incident. Additionally, it allows for other exploitation opportunities (see ATP 2–22.2–2 for more information regarding exploitation).

(3) OPSEC considerations for CI investigations include—

(a) Informing the commander.

(b) Responding to media inquiries.

(c) Special handling considerations.

(4) Command support, or the lack thereof, can make or break any investigation. The best course of action in all cases is to have a positive relationship with the commander of the unit affected by the incident or concerned by the subject under investigation. This is vital in the successful completion of investigations, especially when SAs require command support and emphasis.

(5) At some point during a CI investigation, SAs will normally have to brief a commander concerning an incident involving or affecting their unit or when someone in their unit is implicated in a CI investigation. Any discussions with the commander must be documented in ACOP. During the early stages of an investigation, having the entire chain of command aware and involved in an investigation can potentially compromise the investigation. Deciding which commanders should be briefed, and in what order, is a delicate matter. Briefings generally occur from the top down. The lower the echelon SAs brief, the closer they get to the subject and the more risk there is for the compromising the investigation.

(6) In terrorism cases where there are force protection concerns or espionage cases involving highly classified information, early briefing at the general officer level will often be necessary and appropriate.

(7) Informing a supported commander requires SAs to coordinate for the release of investigative information and to brief the commander.

i. Coordinate for the release of investigative information.

(1) SAs are required to obtain ACICA approval to brief senior leaders, both within and outside of CI channels. The ACICA must approve all requests to brief senior commanders regarding the details of CI Investigations. The ACI office must identify the information to be briefed and submit requests for approval at least 3 days in advance. The majority of such requests involve general officers and senior executive service level personnel.

(2) Each request to brief a senior leader will include an EXSUM and the briefing slide. The briefing slide is not required to be given to the person being briefed. Rather, it is a guide to ensure the agent understands the main points to be briefed and stays on topic. In instances involving nongeneral officer level commanders or leaders of a unit (for example, a brigade commander or a division G–2), the ACICA should be notified in advance with at least an EXSUM of the planned briefing. No slide is required in this situation. When in doubt concerning 0–6 and below briefings, the SA or responsible operations management element should contact the ACICA for guidance.

(3) Briefing CI investigations, especially to a non-MI leader, requires SAs to be well versed in expectation management and the overall case facts. During the briefing, commanders may ask questions not necessarily related to the investigative acts planned by the supporting CI unit. The SA should not commit to or affirm any activity not within their purview. However, the SA should be able to address each of the commander's logical concerns for security of their assigned U.S. Army equities. When possible, the SA responsible for CAP activities for that unit should accompany the SA briefing unit and activity commanders.

j. Briefing the supported commander. SAs consult with their operations management element and ACICA concerning when and what information may be briefed to a supported commander regarding an ongoing CI investigation.

k. Prepare for and brief the commander.

(1) The commander should be provided with a synopsis of the situation and an explanation of any potential immediate force protection risks. Regardless of the status of the investigation, the commander should be informed if the immediate force protection risks are high.

(2) If the SA requires assistance from the supported command to conduct investigative activities, such as personnel or military records checks, the SA should be prepared to brief the commander concerning the incident or issue being investigated in accordance with guidance from the ACICA to gain the commander's support. The briefing should also include recommended security countermeasures to neutralize a force protection threat while preventing the investigation from being compromised.

(3) The commander should be advised not to disclose the information presented nor discuss it with anyone outside CI channels, including other staff officers or higher command channels, as the investigation may be compromised if information leaves the proper channels. The commander should be informed that periodic updates regarding the progress of the investigation will be made available, as the situation allows.

(4) After briefing the commander, SAs will submit an EXSUM in ACOP to the ACICA.

l. Responding to media inquiries. SAs should be prepared for inquires by local media. In some cases, subjects themselves will contact local media in an effort to disrupt an investigation. SAs should know in advance what can be said and to which public affairs office (PAO) representative the inquiry can be referred. If an investigation has the potential for high visibility actions (for example, search and seizures, physical surveillance, or other), SAs should work with the ACICA to develop a media inquiry plan and prepare guidance for the local PAO. A common technique is to have the local PAO refer the matter to the INSCOM PAO or the Headquarters, Department of the Army (HQDA) PAO. SAs should immediately notify their operations management element and chain of command of media inquiries or potential media interest in a CI investigation.

m. Special handling considerations. Certain CI investigations require special handling procedures because of unique circumstances involving the subject or information involved in the investigation. Special handling considerations include—

(1) U.S. versus non-U.S. persons and protection of information.

(2) BIGOT cases and close hold investigative activities.

(3) Handling sensitive compartmented information (SCI) in investigations.

(4) SAPs.

n. U.S. persons versus non-U.S. persons and protection of information. There is a significant distinction between collecting information concerning U.S. persons and non-U.S. persons, both in terms of the procedures required and resources available. While classified source research is likely to yield far more information on foreign entities than U.S. entities, care should still be used to recognize potential U.S. person information and handle it appropriately. Information on U.S. persons even in Government databases will often require a formal request for information or may need to be obtained through a records check.

o. BIGOT cases and close hold investigative activities.

(1) A BIGOT investigation is an investigation that, due to the sensitivity of the subject or the nature of the investigation, requires that it be handled on a strict need-to-know basis. The subject categories that qualify for a BIGOT caveat and the maintenance of a BIGOT list include—

(a) SAs or persons in CI units.

(b) Military officers 0–6 and above.

(c) Soldiers at the grade of E–9.

(d) Civilian DOD employees general schedule (GS)-15 (or equivalent) and above.

(e) Cases involving subjects in which another agency has specifically requested information be held in limited distribution.

(f) Cases involving subjects in which the initial report originated from sensitive sources or methods.

(2) Since knowledgeability of these investigations will be strictly limited to those with an absolute need to know, access to information concerning these investigations is controlled by maintaining a list of personnel who have been approved for access, referred to as a BIGOT list. The BIGOT list is maintained by the ACICA within ACOP.

(3) In all cases, coordination will be made with the ACICA to ensure the BIGOT caveat is both properly applied and under what standard, as identified in paragraph 2–45*o*(1).

Note. See AR 381–20 for policy on BIGOT investigations.

p. Handling sensitive compartmented information in investigations.

(1) SAs should always be alert for the involvement of SCI in a CI investigation. Indicators that this might become an issue include—

(a) Subject has a top secret or SCI security clearance with access to SCI information.

(b) Subject is assigned to an intelligence unit or holds an intelligence military occupational specialty.

(c) Subject works in a sensitive compartmented information facility (SCIF).

(d) A reported incident occurred in a SCIF.

(e) The presence of unmarked information that deals with subject matter that has a high probability of being SCI (for example, signals intelligence, cryptography, or other).

(2) Upon determining the involvement or potential involvement of SCI information in an investigation, SAs will coordinate with the local special security office (SSO) for appropriate storage of the SCI information. SAs will wrap and seal the SCI information being stored in the SSO to preclude access by personnel without the need to know. Such protection will be afforded to the information until a final determination is made as to the classification of the information involved. Potential SCI information obtained during the course of an investigation will be stored separately and in a security container accessible only by SAs participating in the investigation.

(3) SAs should immediately notify their responsible operations management element upon determining actual or potential SCI information is involved in a CI investigation. Review of SCI information involved in a CI investigation will only be conducted within an accredited SCIF. Transmittal of SCI information will be conducted in accordance with AR 380–28. Final disposition instructions for all SCI information obtained during the course of a CI investigation will be provided by the ACICA. These instructions will include the procedures for addressing SCI information within an ROI.

q. Special access programs. AR 380–381 governs the security of the SAP in the Army. The SAP is an approved security program imposing strict controls on individual access and dissemination of information. These controls are selectively applied to especially sensitive Army programs involving military research and development, activities, or operations. SAs will be familiar with the indicators of the SAP (for example, special handling instructions, special caveats, nicknames, and code words). The ACICA will be immediately notified when a CI investigation involves SAP information. AR 380–381 requires that the Army Special Programs Division, HQDA be notified of the possible compromise of SAP information within 24 hours. Whenever SAs encounter potential SAP material in the course of their duties, the material will be brought under immediate control, inventoried, and handled as evidence. Exposure and knowledge of SAP information will be strictly limited. SAs should contact the ACICA for determinations of potential SAP information and to receive handling guidance.

r. Special access program indoctrination. The ACICA will identify the requirements for SAP indoctrination (referred to as a read-on), to include other SAs, operations management, and other support personnel involved in the CI investigation. No CI investigation involving SAP information will be run without indoctrination for key command, operations management, and oversight personnel. SAP indoctrinations will be coordinated through the operations management element and designated SAP control officer as required.

s. Two case files. Two investigative case files will be maintained on SAP investigations. One case file will be kept at the classified collateral level within ACOP and the other will contain the SAP material and be marked, stored, and

handled in accordance with AR 380–381. When an ROI entry or other investigative reporting is required for an investigation involving SAP information, SAs will use a dual reporting system. SAs will submit two reports: one containing classified collateral information submitted in ACOP and one containing SAP information that is handled, transmitted, and stored in accordance with AR 380–381. On termination of the investigation, two ROIs will be prepared. One will contain all case documentation, including the code word material.

t. Security procedures. SAP security procedures will be strictly adhered to throughout the conduct of the SAP investigation. Storage, handling, transmission, and accountability of SAP information, physical security requirements, and other SAP security procedures will apply.

Chapter 3
Counterintelligence Records Checks

A records check is the process SAs use to obtain relevant information about sources or subjects from the records and information holdings of military, civilian, or Government agencies, as well as certain commercial companies and vendors, during the conduct of an investigation. Information from records checks may be obtained during a personal encounter between SAs and a representative of the agency or company from which information is being requested. Records checks may also be conducted by telephone, email, facsimile, or an online database. SAs conducting a records check must be able to articulate the CI mission, function, and authority when collecting information concerning a U.S. person.

3–1. Government agency checks

There are three types of Government agency checks: local, military, and national. All records checks are managed and documented in ACOP.

a. Local agency check. A local agency check is a record or file check of official or publicly available information conducted at any local office of Government agency within the AO of the CI element conducting the check. These records may include holdings and databases maintained by local and state law enforcement agencies, local courts, and local offices of Federal agencies to include, but not limited to—

(1) Bureau of Vital Statistics (birth and death records).
(2) Civilian medical facility.
(3) Joint task forces.
(4) Local courts.
(5) Local offices of the U.S. Postal Service.
(6) Local offices of Federal agencies.
(7) Local police departments.
(8) Public utilities.
(9) Regional police and law enforcement networks.
(10) Schools and universities.
(11) State police.
(12) State Department of Motor Vehicles.
(13) Tax assessment offices.
(14) Voter registration records.

b. Military agency check. A military agency check is a record, file, or database check requested from a military agency within the AO of the CI element conducting the check. Military agency checks include, but are not limited to—

(1) Civilian Personnel Office (employment and finance information).
(2) DCII.
(3) Defense Eligibility Enrollment System.
(4) Defense Manpower Data Center.
(5) Defense Person Search.
(6) Interactive Personnel Electronic Records Management System.
(7) Joint Personnel Security Adjudication System (JPAS).
(8) Local and regional USACIDC offices.
(9) Local offices of other military service law enforcement or intelligence offices.
(10) Military finance and personnel offices.
(11) Military medical facilities.
(12) Military police (Customs and Investigations).

(13) Military police or provost marshal office (PMO).
(14) Personnel Network.
(15) Post dishonored check office.
(16) Post education center.
(17) Post locator Reenlistment Eligibility Data Display.
(18) Post vehicle registration office.
(19) Unit and installation security manager.
(20) Unit S–1 and resource management officer.
(21) World Wide Locator.
(22) Other records may be available.

c. Official telecommunications records. Subscriber identity and toll and transaction records associated with official telecommunications systems (for example, Government phones, computer systems, networks, and AKO) are considered official Army records and may be accessed as a military agency check. They are covered by the authorities granted in AR 381–20. Access to these records can be obtained from several sources from the local Network Enterprise Control Center, regional Signal Command, or Network Enterprise Technology Command. This does not extend to the intercept (real-time monitoring) of the content of communications that can only be accessed in accordance with AR 25–2 and only with a properly approved procedure in accordance with DODM 5240.01 and AR 381–10.

d. Retrieving Defense Information Systems Agency enterprise email.

(1) The Army has migrated unclassified and collateral classified email systems to an enterprise enclave centrally managed by the Defense Information Systems Agency (DISA). As a result of this migration, DISA Office of General Counsel has implemented a new process for obtaining access to electronic mail records, which reflect the new Army standard on privacy rights, authorized monitoring, and searches as detailed out in AR 25–2. Consistent with DOD banners and user agreements, any use of Army information technology is made with the understanding that users have no expectation of privacy or confidentiality of any electronic communication, including minor incidental personal uses. The Army now reserves and will exercise the right to access, intercept, inspect, record, and disclose any and all electronic communications on Army information systems, including minor personal uses, at any time, with or without notice to anyone, unless prohibited by law or privilege.

(2) Prior to submission of a request to DISA, the investigating SA will ensure that the request supports a properly authorized CI investigation and that the request has been reviewed and approved by the SJA. The requestor will provide the following attached to the request:

(a) A signed affidavit by the agent with email addresses, date ranges, and any associated keywords or phrases as applicable. The affidavit will also provide confirmation of the authority of the investigating organization to request the search, the investigation number, a brief explanation of the nature of the investigation (that is, CI investigation), and written confirmation that legal counsel has approved the investigation.

(b) An appointment memo signed by the supervisor, agent-in-charge, or other chain of command official stating the requestor is assigned to the specific investigation and is authorized to request the Department of Defense Enterprise Email (DEE) search and receive the results.

(3) To retrieve DEE information, the investigating SA—

(a) Contacts the DEE Law Enforcement and Counterintelligence (LECI) requests section using the Non-Secure Internet Protocol Router Network (NIPRNET) at disa.dscc.eis.mbx.cols-leci-requests@mail.mil for NIPRNET email.

(b) Contacts the DEE LECI requests section using the SIPRNET at disa.dscc.opc.mbx.cols-leci-requests@mail.smil.mil for SIPRNET email.

(4) DISA will gather the information, convert it to a zip file, encrypt the file, then place it in a password-protected electronic drop box on NIPRNET or SIPRNET, and notify the requesting SA. Utilizing established command procedures, the SA will retrieve the email and create an ACOP ROI entry where the zip files provided by DISA will be saved as an attachment, along with a copy of the DISA email providing access to the files and any information on the associated cryptographic hash used for documenting file integrity. At no time will any SA open the zip file and review the emails on a NIPRNET- or SIPRNET-connected computer. If the requesting SA is unable to upload the files to ACOP, then they will contact their data transfer agent to have the files burned to compact disc (CD) and document the activity via DA Form 4137 (Evidence/Property Custody Document).

(5) Once the information is received by the requesting SA, their supporting CI cyber element will recover the files from ACOP and contact their data transfer agent to have the files burned to a CD for examination purposes. This examination will be conducted by CI cyber personnel certified, at a minimum, as a digital forensic examiner and conducted on a DA G–2 certified digital forensic workspace. All reviews will be conducted on stand-alone systems equipped to conduct digital forensic examinations.

Note. The CI cyber element will provide an ACOP ROI entry and technical report to the requesting SA.

e. National agency check.

(1) NACs are formal requests to Federal agencies for searches of their indices, databases, and files for information of investigative interest. NACs include DOD agencies, as well as other Federal agency holdings. SAs will request a NAC through their responsible operations management element, with the exception of National Crime Information Center (NCIC) checks. When available, SAs will use a local NCIC terminal in support of investigative activities. Military installation military police stations, PMOs, USACIDC offices, and installation security offices usually have an NCIC terminal. NCIC access can also be coordinated through liaison with local police departments and law enforcement agency joint task forces. The ACICA is the final authority for reviewing NAC requests. The ACICA is responsible for coordinating information requests for national-level intelligence community partners.

(2) NACs include, but are not limited to—

(a) DOD.
(b) DCII.
(c) DOD Inspector General.
(d) Defense Manpower Data Center.
(e) Defense Industrial Security Clearance Office.
(f) Directorate for Industrial Security Clearance Review.
(g) FBI.
(h) Criminal records.
(i) Intelligence records.
(j) FBI fingerprint checks.
(k) Bureau of Alcohol, Tobacco, Firearms and Explosives.
(l) The Federal prison system.
(m) Federal Aviation Administration, Department of Transportation.
(n) Social Security Administration.
(o) CIA.
(p) Department of Homeland Security.
(q) Immigration and Customs Enforcement.
(r) Transportation Security Administration.
(s) U.S. Coast Guard.
(t) Department of the Treasury.
(u) Internal Revenue Service.
(v) U.S. Secret Service.
(w) Department of State. Three elements under Department of State for NACs include the Security Division, Passport Division, and Intelligence and Research Division.
(x) Military Departments (Air Force, Army, Marines, and Navy).
(y) Army Crime Records Center (ACRC).
(z) USAIRR.
(aa) National Guard Bureau.
(bb) Office of Personnel Management.

f. Records checks coordinated by the Army Counterintelligence Coordinating Authority. Requests for information not covered by any of the checks or agencies in paragraph 3–1*e*(2) can be submitted to ACICA via an MFR or electronic mail, stating specifically the information sought and why the information is needed. The ACICA will assist in recommending specific checks and agencies to assist in finding the desired information. ACICA records checks requests must be pertinent to the predication, allegation, and objectives of the CI investigation (see table 3–1 for a listing of records checks coordinated by the ACICA).

Table 3–1
Records checks coordinated by the Army Counterintelligence Coordinating Authority

Record	Description
AKO Linguist Database	Contract linguist screening packets. This includes linguist application, SF 86 (Questionnaire for National Security Positions), screening results, and record check results. Linguist packets are also retired to the USAIRR. An investigation number with a code of “TC”

Table 3–1
Records checks coordinated by the Army Counterintelligence Coordinating Authority—Continued

	will be listed in DCII indicating that a linguist screening packet is available.
ACRC	USACIDC investigative records. A DCII check should be conducted first. If the ACRC file exists, the check should be completed.
Army G–2X, Collection Management	Request searches U.S. Army source registries to determine if the individual is an active, inactive, or terminated Army source.
USAIRR	Retired DOD case files and linguist screening packets for Category III linguists. A DCII records check must be completed first. Once it is known there was an investigation closed (submitted to the USAIRR) on the person of interest, an USAIRR records check could be completed.
Army Special Programs Directorate, SAP	This will provide whether or not the individual was read-on to a DOD (U.S. Army, U.S. Navy, U.S. Air Force, and so forth) SAP. Checks are of the Joint Access Database System and the Defense Contract Action Data System. Does not contain information about NSA or the National Reconnaissance Office (NRO) SAPs.
Bank letters	An official letter to a subject's financial institution to obtain account information. The letter must be addressed to a specific financial institution and point of contact (person or office). The letter must be reviewed and approved by the INSCOM SJA.
CLIP	CLIP contains information on contract linguists, to include name, social security number (SSN), date and place of birth (DPOB), NAC results, and company of employment. This information is obtained through the Linguist Screening Detachment.
Department of State Passport	This check provides information concerning passport applications and photographs. It does not contain travel-related information.
Department of State, Diplomatic Security Bureau	This check normally only contains information on current and former Department of State employees or personnel assigned to an embassy. However, it may contain CI information in the records of the Diplomatic Security and CI Office databases. It does not contain travel-related information.
DOD Central Adjudicative Facility	This check includes information that may be included in an individual's SF 86 request. Can also request JPAS incident reports. An incident in JPAS must be listed to request the report.
ACICA National Agency liaison officer	For information not covered by standard NACs listed below, ACICA liaison officers (for example, Joint Terrorism Task Force, CIA, DIA, or other) can request additional information. A request requires an MFR that identifies what type of information is desired and the agency to submit the request to.
CIA External Name Trace System	CIA External Name Trace System is a name trace system that searches the records of the CIA. This is the primary CIA check.
CIA, Stafford	Stafford only contains information on former and current CIA employees, applicants, and persons detailed from another organization to work for the CIA. This is an internal CIA security information system that contains biographical information, security clearance dates, type of investigation, and polygraph information. Only information owned by the CIA is released.
CLEAR NCR	NCR records checks include possible aliases, addresses, vehicles, liens and judgments, relatives, death records, utility services, phone listings, fraud alerts, driver's licenses, property ownership and deed transfers, criminal records and traffic citations, arrests, bankruptcies, lawsuits, business affiliations, voter registration, and marriage and

Table 3–1
Records checks coordinated by the Army Counterintelligence Coordinating Authority—Continued

	divorce records. This check is similar to LexisNexis and it may not be necessary to have both records. SAs should specify if both records checks are needed or one is preferred over the other.
DIA Counterintelligence Operations and Investigation Network	The records check includes checks of DIA CI investigative and operations files.
DIA Office of Security (SEC–4)	The Investigative Case Control System of SEC–4 and the Personnel Security Support System contains information on military Servicemembers, contractors, and civilian employees assigned, attached, or augmenting DIA.
DIA Defense Source Registry	The Defense Source Registry can identify if an individual has ever been used as a source by DOD.
Department of Homeland Security, U.S. Customs and Border Protection (CBP)	A CBP check provides information concerning travel to and from the U.S. This check includes passport or identification number used during the travel, dates of travel, airline, and flight number for inbound and outbound international flights. It may also include pedestrian and vehicular border crossing information. A request of a special research report may reveal if the individual was subject to additional secondary screenings or derogatory information observed by CBP while passing through a U.S. Customs screening point.
FBI	Requests for FBI database checks, including case files, which may provide information on criminal records, intelligence records, and fingerprint cards.
FinCEN	A FinCEN check may identify currency transaction reports and SARs. Currency transaction reports are filed by U.S. financial institutions for transactions of over $10,000 in cash. SARs are reports by U.S. financial institutions of suspected criminal activity. The SAR is only filed by a financial institution if a transaction by an individual appears suspicious.
LexisNexis	This check provides public records, to include aliases, address history, real estate records, voter registration, bankruptcy information, judgments or liens, relatives, neighbors, and associated entities. This check is similar to Accurint and Choice Point CLEAR, which are commercial records check agencies use to locate people, assets, businesses, and affiliations.
NSA	The NSA security database contains information on current and former employees or persons who have ever worked at or visited the NSA. This records check searches the NSA security database and internal CI database. The internal CI database includes information on CI investigations conducted by NSA. An NSA check can also identify if an individual has ever been indoctrinated for access to an NSA SAP.
NRO	An NRO check identifies if an individual has ever been indoctrinated for access to an NRO SAP. Before requesting the check, SAs should have a reasonable belief that an individual's duty positions (current and past) would require a read-on to an NRO SAP.
Traveler Enforcement Compliance System	A Traveler Enforcement Compliance System is the primary international air travel check. This check includes passport or identification number used when traveling, dates of travel, method of travel, airline, and flight number for inbound and outbound international flights.
U.S. Customs and Immigration Service (USCIS)	A USCIS check provides information on individuals who have immigrated to the U.S. This information is contained in an Alien File (A-

Table 3–1
Records checks coordinated by the Army Counterintelligence Coordinating Authority—Continued

	File). This check provides digital copies of the most pertinent immigration documents. A request for this check must include the specific information being sought (for example, identification of relatives, last foreign address, and other). The entire A-File is a lengthy document that can only be viewed by hardcopy at a USCIS office. The hardcopy should only be requested when absolutely needed.

3–2. Personal information records checks

Personal information records checks include medical, financial, commercial telecommunications, and commercial companies. Medical records comprise military and civilian records.

a. Military medical records.

(1) Medical record checks for active duty military are located at the supporting military medical treatment facility. In-patient and psychological treatment records may be retained at the facility that provided treatment and may not always be fully reflected in outpatient records. Retired and separated service member records may be located at the U.S. Army Reserve Personnel Center records facility in St. Louis. This type of records checks requires time to be completed. SAs will not gain direct access to the medical record itself. The analysis and assessment of the content within medical records are conducted by a medical officer or authority and the findings are provided to the agent. If the findings are provided in writing, they will be detailed in an ACOP ROI entry, attached as an exhibit, and documented in the investigative case file.

(2) Medical record checks are conducted when—

(a) Investigating a suicide.

(b) Information obtained indicates a subject was directed to counseling or treatment for a mental or medical condition such as substance abuse, gambling, depression, anxiety, or self-destructive behavior.

(c) Directed by operations management element or ACICA.

(d) Effects of prescription medications may potentially affect the results of a CSPE.

(3) SAs will not directly review medical records. A medical officer will conduct the review. Information in psychiatric evaluation files will not generally be made available to SAs. However, a medical authority will review and discuss the contents in general. SAs should brief the medical officer prior to the review concerning the type of information required for an investigative activity. The following information of the reviewing medical officer should be noted in the agent's notes for the subsequent investigative report: name, rank, position, and medical facility name and address. If medical records are in possession of the subject, the commander of the medical facility or the subject's commander should be discreetly contacted to have the medical records returned to the medical facility for review.

b. Civilian medical records.

(1) A warrant, subpoena, or written release from the subject is required to conduct a check of civilian medical records. Civilian medical records are considered privileged information and will not be released to investigators.

(2) Previously executed personal records release forms from personnel security investigations (DCSA or the Office of Personnel Management) will not be used by SAs during the conduct of CI investigations.

(3) If a medical records check is necessary during a CI investigation, SAs will coordinate with their responsible operations management element to obtain required approvals or warrants.

c. Financial records. The right to privacy extends to the financial aspects of a person's life. The U.S. financial system is complex and consists of several different types of institutions, each covered by different laws and regulations that restrict the Government's ability to access those records. SAs may access certain portions of financial data concerning a subject using the following authorities, exceptions, and procedures:

(1) Fair Credit Reporting Act (see PL 91–508 and 15 USC Chapter 41 Subchapter III) significantly restricts the ability of the Government to perform unconsented checks of consumer reporting agency records (credit reporting services). Usually these records can only be obtained with consent from the subject or by a warrant, administrative or judicial subpoena, or other court order. However, some financial information may be obtained if the following exceptions apply:

(a) Exception for identifying data (see 15 USC 1681f) allows all governmental agencies access to limited identification information from consumer reporting agencies based upon a formal written request. This exception allows ACI to obtain the name, address, former addresses, places of employment, or former places of employment for named consumers. This limited authority can be used for all authorized investigative and operational purposes.

(b) FBI CI exception (see 15 USC 1681u) allows the FBI a specific exception for disclosures for CI purposes. This does not apply to ACI. However, the FBI can provide this information to ACI during joint investigations. This exception also allows the FBI to provide information to the military for subjects who are under the purview of the UCMJ.

(c) Exception for international terrorism (see 15 USC 1681v) is a broad exception established by the Patriot Act (see PL 107–56), which allows a Government agency to conduct unconsented checks of these records. This exception applies to agencies authorized to conduct intelligence and CI investigations, operations, and analysis related to international terrorism. To use this exception, SAs must submit a formal written request certifying compliance with the code.

(2) Right to Financial Privacy Act of 1978 (see 12 USC Chapter 35) is the primary source of financial privacy rights and governs a broad spectrum of records across a wide variety of financial institutions. Government access to records of financial institutions may be obtained through consent, search warrant, administrative or judicial subpoena, court order or formal written request. Financial information may be obtained if FBI and terrorism exceptions (see 12 USC 3414(a)(1)(A) and 12 USC 3414(a)(1)(C)) apply. These exceptions allow a Government agency to conduct unconsented checks of these records. These exceptions apply to agencies authorized to conduct intelligence and CI investigations, operations, and analysis related to international terrorism. This exception may be used by SAs based upon a formal written request certifying compliance with the code.

(3) AR 190–6 implements DODI 5400.11 and DODI 5400.15 and provides additional guidance on obtaining information from financial institutions by consent, search warrant, judicial subpoena, and formal written request. This publication also provides sample templates for each type of request. AR 190–6 provides a specific exception for foreign intelligence and foreign CI and delegates signature authority for certificates of compliance with 12 USC 3414(a)(3) to MI group commander, investigative control office, or the Commanding General (CG) or Deputy CG, INSCOM.

d. Financial institution letters.

(1) A financial institution letter (also referred to as a bank letter) is used to obtain bank records (for example, bank account, brokerage account, or other). AR 190–6 provides guidance on accessing financial data for subjects of CI investigations. Bank letters provide the financial institution the information and legal citations necessary for them to comply with the law. They also certify (act as certificates) that the Government has met the standards required by the appropriate statute and that the request complies with the law. The certificate relieves the financial institution and its employees from any possible liability in connection with their disclosure of financial records.

(2) Under the provisions of the Right to Financial Privacy Act of 1978, ACI is authorized to officially request personal financial information from U.S. and U.S.-based financial institutions during the course of authorized CI investigative activities conducted under the technical control of the ACICA, DA G–2X, or DA G–2.

(3) Prior to exercising the authority under the Right to Financial Privacy Act, the CI investigative element must determine if the records can only be obtained through the consent of the subject. If requesting consent from the subject may compromise the investigation, the CI investigative element may pursue requesting financial information in accordance with the following process:

(a) Financial records may be sought when the investigation has reached a stage in which access to financial records are both necessary and appropriate.

(b) The bank letter is a formal letter that must—

1. Cite the specific authorities.
2. Contain the statutorily required certifications and nondisclosure statement.
3. Notify the financial institution that the Army will reimburse it for the reasonable costs associated with the search and reproduction of the requested records.
4. Include a statement that the formal request complies with the requirements of 12 USC Chapter 35.

(c) Upon receipt of the draft bank letter from the SA, the ACICA will review the case file to ensure that all reasonable and appropriate nonintrusive investigatory means have been exhausted and evaluate whether a request for financial records is a prudent operational step. If the ACICA concurs with the request, the request is forwarded to the Office of the SJA, INSCOM.

(d) Upon receipt by the Office of the SJA, INSCOM, an attorney who is familiar with the underlying basis for the investigation and the status of investigative activities will conduct a legal review of the draft bank letter. The attorney conducting the review will have full access to all investigative records and may confer with both the ACICA and requesting CI investigative element, as required. If operational or legal objections are noted during the review process, those objections will be brought to the attention of the ACICA and must be resolved before the bank letter may be staffed for approval and signature. If no operational or legal objections are noted during the review process, the draft bank letter is returned to the ACICA for staffing within the appropriate MI brigade or group. Upon completion of the internal brigade or group staffing process, the bank letter will be presented to the brigade or group commander for

signature. The commander (for example, 902nd, 513th, 66th MI Group), ACICA chief, or CG or Deputy CG, INSCOM are the only signature authorities for bank letters.

(e) Upon receipt of the signed bank letter, the investigating SA will deliver the letter to the appropriate financial institution officer. The SA is responsible for determining the appropriate bank letter delivery method. Hand delivery is generally the preferred method. However, some financial institutions will only accept delivery by other means (for example, facsimile, email, or other). The SA will request both hard and soft copies of the information. The officer at the financial institution will provide the information directly to the SA, and it will not be mailed.

(f) The requesting agent will ask the financial institution officer for an invoice for the cost of services. Upon receipt of the invoice, the agent should verify that the invoice is correct, completely remove all personal subject data, and submit it to the respective resource management office. The resource management office will prepare SF 1034 (Public Voucher for Purchases and Services Other Than Personal) using the specific fund site and send it to Joint Field Support Center for payment. If the institution bills the unit for services, then the agent submits a memorandum requesting ICF advance to the Group ICF Class A agent to pay for services. The memorandum must state the institution refused to provide a bill and indicate the required data for the cash advance. The agent will submit DA Form 3697–R (Sub-voucher for Distribution from Confidential Funds) to the Class A agent.

(g) If SAs receive information from a financial institution that is outside the scope of the information originally requested or if the information is otherwise nonresponsive, the investigating SA will destroy the nonresponsive information and recontact the institution to explain the nature of the discrepancy and ask for the information as originally requested in the Army bank letter. Destruction of the nonresponsive material will be detailed in an ACOP ROI entry and documented in the investigative case file.

e. Marking of responsive financial information. Any responsive financial information received as a result of the use of this authority will be clearly identified in ACOP as personal financial information and will be marked with the following language: "Information contained in this report is financial record information obtained pursuant to the Right to Financial Privacy Act of 1978, 12 USC 3401 (et seq). This information may not be released to another Federal agency or department outside the DOD without compliance with specific requirements of 12 USC 3412 and AR 190–6."

f. Financial Crimes Enforcement Network checks.

(1) FinCEN checks are considered NACs. The ACICA is the only ACI element authorized to coordinate FinCEN checks. ACI only requests FinCEN checks on U.S. persons who are subjects of an open investigation. The required information to conduct a FinCEN database check is—

(a) ACICA case control number subject's name.

(b) SSN.

(c) Justification from the requesting CI element for conducting the check.

(2) FinCEN reporting results usually consist of either a currency transaction report or the SAR. This may also be referred to as a bank SAR. There are different types of currency transaction reports and the names or types may change or be added. FinCEN has the capability for analytical support, research, and products. However, complex money laundering and money trails are usually not associated with ACI investigations. The SAR allows SAs to develop leads and obtain underlying documents from the financial institution (for example, deposit slips, wire transfer records, or other) that are used as evidence in the investigation.

(3) When reporting FinCEN-derived information, it is important to note restrictions involved, especially concerning the SAR. The following provisions apply to SAR information:

(a) SAR information is used only for official purposes.

(b) SAR information cannot be provided to law enforcement without subpoena.

(c) Referenced in any CI report or document such as ACOP ROI entries, ROIs, memoranda of interview, affidavits, indictments, warrants, or subpoenas. The ACOP ROI entry should only reflect that lead information was found during a FinCEN check.

(d) Used during source or witness interviews or SIs.

(e) Provided to other individuals (for example, command or senior leader briefings).

(f) Protect SAR source information. SAR information is for lead generation purposes only and must be treated as protected confidential source information.

(g) Understand that SAR information does not provide substantiating information concerning a subject. SAR information is the opinion of a bank employee that is providing the information with the expectation that it will be confidential. The information is uncorroborated opinion and ACI is not allowed to use it outside of the guidelines provided by FinCEN.

(h) Generally may not be used in open court (if necessary the ACICA will coordinate with the FinCEN's Office of Chief Counsel for guidance).

g. Department of the Treasury suspicious activity report information guidance. SAR information is not to be treated the same as other financial records. The difference between financial records and SAR information is that financial records are considered factual statements in court. SAR information is viewed as coming from a confidential informant where the bank teller or individual who completed the SAR is afforded confidentiality to protect their identity. Information provided in SARs will be used for lead generation only. Failure to comply with the rules and regulations regarding security of the data and FinCEN will result in the immediate dismissal of requester of information and possibly the Army from the FinCEN program.

h. Reporting currency transaction report information. When reporting information concerning the currency transaction report information, the following caveat should be included in the report: "The enclosed information was collected and disseminated under provisions of the Bank Secrecy Act (BSA) and U.S. Department of the Treasury regulations implementing the BSA. See 31 USC 5311, et seq.; 31 CFR Chapter X. The information is sensitive in nature and is to be treated accordingly. The information may be used only for a purpose related to a criminal, tax, or regulatory investigation or proceeding, or in the conduct of intelligence or counterintelligence activities to protect against international terrorism, or for a national security matter. See 31 USC 5311. The information cannot be furthered released, disseminated, disclosed, or transmitted without prior approval from the Director of the Financial Crimes Enforcement Network or their authorized delegate. SARs filed under the BSA must be treated with particular care given that they contain unsubstantiated allegations of possible criminal activity, akin to confidential informant tips. Such reports, or the fact they have been filed, may not be disclosed by a Government employee to any person involved in the transaction, other than as necessary to fulfill the official duties of such officer or employee. See 31 USC 5318(g)(2)(A)(ii). Unauthorized release of information collected under the BSA may result in criminal or civil sanctions."

i. Commercial telecommunications records.

(1) Communication is present in most of the national security crimes we investigate. The ability of SAs to obtain telecommunications records is critical to the investigation. Telecommunications technology (for example, email, cellular telephones, instant message, or other) has proliferated in recent years. This provides an increased pool of information to support CI investigations. However, the Government has not been able to update statutes and policy to address new technology due to the rapid pace of telecommunications development and increased public use.

(2) Accessing telecommunications records in support of a CI investigation is focused administrative information (for example, toll and transactional records) and not the content of the communications themselves. Access to real-time content of telecommunications is electronic surveillance and requires the approval of DODM 5240.01 and AR 381–10 special investigative techniques. The investigative objectives telecommunications records checks include—

(a) Identification of accounts associated with subject.

(b) Identification of subject's associates and their accounts and numbers.

(c) Identification of locations of stored telecommunications content (also referred to as records at rest).

(d) Preservation of stored telecommunications until they can be recovered through warrant, subpoena, or other appropriate mechanisms.

j. Electronic Communications Privacy Act. PL 99–508 governs access by governmental agencies to nonofficial toll and transactional records. It severely restricts nonconsensual access to nonofficial telecommunications records and prohibits access to the content of stored telecommunications, which can be obtained only with consent or by warrant, administrative or judicial subpoena, or court order.

k. Federal Bureau of Investigation counterintelligence exception. Section 2709, Title 18, USC provides an exception to the FBI to obtain telecommunications subscriber data and toll and transactional data from commercial providers for use in CI investigations. The FBI may obtain nonconsensual access to toll and transactional records with a formal written request certifying compliance with the code. This exception is reserved solely to the FBI and cannot be exercised by SAs even during the conduct of joint investigations. An FBI agent must be present to serve the certificate and take custody of the records.

l. Preservation letters. Although ACI does not have the authority to directly obtain nonconsensual access to telecommunications records or content without a warrant or subpoena, it does have the ability to compel the telecommunications provider to preserve such records by preventing the destruction or inadvertent deletion until the necessary authorizations can be obtained. This authority is contained in 18 USC 2703(f). A formal written request in the form of LHM is the mechanism to notify a provider of the need to preserve evidence. While any CI agent may sign such a request, it is ACICA policy that the SA in charge of an office or unit commander signs the memoranda. Preservation letters should be served as soon as practical upon the discovery of telecommunications accounts of interest. In joint cases, coordinate with the FBI to determine who will serve the preservation letter.

m. Commercial company records.

(1) There are commercial company records outside the heavily regulated financial and telecommunications areas that may be of interest to the investigating SA (for example, travel-related vendors and institutions). Obtaining information on airline, train, or rental car usage by subject can be critical to a CI investigation. Some related information can be obtained via financial institution records. However, if that avenue is not available or if more detail is required, a request to the travel service provider is appropriate.

(2) Since specific privacy rights have not been afforded to general commercial records, companies are free to allow access to records consistent with company policy. ACI is free to request voluntary disclosure of these records from the company. The usual mechanism for such a request is a formal memorandum. However, if a verbal request will be honored by the company, then that technique can be used. While formal request memoranda are carefully worded to encourage cooperation, it is important to note that such cooperation is strictly voluntary. If a company refuses to provide voluntary access, a warrant or court order is the only means of compelling them to grant access.

Chapter 4
Counterintelligence Interviews

An interview is a process that SAs use to obtain information verbally from people associated with or who have direct knowledge relevant to a CI investigation. It occurs during a personal meeting between SAs and the person who has information concerning the investigation. Interviews are used to further develop information to refute, mitigate, or resolve allegations of a national security crime or incident of CI interest.

4–1. General interview techniques

a. Types of counterintelligence interviews. Interviewing persons knowledgeable of, witnesses to, or involved in alleged national security crimes or incidents within ACI purview is the basis of all CI investigations. Interviews can successfully resolve suspected allegations when conducted meticulously and with all legal requirements or can jeopardize the ability to neutralize or exploit threats to national security. There are three types of CI interviews—

(1) Walk-in.

(2) Witness.

(3) Subject.

b. Preparation for counterintelligence interviews. A thorough preparation for interviews is critical to establishing the SA's authority and professional credibility to interviewees. While walk-in interviews cannot be planned, the SA's knowledge of procedures, laws, policies, and investigative techniques will assist during walk-in interviews. Planning and preparation are critical to conducting a successful interview. Each type of CI interview has a different focus and unique planning considerations.

c. Interview plan and agenda development.

(1) A written interview plan is a good technique for witness and SIs. Developing an interview plan includes reviewing the case file, identifying investigative objectives that should be addressed during the interview, and developing a questioning plan to ask the necessary questions to meet those objectives. The SI requires an approved SIP (see paras 2–14, 2–39, and 2–41*b*) prior to conducting of the interview. SAs should try to learn as much about the interviewee (witness and subject) as possible prior to the interview. This includes the interviewee's age, gender, background, and personality. These demographics can help SAs plan and develop an approach for a specific interviewee.

(2) An interview agenda is another type of investigative aid that allows investigating SAs to decide how they want the flow of the interview to go. Interview agendas allow investigating SAs to manage the interview and serve as a road map to key SAs on the completion of mandatory documentation and security warnings required during the interview process.

(3) Interviews are conducted based upon the experience level of the investigating SA and how they like to transition between different topical areas. For example, some investigating SAs like to complete all administrative documentation (that is, Privacy Act advisement and secrecy affirmation) at the beginning of the interview, then complete information exploitation and followup with executing DA Form 2823 (Sworn Statement) and final security warning. Other investigating SAs may prefer to conduct all the information exploitation, obtain witness data, cover all administrative documentation, and then execute the sworn statement and issue the security warning.

(4) When using interview agendas, the investigating agent should always keep it concealed or out of sight. If a witness recognizes the agent is relying on this document to complete the interview, it may undermine the credibility and professionalism of the investigating agent and may result in the witness being more cautious, confrontational, or uncooperative. The amount of detail the agenda contains is left to the discretion and amount of experience of the investigating SA. The following is an example of an interview agenda:

(a) Identification witness.

(b) Present badge and credentials.
(c) Synopsis of the information.
(d) Detailed account of the incident by the witness.
(e) Use of interrogatives.
(f) Privacy Act of 1974.
(g) Secrecy affirmation.
(h) Sworn statement.
(i) Security warning.

d. Witness or subject assessment. After the initial walk-in, the investigating SA will begin preparing for follow-on source and potential SIs. SAs must anticipate and mentally prepare for the interviews, which include assessing credibility and anticipating demeanor.

e. Assessing credibility. In most cases, except walk-ins, SAs will have to locate and convince the witness to cooperate with and provide information to ACI. Some witnesses will be cooperative and credible. Others will have to be persuaded and may intentionally lie. Some factors to consider in understanding and determining a witness's credibility are—

(1) *Physical condition.* The physical condition of witnesses at the time of the incident under investigation and at the time of the interview can affect the information that is developed during the interview. For example, fatigue, illness, or loss of hearing or eyesight may affect the witness's perception of what they observed or heard.

(2) *Mental condition.* Mental issues may also affect a witness's perception and the context of the information the witness may have. This includes mental factors such as stress or apprehension over being interviewed and medically diagnosed mental illness.

(3) *Age.* Age also affects credibility. Children have a tendency for exaggeration while elderly people may have impaired memory function.

(4) *Objectivity.* Strong personal prejudices influence the way people see and remember things. These biases can be witting or unwitting and careful questioning may be required to uncover them.

(5) *Time.* The more time that has elapsed between the incident and the interview, the more details the witness will likely forget. This usually results in the witness using their imagination or experiences to fill in the gaps and potentially distort the story.

(6) *Motivation.* A witness's motivation or hidden agenda will also affect the context and how they present the information. Fear, revenge, jealousy, protection of self or family, and personal gain are all potential motivations that could affect the credibility of a witness.

f. Subject interview rehearsal. During rehearsals for the SI, SAs should include hypothetical situations. For example, the subject may state they did not do it, refuse to talk, admit they are guilty, become hostile or confrontational, or confess to another crime. SAs should be prepared to handle any of the situations that may arise, know what their authority is, and be prepared to exercise that authority.

g. Anticipating demeanor. SAs have to anticipate the demeanor of the witness when conducting their pre-interview planning. Cooperative interviews usually will yield more information. The demeanor of a witness may also change during the course of an interview. SAs with good interpersonal skills can usually control the pace and influence the witness's demeanor with the proper use of interview techniques. Directly confronting or exhibiting suspicion of a witness may result in a hostile interview.

(1) *Cooperative interview.* An interview where the interviewee voluntarily and willingly participates in the interview. The majority of all witness interviews fall within this category. SIs may also be cooperative, especially where subject is volunteering information to refute, mitigate, or explain allegations.

(2) *Hostile interview.* If interviewees are resentful of people in authoritative positions or have a close relationship with the subject, they may be uncooperative and hostile during the interview. The investigating SA should be firm, but professional, and establish authority. SIs are often uncooperative or hostile. People confronted with allegations of criminal activities are naturally defensive and confrontational. Senior-ranking subjects may be resentful of an interviewer or accuser whom they perceive is junior to them in age or rank. The investigating SA should anticipate hostile reactions during SIs, however, these reactions should not affect professionalism or tactfulness during the interview. The SA's professionalism, knowledge, and interpersonal skills are instrumental to managing the interview.

h. Telephonic contact with witness or subject. When making telephonic contact with a witness or subject to arrange for or to coordinate an interview, the investigating agent has to balance security of the investigation while providing the minimum amount of information to induce cooperation. The SA should conduct telephonic contacts as follows:

(1) *Identification.* SAs will identify themselves and ask for the prospective witness or subject by rank (if military) and full name. SAs will identify themselves by name and unit only after the witness's or subject's identity has been

confirmed. Afterwards, the SA will identify themselves with the title "SA" followed by their "last name" instead of "SA."

(2) *Witness or subject identification.* SAs will verify that they are talking to the prospective witness or subject.

(3) *Reason for contact.* SAs will explain they are investigating or conducting an inquiry into a security matter and that they would like to arrange to speak with the interviewee. Using verbiage like "a matter of national security," "SA," or "CI investigation" may spook the prospective witness or subject.

i. Telephone operations security. SAs will never provide details of a CI investigation over the phone to a witness or subject. Prospective witnesses or subjects may believe they do not have any knowledge of an incident or security-related matter. SAs needs to stress the importance of the interviewee's cooperation and that the prospective witness or subject would be assisting in resolving a sensitive security matter.

(1) *Establish interview.* Establish the date, time, and location of the interview and ensure the prospective witness or subject has directions to the interview. Ensure the prospective witness or subject understands that the interview may last 1 to 2 hours. If the prospective witness or subject is hesitant about being away from their place of employment for that long, offer other alternatives such as during lunch or before or after duty hours.

(2) *Provide security warning.* The prospective witness or subject should be advised of the official nature of the interview and that they are not to disclose their cooperation with anyone, including their supervisor. If they are adamant that their supervisor or chain of command should know, the SA should obtain contact data for those persons and coordinate with the ACICA regarding these contacts.

(3) *Provide recontact information.* SAs provide their official cellular or telephone numbers should the prospective witness or subject need to contact them before the scheduled interview.

(4) *Summarize.* Reiterate a security warning, date, time, and location of the interview and thank the interviewee for their time.

j. Use of interview aid.

(1) CI investigative interviews are complex and time consuming. Regardless of the level of experience, investigating SAs should never go into an interview thinking they will be able to remember all the different protocols, legal warnings, and documentation required to complete an interview and still be able to effectively exploit all the information a witness or subject may know.

(2) Investigative aids, such as the interview aid, assist in the exploitation of information. The most commonly used investigative aids include known and unknown person, location, and vehicle identification sheets. Aids allow CI agents to fully identify persons involved in the incident who can assist with future investigative activities, including records checks, and help in completing all documentation required during the investigation. SAs may also develop investigative aids for actions and objects (such as documents and electronic media) as these may likely be a part of a CI incident (see appendix C for additional investigative aids and table 4–1 for an interview aid to assist in fully identifying known persons, unknown persons, locations, and vehicles).

Table 4–1
Interview aid

Known person identification	Unknown person identification	Location identification	Vehicle identification
Name – first, middle, and last	Sex (male or female)	Room number and name	Make
DPOB	Race (for example, Asian, Black, Caucasian, Hispanic, or other)	Floor number	Model
Residential address	Skin color (for example, dark, tan, or white)	Building number and name	Year
Rank and title	Skin complexion (for example, smooth or pock-marked)	Street address or geographic coordinates of location	License plate number
Military component	Age (within a 5-year range)	Nearby landmarks	License plate state
SSN	Height (within a 2-inch range)	Surrounding area description	Color
Duty position	Weight (within a 10-pound range)	Installation, city, or town	Distinguishing characteristics (for example, stickers or damage)

Table 4–1
Interview aid—Continued

Unit of assignment	Build and posture (for example, small, medium, or stooped)	State or province	U.S. military installation
Installation	Hair (for example, black, blond, brown, grey, red, or bald)	Country	
Work address	Eyes (for example, black, blue, brown, green, or grey)	ZIP code	
Permanent change of station date	Dress (for example, headwear, upper- to lower-body wear, footwear, or jewelry)		
Expiration of term of service date	Distinguishing characteristics (for example, physical handicap, tattoos, body piercing, birthmarks, moles, or other)		
Security clearance			
Level of daily access			
Special access – SCI only			

k. Interview room setup.

(1) It is important to determine what physical setting or environment will be most conducive to gaining the trust and confidence of the witness and will produce the most truthful and meaningful information. Interviews can be and frequently are conducted in a myriad of settings, locations, and environments. It is completely acceptable to conduct an interview at a witness's place of work, home, or other location where they may feel more comfortable. Comfort sometimes allows a subject to talk more openly and freely, which can greatly benefit the investigative process.

(2) The SI must be strictly planned and controlled. The location selected for the SI should provide complete privacy (free from distraction or disruption). Interview rooms should not be equipped with phones, outside windows, wall ornamentation, and so forth. In addition to these requirements, the room should be strategically arranged to ensure the most practical and conducive environment. If the room is equipped with a one-way mirror, the subject should not face directly toward it. This serves as a constant reminder that someone may be monitoring the interview.

(3) Interview rooms should be equipped with a desk and at least three chairs if using an assisting agent or four chairs if an interpreter is used. The interviewing SA should be located directly across from the interviewee. If an assisting agent is used for notetaking or witnessing, they should be located to the side of the interviewing SA, far enough away so they are not in direct line of sight of the interview.

(4) When possible, the interview chair should be a four-legged chair with no armrests. This removes any potential psychological barriers or defense mechanisms and allows for easier recognition of body posture and physiological indicators of deception during the interview. If using an interpreter, they should be placed to the side and slightly behind the interviewee to ensure that their focus is directed towards the investigating SA. If the room is equipped with video recording equipment, it should be mounted in a corner with visibility on the interviewee's face, yet still out of direct eyesight so that it is not a distracter.

l. Recording of interviews.

(1) A careful risk or gain assessment must be done to ensure the benefits expected by taping the interview outweigh potential risks to the investigation. There is a significant logistical and administrative burden involved with such activities.

(2) When the intent of an investigation is to prove a criminal act, a written report accompanied by an incriminating signed sworn statement (DA Form 2823) is sufficient. No value is added by including a recorded confession. More often than not, the recording becomes a target for the defense to accuse wrongdoing on behalf of the investigating agency or prosecution. Interviews and debriefings of subject as part of a plea bargain or after the trial is complete for conducting damage assessment are common. Taping interviews should be considered when—

(a) Interviews are conducted in foreign languages.

(b) An interpreter is used.

(c) Interviews are lengthy.

(d) Interview topics are technical or extremely complicated in nature.

m. Information development.

(1) At the beginning of an interview, the investigating agent will have the interviewee provide a detailed explanation of the incident starting with the earliest relevant date and time concerning the incident. The investigating SA will not interrupt and will take very few notes. This helps the interviewee refresh their memories and mentally recount the incident. After this initial dialogue, the investigating agent will have the interviewee go back to the beginning of the incident and slowly have them recount the details while the investigating agent takes detailed notes.

(2) This interview sequence applies primarily to walk-in complainant, witnesses, and others knowledgeable. Because SIs are choreographed to set the desired conditions, SAs can only utilize this interview sequence once the subject begins to provide information that refutes or mitigates the allegation. This specific point is hardly ever expected to occur at the beginning of the interview, but SAs must be ready in case the subject commences providing information.

(3) The interview should flow sequentially to develop a logical timeline of what happened. As the interviewee provides details concerning the incident and reveals other information, the SA should make a note and follow-up with a separate line of questioning of that new lead or issue after the current topic has been fully exploited.

(4) When asked for specific dates, times, and locations, the interviewee may not be able to provide exact information. In this case the investigating SA needs to identify the details as precisely as possible. If the interviewee cannot remember a specific date, the agent needs to gradually broaden time spans to a day of the week, week, month, time of year, or even season to get the most precise information available.

n. Questioning techniques.

(1) How an investigating SA asks questions in an interview is also important. Good questioning techniques limit confusion of the interviewee, maintain the tempo and control of the interview, and save time by limiting repetitive clarifying questions.

(2) Direct questioning using the basic interrogatives (who, what, when, where, why, and how) is the most efficient way to exploit information in most interviews. Investigating SAs will never use compound or leading questions. SAs should limit the number of questions that can be answered by a simple yes or no. Instead, they should ask questions that require lengthy responses. The investigating agent should avoid asking questions like these—

(a) Wrong. "Can you spell John's name?" This creates two questions and two answers. The initial question and the answer, which will usually be yes or no, and the followup question, "Spell John's name."

(b) Right. Spell John's name.

(c) Wrong. "You saw John take the classified document home, right?" This is a leading question because the question prompts the desired answer.

(d) Right. "Who took the classified document home?" "Did you see John take the classified document home?"

(e) Wrong. "Was John in the office and who was with him?" These are two questions at once. Separate questions by allowing the interviewee to respond.

(f) Right. "Was John in the office?" After the answer, ask the followup, "Who was with him?"

(3) Elicitation is the use of generalized questions to ascertain someone's knowledge on a particular topic. In some cases of witness interviews where it is unknown whether the interviewee has knowledge concerning the incident, it may be necessary to begin elicitation to ascertain their knowledge of the incident. If the interviewee has no information concerning an incident under investigation, then the investigating SA will not have given away any circumstances surrounding the incident that could be compromised later on.

(4) To elicit an interviewee's knowledge, SAs may ask, "Do you know of any security incident that may have happened in a specific timeframe?" "Where were you on this date?" "Did you notice anything suspicious on that day?" Once the interviewee has acknowledged knowing about the incident in question, the investigating agent may then begin asking direct questions.

o. Backup information. Part of the interview preparation is to have prepared copies of all administrative and legal documentation that may be required in a particular interview. These include copies of the Privacy Act of 1974, sworn statement (DA Form 2823), DA Form 3881 (Rights Warning Procedure/Waiver Certificate), consent to release forms, and secrecy affirmations. The investigating agent should have multiple blank copies of all these documents available, as well as multiple copies that have all areas that require signatures or initials highlighted to ensure they are properly documented during the interview. Copies of DA Form 3881 should also be available during walk-in, source, or witness interviews since there may be times when these interviewees, although cooperative, may implicate themselves in a criminal offense. During SIs, investigating SAs should also have a copy of all charges (18 USC and UCMJ) available to explain why their suspected actions are viewed as criminal offenses.

p. Notetaking.

(1) Accurate, detailed, legible, and properly sequenced notes are critical in articulating the information obtained during all interviews. During the interview, as information is developed, if the interviewee provides another lead or issue that requires exploitation, make a note in the margin, fully develop the current topic, and go back and exploit the lead or string provided earlier. This helps maintain the tempo of the interview, limits interviewee confusion by disrupting a sequence of events, and makes it easier to transcribe the notes into a report or sworn statement. If the interviewee is providing details about a specific event and mentions a name, for example, "John," do not interrupt to request John's personal identifying information. Make a note. After exhausting the current topic, go back and follow-up with questions concerning John.

(2) The organization of notes is also important. Depending upon the anticipated amount of information and level of detail associated with it, SAs may choose to write about only one topic per page or multiple topics per page. Generally, the longer the interview, the greater the number of topics to be discussed or the higher level of detail the information will be on each topic. In such cases, it is good practice to record just one topic on any one page of notes. If more pages are needed to record information on a particular topic, begin the next and subsequent topics on separate pages. While this may leave a lot of empty space in the SA's notes, a major benefit to this practice is to leave room to add more information on a particular topic immediately next to the other information already collected on it should a witness provide more information on that topic later in the interview. Recording notes in this manner offers the following advantages:

(a) It minimizes the number of times SAs have to write information on one topic at different locations within their notes.

(b) The notes are more organized and accurate, making it easier for SAs to find information in their notes.

(c) Conducting followup questioning on each topic is easier and more accurate because all the information relating to one topic is grouped together.

(d) Others reading the notes can quickly and easily locate and understand information on one topic.

q. Identification of indicators of deception. Detection of deception is not a simple process and it normally takes years of experience before SAs can readily identify deliberate deceit. Inconsistencies in the witness's actions or words do not necessarily indicate a lie, just as consistency is not necessarily a guarantee of the truth. However, a pattern of inconsistencies or unexplainable inconsistencies normally indicate deceit.

r. Internal inconsistencies.

(1) Frequently, when an interviewee is lying, the investigating SA is able to identify inconsistencies in the timeline, the circumstances surrounding key events, or other areas within the questioning.

(2) During time inconsistencies, the interviewee may spend a long time explaining something that took a short time to happen or a short time telling of an event that took a relatively long time to happen. These internal inconsistencies often indicate deception.

(3) Body language does not match verbal message. An extreme example of this would be the interviewee relating a harrowing experience while sitting back in a relaxed position. The investigating SA must be careful in using this clue since body language is culturally dependent. Failing to make eye contact in the United States is considered a sign of deceit while in some Asian countries it is considered politeness.

s. Lack of extraneous detail. Often false information will lack the detail of truthful information, especially when the lie is spontaneous. The investigating agent needs to ask followup questions to obtain the details. When the interviewee is unable to provide the details that they know or are expected to naturally know, it is an indicator of deceit. If the interviewee does provide this additional information, it must be checked for internal inconsistencies and verified by repeat questions.

t. Repeated answers with exact wording and details. Often in the case of subjects, if a subject plans to lie about a topic, the subject will memorize answers or details. If the interviewee always relates an incident using exactly the same wording or answers repeat questions identically (word for word) to the original question, it may be an indicator of deceit. In an extreme case, if the interviewee is interrupted in the middle of a statement on a given topic, they will have to start at the beginning to "get their story straight."

u. Physical cues.

(1) The interviewee may display physical signs of nervousness such as sweating or nervous movement. These signs may be indicators of deceit. The fact that an individual is being questioned may be, in itself, cause for some individuals to display nervousness. The investigating agent must be able to distinguish between this type of activity and nervous activity related to a particular topic. Physical reaction to a particular topic may simply indicate a strong emotional response rather than lying, but it should key the agent to look for other indicators of deceit.

(2) The interviewee may fail to answer the question asked. When an interviewee wishes to evade a topic, they will often provide an evasive answer and not in response to the question asked. For example, if the interviewee is asked, "Were you in the office when the document was taken?" and interviewee replies, "I was in the office that day," they

have truthfully answered a question, but have avoided being put into a position that may implicate them in the incident. In addition, when a person repeats a question, it may be a stall tactic while they try to think of a plausible answer to the question.

v. Witness confidentiality. Witnesses, even walk-ins, may be reluctant to talk to SAs based on a fear of becoming involved in a legal proceeding or having to face cross-examination or reprisal by the subject or agency or unit's chain of command. Rapport-building, reassurance, appeals to duty, and encouragement to do the right thing are the preferred method for obtaining cooperation. However, if a witness is still apprehensive about cooperating, under the provisions of the Privacy Act of 1974, investigating SAs can protect witness's identity and grant confidentiality to ensure the witness's identity is not revealed outside official or law enforcement channels. This protection would include any documentation petitioned from external agencies outside law enforcement and military channels under the FOIA. The Privacy Act of 1974 caveat and requests for confidentiality will be annotated within investigative reports. Confidentiality should be offered as a last resort and not until it is apparent to the investigating SA that rapport-building, reassurance, appeals to duty, and encouragement to do the right thing do not dissuade the witness's reluctance to provide answers to the investigating SA's questions.

w. Required verbal warnings during counterintelligence interviews. The following verbal warnings are required during interviews:

(1) Security warning. Administer to all interviewees after each interview session. "The matter that we have discussed today is regarded by the DA as extremely sensitive in nature. To protect the integrity of this investigation, we request that you not discuss this matter with anyone outside the official investigative channels of this office. Thank you for your cooperation."

(2) Followup security warning. Administer at the end of followup interviews with the same person. "I want to thank you again for not discussing this official and very sensitive matter with anyone outside the official investigative channels of this office."

(3) Telephonic security warning. Administer at the end of an interview coordination telephonic contact with witnesses or subjects. "Despite the fact that I have provided you with limited information concerning this matter, I ask you not to discuss this matter outside the official investigative channels of this office. Thank you for your cooperation."

(4) Consent to release under the FOIA. Use this warning for walk-in and witness interviews only. "I need to inform you that the information we have discussed today will be made into an official report and that report will become part of official U.S. Government files. Under the provisions of the FOIA, any U.S. person mentioned in this report may request a copy of those files once the case is closed, adjudicated, and made a part of official U.S. Government records. Do you have any objections to having your name released as the provider of this information?"

(5) Oath of truthfulness for SIs. Administer to subject at the beginning of the initial and followup interviews. "The DA desires that this interview be conducted under oath. Are you willing to be interviewed under oath? Do you swear or affirm that the information you are about to provide in this interview is the truth, the whole truth, and nothing but the truth?"

(6) Sworn statement oath of truthfulness. Administer just prior to the person making a statement signing the affidavit section of the sworn statement (DA Form 2823). "Please raise your right hand. Do you swear or affirm that the information you have provided is the truth, the whole truth and nothing but the truth?"

4–2. Walk-in interview

Interviewees are regarded as walk-in complainant when they have knowledge of a national security crime or incident within the purview of ACI and they voluntarily report the information to ACI. The walk-in interview consists of—

a. Approach.

(1) The approach phase of the interview allows the SA to confirm the complainant's identity, assess the complainant's motivation for reporting the information, and identify physical or emotional triggers that may be manipulated by the SA to induce the complainant's cooperation. During the approach phase of a walk-in interview, SAs will—

(a) Invite the complainant into the CI office. SAs do not have to identify their agent status or military affiliation at this time. For example, "Hi. My name is John. What can I do for you?"

(b) Allow the complainant to provide a brief summary of the incident they wish to report. Do not take detailed notes at this time because the information may not be in CI jurisdiction.

(2) Any complainant (walk-in, telephone caller, or written message) who volunteers information, the collection of which is unauthorized by DODM 5240.01 or AR 381–10, will be referred to the proper authorities. These witnesses and the information they provided are referred to as unsolicited complainant and unsolicited information. If possible, all unsolicited complainant will be fully identified and, if the information volunteered is of no interest to Army intelligence but may be of interest to another agency, the complainant will be referred to the appropriate agency.

(3) Once it is determined that the complainant has a genuine need to talk to the SA, the SA will present their badge and credentials to the complainant. The SA should then request the complainant's military identification card or picture identification to verify their identity. The complainant's identity will be cross-checked against the local known nuisance databases even if the information is of interest to MI.

(4) No walk-in is ever turned away even if they have been previously identified as a nuisance.

b. Information development. This phase allows the SA to obtain all the information concerning an allegation of a national security crime or incident CI interest. This includes—

(1) *Fully developing all information.* SAs should begin by having the complainant retell their story from a point in time prior to the allegation or incident to the time they began the interview. The complainant should be instructed to expand upon what they initially told to the SA in detail. During this time SAs, may ask questions to help logically guide the interview, maintain an efficient tempo, and prompt the complainant to provide other details concerning data on vehicles, persons, locations, or activities. After all the information has been fully developed, review notes with the complainant to ensure all information has been accurately annotated. Ask the complainant if they have any further information to add.

(2) *Identifying leads.* Ascertain who else was in the area at the time of the incident or who else has knowledge of the incident. Attempt to identify these individuals and where they work. By talking to several people that were in the area at the time of the incident, facts may be obtained, discrepancies clarified, and a logical conclusion can be made.

(3) *Developing espionage and insider threat indicators.* Fully develop any espionage indicators. Espionage indicators provide a general idea as to the type of individual that may be investigated. The complainant may not have personal knowledge of the subject. However, ask the complainant if they have any knowledge about the subject concerning the following:

(a) Finances. Have they received any letters of indebtedness or unpaid bills? Do they have any financial problems? Do they have a problem paying bills? Do they appear to be spending more money than they make?

(b) Lifestyles. Do they live life "in the fast lane?" Are they quiet individuals who keep to themselves? What interests do they have? Do they have a highly social life?

(c) Hobbies. Have they ever talked about their likes or dislikes outside the workplace? Do they collect any objects? Do they belong to any organizations outside the military?

(d) Associates. With whom do they associate during the duty day? With whom do they associate after duty hours? With whom do they work? Who can provide more information concerning subjects?

(e) Foreign connections. Do they have any U.S. relatives living abroad? Do they have any foreign contacts or business connections or own any foreign property?

(f) Foreign travel other than official military travel. What foreign travel have they taken? Where do they go? How often do they travel? What are their reasons for traveling abroad?

(g) Loyalty and allegiance. Do their personal beliefs, statements, actions, or associations indicate they may not be loyal to the U.S. military or Government?

(h) Work habits. Do they have the combinations to the security containers in the office? Have they ever had any security violations? Do they volunteer for extra work? Do they volunteer for sensitive assignments? Do they excessively use the copier? Have they ever been cited for a security violation? Do they often work late or come in to work early? Are they signed for a set of keys to the building or office?

(i) Emotional, mental, and personality disorders. Do they have any known or suspected emotional, mental, or personality disorders that may affect their behavior or actions or cause them to be susceptible to influence or coercion?

(j) Access to electronic information. What email addresses do they have? What social media networks do they use? What user identifications do they use? Do have a non-secure internet protocol router account? Do they have a secure internet protocol router account?

(4) *Obtaining sketches.* A sketch of the incident area generally assists in understanding the incident, as well as allows time to formulate additional questions. Ask the complainant to provide a sketch of the area. Ensure that all markings on the sketch are those of the complainant. Have the source—

(a) Title the sketch and annotate the date and time of the location of the incident.

(b) Indicate the north compass direction if the sketch is of an outside location. If the direction is unknown, use cross-street information.

(c) Indicate where all persons involved were located.

(d) Indicate any obstacles that would have deterred their line of sight to the incident.

(e) Print their full name, sign, and annotate the date the sketch was drawn.

c. Documentation. For walk-in interviews, the SA will obtain all documentation required for the interview. This includes—

(1) *Privacy Act of 1974.* Discuss the Privacy Act of 1974 at the beginning of the interview and have the complainant sign an acknowledgment form.

(2) *Secrecy affirmation statement.* The complainant will sign a secrecy affirmation statement or execute a nondisclosure agreement.

(3) *DA Form 2823.* The best policy is for the investigating SA to type the sworn statement (DA Form 2823) from the notes of the interview. However, it is allowable to have a complainant handwrite their sworn statement. Have the complainant check for accuracy, correct any mistakes, and have the complainant sign the sworn statement. Arrange for the complainant to return and sign the sworn statement after it is prepared by the SA. Upon final execution of the sworn statement, reiterate the official and sensitive nature of the investigation.

d. Interview termination. During this phase, SAs will finalize all the administrative procedures and ensure they have all the necessary information to complete their investigative and administrative reports. These procedures include—

(1) Have the complainant read the provisions of the Privacy Act of 1974, answering any questions the complainant may have about it, and signing a Privacy Act of 1974 acknowledgment form.

(2) Obtain full identification of the complainant, to include—

(a) Full name.

(b) SSN.

(c) Military rank or civilian pay grade.

(d) DPOB.

(e) Duty position and title.

(f) Unit of assignment.

(g) Residential address.

(h) Expiration of term of service date.

(i) Permanent change of station date.

(j) Date of last TARP briefing.

(k) Security clearance level.

(l) Level of classified information they have access to and the frequency of access.

(3) Ask the complainant why they reported the incident. Sometimes, the complainant's motivation may provide more insight as to the validity of the information. Some of the basic motives why individuals report possible CI incidents include ideology, compromise (fear or protection), and ego (revenge or elitism).

(4) Ask the complainant if they have any objection to being recontacted for additional information. If the complainant has no objection, ask if they prefer to be contacted at work or at home. If the complainant does have objections, remind the complainant that the information discussed is considered part of an official CI investigation and the details of the interview or the information concerning the incident are not to be discussed with anyone else.

(5) Inform the complainant that the information can be obtained through the FOIA and explain the consent to release process.

(6) Issue a security warning to the complainant to not discuss the reported issue with anyone and execute a secrecy affirmation statement. If the complainant has already talked to several individuals, get identifying information on those individuals to include in the report as others knowledgeable. Normally, it is not desirable to have numerous individuals know about an incident or a pending or ongoing investigation. The fewer people who have knowledge of the incident outside official channels, the less chance there is of compromising the investigation or potential for exploitation.

(7) Thank the complainant for the information provided.

4–3. Witness interview

Witnesses are those persons who may have observed, heard, or have knowledge of a CI incident or national security crime within CI investigative authority and jurisdiction. Witnesses and others knowledgeable are normally identified during the conduct of a walk-in interview. Witness interviews are conducted using the same basic principles used in the conduct of a walk-in interview.

a. Approach.

(1) During the approach phase, SAs confirm the witness's identity. After introductions, the SA determines whether the witness has knowledge or information regarding the CI investigation. Conducting a witness interview is similar to conducting a walk-in interview. SAs will—

(a) Identify themselves, first by name and organization and then by showing or presenting their badge and credentials to the witness.

(b) Identify the witness or others knowledgeable by verbally verifying the witness or witness's name and rank and requesting picture identification, such as a military identification card.

(c) Explain the purpose and official nature of the interview and ensure details of the investigation are not revealed to the witness.

(2) SAs will determine if the witness was at the location of the incident during the reported timeframe or if they have any knowledge concerning a security incident at a particular location during a specific timeframe. If the witness was not present or does not have any information, ascertain if they know of anyone who has knowledge of the allegation or incident.

(3) If the witness states that they were at the scene, proceed with the interview. Ensure that the witness understands that the U.S. Government considers their presence and all matters discussed during the interview to be official in nature and they are not to be discussed with anyone outside official channels. Determine if the witness has discussed the incident with anyone and tell the witness that they are not to discuss the matter with anyone.

(4) Provide the witness with the Privacy Act advisement.

b. Information development.

(1) Like a walk-in interview, SAs will attempt to obtain all the information concerning an allegation of a national security crime or incident of CI interest. This includes fully developing information of CI interest, identifying leads, developing any espionage and insider threat indicators, and obtaining sketches if necessary.

(2) If the case is such that the number of those knowledgeable of the issue is very limited or if the lead sheet specifies the conduct of a discreet investigation, the witness interview may require SAs to—

(a) Ask indirect questions that will elicit the appropriate responses.

(b) Use methods to conceal the identities of other witnesses to prevent the witness from finding out about the incident or subject of the investigation, however, never lie to the witness.

(c) Allow the witness to tell their story in narrative format all the way through. Notetaking should be kept to a minimum. Focus attention on the witness and listen to their story.

(d) Do not make any promises other than a promise of confidentiality.

(e) Ask clarifying questions. All details noted during the interview should be reviewed with the witness to ensure accuracy. SAs should not assume that they know what the witness means or knows based on previous information or interviews.

(f) Fully develop all information concerning persons, places, objects, or activities revealed by the witness that are relevant to the investigation. Any new information the witness identifies should be fully developed. The six basic interrogatives form the basis for questions: who, what, when, where, why, and how.

(g) Fully develop espionage and insider threat indicators of finances, lifestyle, hobbies, associates, foreign relatives, foreign travel, work habits, and access to electronic information.

(h) Determine if there are any new leads and fully identify leads mentioned by the witness.

(i) Review interview notes again before asking for a sworn statement.

c. Documentation. Request completion of a sworn statement (DA Form 2823). The best policy is for the investigating SA to type the sworn statement from the notes of the interview. However, it is allowable to have the witness handwrite a sworn statement. Have the witness check it for accuracy, correct any mistakes, and have the witness sign the sworn statement. Upon final execution of the sworn statement, reiterate the official and sensitive nature of the investigation. If there is not enough time for the witness to wait and sign a sworn statement prepared by SA, arrangements should be made for the witness to return and sign the sworn statement at a later date and time. In this case, SAs should still reiterate the official and sensitive nature of the investigation, issue the security warning, and then have the witness sign a secrecy affirmation statement. All information from the interview and the sworn statement must be documented in ACOP.

d. Interview termination. During termination of a witness interview, SAs will finalize all the administrative procedures and ensure they have all the necessary information to complete their investigative and administrative reports. These procedures include—

(1) Privacy Act of 1974.

(2) Obtain full identification of the witness.

(3) Objections for recontact.

(4) Consent to release.

(5) Security warning and affirmation statement.

(6) Thank the witness for their time and cooperation.

4–4. Subject interview

An interview of the subject of an investigation is often the only way to put all the information gathered into context and resolve the allegations in an investigation. It may be the single most important investigative action SAs conduct during a counterespionage investigation. It is conducted to allow a subject an opportunity to resolve, refute, explain, or mitigate allegations developed during the investigation. It is possible and sometimes even desirable to conduct multiple SIs during the course of an investigation. The subject is often the best source of the details required to resolve an allegation.

a. Subject interview. ACICA is the authority to approve the SI and the SIP.

b. Approach. During the approach phase of the SI, SAs will confirm the subject's identity through verification of a form of identification. SAs will introduce themselves, present their badge and credentials to the subject, and explain the circumstances of the interview. The approach phase for the SI differs from the walk-in and witness interviews in that the SA needs to advise the person of their rights due to the allegations involved. The SI is predicated on exhaustion of all other interviews and investigative activities, unless otherwise directed by the ACICA. SA's supervisor reviews of the SIP prior to the SJA for legal review and approval by ACICA. The SA will coordinate with the appropriate authorities if detention is anticipated. SAs will execute the following procedures during the approach phase of the SI:

(1) Explain the purpose of the interview.
(2) Execute DA Form 3881.
(3) Provide a perjury warning statement.
(4) Provide Privacy Act advisement.

c. Explain the purpose of the interview. SAs will explain the general purpose of the interview to the subject and reiterate the confidential nature of the interview. Inform the subject that ACI has received information indicating them as a subject in a CI investigation. The interview allows the subject the opportunity to explain, refute, or mitigate information received during the conduct of the CI investigation.

d. Execute DA Form 3881.

(1) The subject will not be questioned until they are properly advised of their legal rights and they voluntarily waive those rights. As appropriate, the interviewing SA will request the subject read and sign DA Form 3881 to acknowledge receipt of the explanation of rights and record the individual's decision to exercise or waive the right to remain silent and to consult legal counsel. It is suggested to administer the rights advisement early in the interview because of the formal and legal presentation of the details of the suspected or accused charges involved. This is usually the peak of anxiety for the subject.

Note. Not all SIs will require a rights advisement. In some cases, the SI is used to clarify information gleaned up to that point of the investigation. If the subject is not suspected of any particular violation of law, rights advisement is not required.

(2) Once the subject agrees to talk with the interviewing SA, the tension in the interview will generally, but not always, subside. If the subject invokes their rights upfront, the SA's time will not have been wasted in delaying the circumstances of the interview while having them fill out all the other documentation. Even if the subject waives their right to counsel initially, they can invoke rights later in the interview.

e. Subject invokes rights. Regardless of when the subject invokes their rights during an interview, SAs must stop questioning the subject and consult with the responsible operations management element and SJA.

f. Provide a perjury warning statement. Before questioning the subject concerning the allegations, the subject must be provided a perjury warning statement established in Title 18 USC. "I need to inform you of Title 18 of the United States Code. Should you willfully provide false information, you could be subject to a $5,000 fine, up to 10 years in prison, or both."

g. Provide Privacy Act advisement. Have the subject read the Privacy Act advisement. Verbally inform subject that the Privacy Act of 1974 requires that each individual who is asked to provide personal information be advised of the following four salient points:

(1) Authority by which the information is being collected.
(2) Principal purpose for which the information will be used.
(3) Routine uses for the information.
(4) Voluntary nature of disclosing information and the possible repercussions of failure to do so.

Note. Have the subject sign a copy of the Privacy Act advisement to retain for the records. If the subject wants a copy, one should be provided.

h. Information development. When conducting the SI, SAs should—

(1) Interview and question the subject concerning only the matter under investigation. SAs should use the SIP and the questions developed during the interview planning and preparation process to fully explore and develop the area of interest to establish the facts concerning the allegations.

(2) Use basic interview techniques to fully develop information and obtain direct responses to all questions concerning the allegations or circumstances of the subject.

(3) Not make off-the-record or unofficial remarks in the interview.

(4) Not make any promises or commitments to the subject, which are beyond the SA's legal authority.

(5) Avoid statements or representations that may be construed as opinion or advice to the subject about past, present, or future actions.

(6) Not argue with the subject or express personal viewpoints on any matter.

(7) Review interview notes with the subject to ensure accuracy of the recorded information and to make any corrections as needed. During the review, the subject should be given the opportunity to clarify or provide additional information. SAs should review their notes whenever they feel it is necessary to clarify information provided.

i. Documentation. Request the sworn statement (DA Form 2823). It is best for the DA Form 2823 to be in the interviewee's own handwriting, though the investigating agent may type the sworn statement from the notes of the interview. Have the subject check for accuracy, correct any mistakes, and have the subject sign the DA Form 2823. If the subject refuses to sign the sworn statement, the refusal should be annotated on the form, be signed by the interviewing SA, and retained in the case file. It is allowable to have the subject handwrite the sworn statement if they choose to do so. The subject's sworn statement will be prepared before rendering any decision on the disposition (release or detention) of the subject.

j. Interview termination. When terminating the SI, SAs should address the following:

(1) Ask the catchall question. When all investigative requirements have been satisfied and all relevant or derogatory information has been fully developed, SAs should ask the subject if there is anything they would like to add to the interview. If the subject adds something, record the information and continue to ask the question, "Is there anything else you wish to add?" Repeat this line of questioning until a negative response is obtained.

(2) Ask the subject if they are willing to submit to a polygraph examination.

(3) Provide the subject with a security warning (nondisclosure statement). State, "I need to remind you that the information we have discussed during the interview is to be considered confidential and official in nature and should not be discussed with anyone outside the investigative channels of this office."

(4) To maintain the established rapport, thank the subject and terminate the interview.

(5) Determine proper disposition of subject (release or detain). If the anticipated direction of the interview has changed, consult with SJA before making a final decision on the disposition.

Chapter 5
Counterintelligence Investigative Reporting Document Management

Reporting procedures and management of investigation-related documents are essential to maintaining an investigation on track and supportive of prosecutorial objectives. Case management begins with the initial report of an activity or incident of CI interests and ends when ACICA informs the investigative element that the case has been closed and placed in the USAIRR and provides guidance to destroy additional document copies. All investigative activities are documented and managed in ACOP.

5–1. Reporting procedures

Incidents of CI interest reported to SAs or elements have different reporting procedures based upon ACICA guidance, which includes submission times and telephonic notification.

5–2. Submission times

Submission times for reporting information of CI interest include 24-hour, 72-hour, and concurrent reporting.

5–3. Requirement of 24 hours

Initial reports concerning sabotage, potential terrorist attacks, or other incidents involving physical security threats to Army personnel or facilities will be reported immediately to the ACICA by the most expeditious means available, but no later than 24 hours after receipt. These incidents must be reported to the Army Operations Center at HQDA within 24 hours of receipt. Providing timely warning of force protection threats to affected local commands, local PMO, and USACIDC is the first priority over all other reporting requirements. In these situations, secure telephonic notification will be used for initial reporting followed by preparation and submission of a written report.

5–4. Requirement of 72 hours

a. AR 381–12 and AR 381–20 establish a basic requirement that CI reports will be put into ACOP within 72 hours of receipt of reportable information. Reports should be sent as early in the 72-hour window as feasible. It is imperative that this timeline be adhered to in order to preserve the exploitation value of incidents where FIE involvement is eventually uncovered.

b. While agents will make every reasonable attempt to fully identify and interview the original or best source of information, initial reports will not be delayed solely for that purpose. SAs must balance their ability to gain additional facts in support of the initial report against the probability of FIE involvement and likelihood of recontact.

5–5. Telephonic notification

To ensure expeditious handling of time-sensitive reports, the reporting CI element telephonically notifies the ACICA of all reports meeting the 24-hour or less reporting requirement. This also includes any incident where FIE involvement is confirmed and FIE recontact is expected or imminent. Telephonic notification should be provided as soon as possible after receipt of reportable information.

5–6. Documents management

a. ACOP is the only authorized database for CI investigative activities. Efficient case file maintenance allows investigating SAs and operations management elements to know—

(1) The status of an investigation.
(2) What investigative activities have occurred.
(3) What reports and supporting documentation has been submitted.
(4) Pending investigative activities and documentation.
(5) Guidance from the operations management element to the investigating SA or element.

b. Case files maintenance is the responsibility of the investigating SA. It begins with the initial walk-in or when the information of CI interest is obtained and ends when the investigation is terminated and the case file is forwarded to the ACICA. Case file maintenance includes—

(1) Assigning case control numbers.
(2) Organizing case file content.

5–7. Assign case control numbers

CI investigative activities are assigned two different case control numbers: the LCCN and the Army case control number (ACCN).

a. Local case control number. The LCCN is assigned in ACOP based on the investigating CI element. The LCCN is used for tracking purposes until a formal investigation is opened by the ACICA and a permanent ACCN is assigned.

b. Army case control number. The ACCN is assigned within ACOP depending upon the type of investigation. The ACCN is used to identify a specific CI investigation and to track investigative reports and other supporting documentation associated with that investigation.

c. Army case control number designators. An ACCN is composed of five different designators—

(1) *Investigative activity code.* The investigative activity code is a two- to three-letter abbreviation designating the type of investigative activity. This code may change based upon a change in the status of the investigative activity. Although the investigative activity code may change, the rest of the number, to include the sequence number, will always remain the same. The investigative activity codes are—

(a) LCA for LCAs.
(b) PI for PIs.
(c) FF for FFs.

(2) *Fiscal year.* The last two digits of the fiscal year when the investigative activity was initiated.
(3) *Unit.* The unit to which the investigating element is assigned.
(4) *Investigative element.* A two- to three- letter designator for the investigating element.
(5) *Investigation sequence number.* A three-digit investigation sequence number. Each investigating element will begin their sequence with 001. The next approved investigative activity approved (LCA, PI, or FF) will use the next sequence number. Investigating elements will restart their sequence numbering with 001 at the beginning of each fiscal year.

Chapter 6
Counterintelligence Investigative Reports

CI investigations consist of fact-finding and information collection activities. The results of these activities are prepared in written form and submitted to appropriate offices and agencies. ROI entries in ACOP are the end product of all investigative efforts. CI reports transmit information accurately to the responsible operations management element and higher technical authorities to provide a legal record of investigative activities. CI reports must answer all reasonable questions, which may be raised by reviewing technical and legal authorities.

6–1. Types of counterintelligence investigative reports

a. CI investigative reports are used to report the results of all CI investigative activities. CI investigative reports are also used to report unsuccessful investigative activities (for example, when SAs make unsuccessful attempts to locate witnesses, sources, records, and other information pursuant to the conduct of the investigation). This prevents other SAs from duplicating efforts during the investigation. All information gained from a source, records check, or other investigative activity will be reported. Information that does not appear to be pertinent at a point during the investigation may become pertinent at a later date.

b. CI investigative reports must accurately reflect the information provided by a source, subject, or the record under review. SAs must not make assumptions, interpret the information, modify the information, draw conclusions, or adjudicate what is important or truthful when preparing a CI investigative report. If a source expresses an opinion or belief, it must be reported as such. SAs should attempt to answer all of the basic interrogatives in the report, even if all are negative responses.

6–2. Counterintelligence reports and discovery

a. Types of counterintelligence reports. CI investigative reports are subject to review during the discovery process for legal proceedings. If CI investigative reports are written poorly, contain mistakes, or are not stored and transmitted in accordance with DA policy and procedures, the reports could be detrimental to prosecutorial objectives. There are several types of CI reports used to document the results of investigative activities—

(1) CIR.
(2) ROI.
(3) LHM.

b. Counterintelligence incident report. CIRs are used to report specific allegations that individuals are committing or plan to commit national security crimes, to include terrorism (for example, belonging to or supporting a terrorist group). Elements of national security crimes are addressed in detail in and reported utilizing the CIR. CIRs involving terrorism are subject to a 24-hour reporting requirement.

c. Report of investigation. The ROI serves as an EXSUM of investigative results reported in ACOP ROI entries and exhibits and is maintained in ACOP. ROIs are required for any investigation that goes beyond the interviews of the original sources of information and local and military agency checks. The ROI highlights investigative efforts to either confirm or refute espionage indicators or allegations. The report should be concise, ensuring pertinent results are emphasized. The agent preparing the ROI cites investigative findings to explain, refute, or support allegations or incidents in which espionage activity is suspected. Copies of all ROIs will be retained by the investigating element until the investigation is completed and maintained on file in accordance with AR 25–400–2 until destruction is authorized or in accordance with unit SOPs.

d. Summary of information. The LHM is the document used to share limited details about a CI investigation with other Government agencies. The LHM will not include investigative or intelligence methods of operation or internal Army coordination, tasking, or comments. Information in the LHM is a compilation of facts obtained from multiple investigative activities (for example, ongoing research, files reviews, phone record examinations, or other).

6–3. Reporting caveats

Reporting caveats are found in ACOP. When conducting record reviews or obtaining information from other agencies, special caveats must be added to the appropriate report. The reporting caveats provide the legal source of the information and special handling and distribution considerations required by law. Caveats are included in the reports all in uppercase (see table 6–1 for counterintelligence reporting caveats).

Table 6–1
Counterintelligence reporting caveats

Caveat	Report or source of information

Table 6–1
Counterintelligence reporting caveats—Continued

The information contained in this document is preliminary in nature and is provided for initial notification purposes only. This information will not be used as the basis for adverse legal or administrative actions against individuals without prior coordination with the U.S. Army Counterintelligence Coordinating Authority, Fort Belvoir, VA.	Used in LHM reports provided to other agencies.
Information contained in this report is financial record information that was obtained pursuant to the Right to Financial Privacy Act of 1978, 12 USC 3401 et seq. This information may not be released to another Federal agency or department outside the DOD without compliance with the specific requirements of 12 USC and AR 190–6.	Used in investigative reports containing financial information obtained through the use of bank letters and the Defense Finance and Accounting Services.
The enclosed information was collected and disseminated under provisions of the Bank Secrecy Act (BSA) and U.S. Department of the Treasury regulations implementing the BSA. See 31 USC 5311 et seq.; 31 CFR Chapter X. The information is sensitive in nature and is to be treated accordingly. The information may be used only for a purpose related to a criminal, tax, or regulatory investigation or proceeding; or in the conduct of intelligence or counterintelligence activities to protect against international terrorism; or for a national security matter. See 31 USC 5311. The information cannot be further released, disseminated, disclosed, or transmitted without prior approval from the director of the FinCEN or their authorized delegate. SARs filed under the BSA must be treated with particular care given that they contain unsubstantiated allegations of possible criminal activity, akin to confidential informant tips. Such reports, or the fact they have been filed, may not be disclosed by a Government employee to any person involved in the transaction, other than as necessary to fulfill the official duties of such officer or employee. See 31 USC 5318(g)(2)(ii). Unauthorized release of information collected under the BSA may result in criminal or civil sanctions.	Used in investigative reports containing financial information obtained from FinCEN checks.
This document contains information from Foreign Intelligence Surveillance Act (FISA) collection. This information and any information derived therefrom may not be used in any foreign or domestic criminal, administrative, or other proceeding without the advance authorization of the Attorney General. If concerning a U.S. person, this information may be disseminated to a foreign government only with prior authorization from FBI headquarters. Any reproduction, dissemination, or communication (including, but not limited to, oral briefings) of this information must be accompanied by a statement of these restrictions.	Used in investigative reports containing information derived from an approved FISA activity.
This document contains information obtained or derived from techniques conducted pursuant to the Foreign Intelligence Surveillance Act, 50 USC 1806(b). Such information shall not be used in any criminal or administrative proceeding, including grand jury proceedings and warrant affidavits, without the prior written approval of the Attorney General. U.S. person FISA-derived information may not be disseminated to a foreign government without the prior written approval of the FBI director or their designee.	Used in investigative reports containing information derived from an approved FISA activity.
This information or document, or portions thereof, is derived from a court-authorized FISA order and such information or any information derived therefrom may only be used in a criminal or other proceeding (including, but not limited to, use in search or arrest warrants or affidavits or grand jury subpoenas and proceedings) with the advance authorization of the Attorney General. See 50 USC 1806(b) and 50 USC 1825(c).	Used in investigative reports containing information derived from an approved FISA activity.
Law enforcement sensitive: the information marked (U//LES) in this document is the property of Customs and Border Protection and may be distributed within the Federal Government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials, and individuals with a need to know. Distribution beyond these entities without Customs and Border Protection authorization is prohibited. Precautions should be taken to ensure this in-	Used in investigative reports containing information derived from CBP agency that has been designated as law enforcement sensitive (LES).

Table 6–1
Counterintelligence reporting caveats—Continued

formation is stored or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website or an unclassified network.	
Information in this report was obtained from the Airline Reporting Corporation (ARC). If this information is used for subsequent leads, do not identify ARC as the original source of information. For dissemination outside of Army intelligence channels, serve a subpoena or other lawful demand to ARC, ATTN: Dottie Hogan, 3000 Wilson Boulevard, Suite 300, Arlington, VA 22201; Fax 703–816–8138.	Used in investigative reports containing information derived from records checks with the ARC.
Source requested confidentiality as a condition of providing the information in this report.	Used in investigative reports when the source of the information requests confidentiality.
Source had no objection to their identity being released.	Self-explanatory.
Information contained in this report was obtained from another Federal agency who reserves the right to restrict release.	Used in investigative reports when another Federal agency releases information to Army intelligence, but Army intelligence is not allowed to disseminate to any other entity (for example, FBI, CIA, Department of State (especially the Consular Consolidated Database (CCD)), Department of Homeland Security (including TECS), and so forth).
Information in this report was obtained from copyrighted proprietary records.	Used in investigative reports containing information derived from records checks from CLEAR and LexisNexis.
Information contained in this report was obtained from official Government records.	Used in investigative reports containing information derived from the records of a Government agency.
Information contained in this report was obtained from public records.	Used in investigative reports containing information derived from public records (for example, court proceedings, driving records, land titles, or other).
Information contained in this report was obtained from official military medical records.	Used in investigative reports containing information derived from medical records and facilities.
Information contained in this report was obtained from official military personnel records.	Used in investigative reports containing information derived from military records (for example, evaluations, disciplinary actions, promotions, awards, and decorations).
Information contained in this report was obtained from official civilian personnel records.	Used in investigative reports containing information derived from Government civilian personnel records (for example, evaluations, disciplinary actions, promotions, awards, bonuses, or decorations).
Information contained in this report was obtained from open-source material.	Used in investigative reports containing information derived from open sources (for example, internet websites, newspaper articles, or other).
Information in this report was obtained through online open-source searches of publically available material.	Used in investigative reports containing information derived from information found on social media websites.
Information in this report was obtained through a media analysis.	Used in investigative reports containing information derived from newspapers, radio, and television.

Table 6–1
Counterintelligence reporting caveats—Continued

Information in this report was obtained through computer forensic examination.	Self-explanatory.
Information in this report was obtained through authorized evidence seizure.	Self-explanatory.
Information contained in this report was obtained during an authorized surveillance.	Self-explanatory.
Information contained in this report was obtained from the Consular Consolidated Database (CCD). Information from the CCD may not be disseminated outside of the U.S. Army, DIA, Naval Criminal Investigative Service, or the Air Force Office of Special Investigations without written approval from the Department of State visa office. Additionally, this information cannot be published in an intelligence information report (Department of State CCD).	Used in investigative reports containing information derived from the Department of State CCD.

Chapter 7
Counterintelligence Investigation Management Documents

CI investigations are controlled and developed through a series of investigation management documents that chronicle the history of an investigation from its opening to its closing. Investigation management documents record every aspect of an investigation, as well as the results from actions taken. ACICA must concur with and approve all investigation management documents prior to investigative action being taken and prior to the case being closed.

7–1. Opening message

The opening message is the means by which the ACICA informs the reporting field element of their determination to open a message and assign them a given investigative role either as the lead investigative element or in a supporting role. The opening message will also identify what investigative actions that element needs to accomplish along with suspense dates if applicable. Once the investigation is designated as open, the investigation is authorized to proceed with all approved investigative activities.

7–2. Investigative plan

a. The investigative plan is the document that provides a detailed road map on the conduct of CI investigations including all investigative participants, all investigative activities required, all resources and external support required, and all interagency or legal coordination required to successfully resolve the incident. Investigative plans are living documents and may require revision due to information development and case direction. All updates or revisions will be forwarded to the ACICA.

b. An investigative plan is prepared by the lead agent in collaboration with the senior supervisory SA. The investigative plan is used to outline and request approval for investigative authority and, once approved, serves as the authority document for general investigative activity. The investigative plan and joint investigative plan are essentially the same format.

7–3. Subject interview plan

The purpose of the SIP or JSIP is to ensure the investigating SA is familiar with all information obtained during the course of the investigation and clearly understands what the goals of the planned SI are. The SIP also identifies any external coordination required. The SI may only be conducted once the SIP is reviewed, approved, and signed by the ACICA. It is not required to include specific questions in the SI plan. However, depending on the complexity of the issues to be discussed, this can often assist the ACICA in making a determination to approve the SIP. At a minimum, before conducting the interview, the SA should develop a topical outline that can be used to ensure all SI objectives and requirements are met.

7–4. Request for an investigative polygraph

After all investigative steps have been completed, to include the SI, an investigative polygraph examination may be requested. To request an investigative polygraph examination, DA Form 2805 (Polygraph Examination Authorization) must be submitted to AIPP with areas to be covered during the polygraph examination. Investigators should fully consider what the ultimate goal of the investigation is and how the polygraph examination can assist in that determination. AIPP will review all case facts and approve or disapprove the DA Form 2805. If the DA Form 2805 is approved

by AIPP, the polygraph detachment will assign two examiners to conduct the polygraph. The polygraph examiners will review the case file and develop questions to be asked during the polygraph examination through coordination with the case agents.

7–5. Request for assistance

RFA documentation is completed in ACOP. The requesting agency is usually the one with exclusive jurisdiction over an investigation. An RFA can be used to request everything from a simple records check to personnel support. They are usually a one-time request, limited to a specific action of a short duration (that is, local agency checks and military agency checks or assistance in arranging and facilitating the conduct of interviews on military installations or in a military unit). An RFA does not automatically result in a joint investigation. Once the requested actions are completed, the supporting agency is no longer involved in that investigation. RFAs will not be utilized to circumvent establishing a joint investigation.

7–6. Federal Bureau of Investigation letterhead memorandum

The FBI LHM is a communication vehicle through which the FBI documents official policies, investigative findings, and external coordination. During investigations requiring ACI support, the request for such support is communicated via FBI LHM. Requests can range from investigative actions (for example, records checks) to an invitation to participate in a joint investigation. A joint investigation FBI LHM will provide an appropriate description of the type, scope, and duration of support requested. Both agencies must agree to the role each will play.

7–7. Monthly investigative report

a. The monthly investigative report (MIR), also referred to as a baseball card, is a key tool CI investigative elements produce to keep the ACICA apprised of the status of ongoing ACI investigative activities. This allows for proper CI investigative oversight. MIRs also provide visibility to DA and DOD leadership concerning ACI investigations and operations. This directly affects the priority the ACI investigative program receives and the resources allocated to it. MIRs should be written with the senior leader as the target audience. The number of followup questions asked and the time to answer them is directly proportional to the quality and clarity of the MIR.

b. The MIR is generally a PowerPoint slide with a front and back and is produced in ACOP. The front provides a synopsis of the subject and administrative information concerning the investigating element. The back provides a summary of details concerning the investigation—

(1) Allegation.

(2) Predication.

(3) Actions taken and status of investigative activities (by the investigative element). This will be a synopsis of the results of the actions taken.

(4) Actions pending (other CI investigative activities to be conducted by the investigative element).

c. See ACOP for MIR format. The border of the MIR denotes the category type for the investigation. The category types include—

(1) Espionage (blue border).

(2) Terrorism (red border).

(3) Other (black border).

7–8. Senior leader briefing

a. As outlined in the Deputy Chief Of Staff (DCS), G-2's Guidance Letter, "Implementing Guidelines for the Reporting of Significant Counterintelligence (CI) Activity to the Army Leadership," dated 28 April 2014, subordinate CI elements are required to obtain ACICA approval to brief senior leaders within and outside of CI channels. As outlined in paragraph 2–45*i*(1), the ACICA must approve all requests to brief senior commanders regarding the details of CI investigations. The supervisor must identify the information to be briefed and submit requests for approval at least 3 days in advance. The majority of such requests involve general officers and senior executive service level personnel.

b. Each request to brief a senior leader will include an EXSUM and the PowerPoint slide example, as prescribed in the DCS, G-2's policy letter. The PowerPoint slide is produced in ACOP. The PowerPoint slide is not required to be given to the person being briefed. Rather, it is a guide to ensure the agent understands the main points to be briefed and stays on topic. In instances involving non-general officer relevant commanders and leaders at a given unit, such as a brigade commander or a division G–2, the ACICA should be notified in advance with at least an EXSUM of the planned briefing. No slide is required in this situation. When in doubt concerning 0–6 and below briefings, contact the ACICA for guidance.

c. Briefing CI investigations, especially to a non-MI leader, requires the agent to be well versed in expectation management and the overall case facts. During the briefing, commanders may ask questions not necessarily related to the investigative acts planned by the supporting unit. The SA should make sure Army intelligence does not commit or affirm to any activity not within their purview, yet be able to address each commander's logical concerns for security of their assigned U.S. Army equities.

7–9. Executive summary

The EXSUM is used to report urgent, high-priority information in summary form, usually to a general officer level audience. EXSUMs will be forwarded through operations management channels to the ACICA. Specific events that require an EXSUM include a change in the status of subject, a special collection mission or procedure, or a senior leader or general officer briefing.

a. Change in the status of subject. This EXSUM includes death, arrest (even if unrelated to a CI investigation), hospitalization, flight or absent without leave, or unexpected deployment.

b. Special collection mission or procedure. This EXSUM requires both a pre-event and post-event EXSUM. The pre-mission EXSUM will be submitted 24 hours prior to initiation of the mission followed by a post-mission EXSUM, which is submitted no later than 24 hours after the completion of the mission. Long-term missions (for example, surveillance) may require daily or weekly EXSUMs as directed by an operations management element.

c. Senior leader or general officer briefing. Briefings to senior leaders and general officers require both a pre- and post-briefing EXSUM. The pre-brief EXSUM will be submitted 3 days prior to the planned briefing, followed by a post-brief EXSUM, which is submitted no later than 24 hours after the briefing.

Note. All briefing to a senior above the DA G–2 level will be coordinated through the ACICA to keep the HQDA leadership and the DCS, G–2 apprised of the information.

7–10. Limited counterintelligence assessment summary

The LCA enables SAs to conduct limited investigative activity to explore and develop situations that do not meet the threshold for submission of a CIR when there are insufficient CI indicators to justify opening a formal CI investigation. LCAs use relatively nonintrusive investigative techniques that allow the collection of information to determine if a matter or incident has occurred and if it is of CI interest. LCAs are conducted until a CI incident is resolved or sufficient information has been developed to submit a CIR. A classified example of a limited CI assessment summary example is available in ACOP.

7–11. Termination message

The termination message will cite the justification for case termination and will levy requirements for preparation and submission of an ROI. The termination message serves to inform the investigating element that an open investigation has been terminated and to cease further investigative actions. Further investigative activity will only occur only if directed by the ACICA or if investigative activity was initiated prior to the termination date. When investigative activity cannot be completed prior to the receipt of a termination message, the SA will annotate in the agent's notes of the ACOP ROI entry that the activity was initiated prior to termination and explain why the action could not be completed prior to termination (for example, a local agency check was initiated but the agency was not able to respond until after the case determination was made). When appropriate, the termination message will include instructions to produce an intelligence information report using case information.

Chapter 8
Counterintelligence Investigation Supporting Documents

CI investigation supporting documents are used to request records checks and special investigative or collection techniques that require coordination, staffing, and approval based on guidance in DODM 5240.01, AR 381–10, and AR 381–20.

8–1. Records checks requests

Examples of requests for AKO records, DISA records, DISA legal review, and NACs are available in ACOP.

8–2. Special investigative techniques requests

All requests for the special investigative techniques are submitted to the ACICA for coordination and approval by the appropriate authority. DODM 5240.01 and AR 381–10 provide detailed guidance on the separate approval authorities for all special investigative techniques both in the U.S. and abroad.

Note. All special investigative techniques will be coordinated with the ACICA and approved by the responsible authority.

a. Writing a procedure request. Authority to conduct special investigative techniques is requested via an LHM through operational management elements to the appropriate approving official. This memorandum is strictly formatted based on the type of special technique requested. All requests for special investigative techniques should include—

(1) References.
(2) Summary.
(3) DOD nexus.
(4) Background.
(5) Purpose.
(6) Parameters.

b. References. List references beginning with the section of DODM 5240.01 and chapter of AR 381–10 that apply to the technique requested. In joint cases or where concurrent jurisdiction applies, list any FBI or other agency letterhead memoranda that establish a joint investigation or request Army participation or support. The references list should also include this publication and the opening message including complete title block.

c. Summary. Include a brief description of the special investigative technique requested and objective for its use.

d. Department of Defense nexus. This is a required paragraph regardless of investigative jurisdiction and should describe the DOD connection to the investigation, operation, or activity that the special technique will support and. In some cases, this will be a simple statement that the subject is an active duty Soldier under unilateral investigation by ACI for alleged espionage. In joint investigations or operations where Army shares or does not have primary jurisdiction in the matter, the justification will have to be more detailed to identify Army equities. For example, this may include subject's membership in groups with a history of attacking DOD installations or access to DOD installations or classified information. This paragraph may also list any CI collection or other information requirements that may be answered by ACI use of the requested special investigative technique.

e. Background. This paragraph will provide all relevant details of the investigation or operation to date, to include information provided by partner agencies in joint investigations. This paragraph must stand on its own and provide the approval authorities along with all the relevant information necessary to make an informed decision. This paragraph is used to establish why less intrusive means will not or have failed to obtain the required information. The narrative must establish probable cause to justify the use of the requested techniques.

f. Purpose. This paragraph will describe in detail what investigative or operational objectives will be accomplished by the requested special investigative technique. It should address how the proposed activity will fill information gaps identified in the background paragraph.

g. Parameters. This paragraph describes the execution of the requested special investigative technique in great detail. It should include a description of the employment of the requested technique, to include all the necessary technical information required by the regulation. It must also include the geographical locations of all proposed activity and the start and anticipated end dates and times.

h. Procedure request examples. See ACOP for example requests to conduct the following special investigative procedures: Procedure 6 (concealed monitoring), Procedure 7 (physical search), and Procedure 9 (physical surveillance).

i. Bank letters.

(1) A bank letter is a formal written request to a financial institution by which an investigative element conducts an unconsented check of the financial institution records of a given subject. Agents must use the bank letter tab in ACOP for tracking.

(2) Upon identifying a financial institution account (for example, bank account, brokerage account, or credit reporting bureau) connected to subject during the course of an investigation, the investigative element prepares a draft bank letter and forwards it to the ACICA for review, staffing, and signature. The 902d Group Commander, ACICA chief, or CG or Deputy CG, INSCOM are the only signature authorities for bank letters.

(3) Upon the receipt of the signed bank letter, it can be delivered to the financial institution and the check can then be conducted. The investigating element submitting the bank letter may not always be the element that delivers the bank letter and conducts the check. Under no circumstances will field elements attempt to conduct a financial institution check without a properly signed bank letter provided by the ACICA.

8–3. Exhibits

Exhibits are documentation or physical evidentiary materials supporting the information provided in ACOP. All exhibits must be in .pdf or .tiff format. Create an ACOP ROI entry for all exhibits collected during the course of investigative activity. This evidence may be in the form of records, identification documents, affidavits, statements, photographs, transcripts of interviews, screencaps of social media posts, photocopies, sketches (made by either the SA or other persons), documents, pamphlets, newspaper clippings, sound recordings, surveillance logs, DA Form 4137, DA Form 2823, computer thumb drives, or transcripts concerning the analysis of an information storage medium. Exhibits augment and support, but do not replace, the ACOP ROI entry. ACOP will generate the exhibit cover sheet.

Chapter 9
Investigative Legal Considerations and Evidentiary Procedures

CI investigations of incidents of CI interest and national security crimes must be conducted in accordance with the principles of law and the rules of evidence that govern the prosecution of any criminal activity. AR 195–5 and FM 3–19.13 cover the legal aspects of gathering, handling, documenting, and controlling evidence. CI personnel must have a thorough understanding of the legal principles and procedures involved in conducting an investigation to ensure prosecutorial integrity of the investigation, know when to seek legal guidance before exercising an investigative activity, and recognize those cases where specific guidance, assistance, or approval must be obtained before executing further investigative activities.

9–1. Intelligence oversight for counterintelligence investigations

Basic legal principles always apply to CI investigative situations, as they are designed to ensure the legal rights of subjects are observed. The potential to prosecute any given case must not be jeopardized by illegal or improper CI investigative techniques. In addition, CI personnel investigating activities must obtain advice and assistance from the SJA or legal officer to implement recent court decisions interpreting statutes and regulations (see ATP 2–22.2–1 for more information on legal considerations for CI investigations).

a. Titles 10 and 32, United States Code: status of personnel. Determining active duty status in investigations involving U.S. Army National Guard personnel is essential. If a Guardsman is called to active duty in a Federal capacity under 10 USC, they are under the jurisdiction of ACI. If they are called to active duty in a state capacity under 32 USC, they are under the jurisdiction of the FBI. The most reliable way to establish this at the field level is to obtain a copy of the orders bringing the Soldier on active duty and look for verbiage or fund cites that will identify under which title of the USC they were activated. Any uncertainty should be surfaced through investigative channels and forwarded through the responsible operations management element to the ACICA who can resolve the matter at the National Guard Bureau level.

b. Authority to administer oaths.

(1) SAs, both military and civilian, have the authority to swear a witness or subject to an oath. For military SAs, the authority to swear a witness or subject to an oath is derived from UCMJ, Article 136(b)(4). For DOD civilian SAs, the authority to swear a witness or subject to an oath is derived from 5 USC 303(b). Rule 603 of the Federal Rules of Evidence requires that "before testifying, a witness must give an oath or affirmation to testify truthfully. It must be in a form designed to impress that duty on the witness's conscience." The combination of the written statement and the oath meets this requirement and renders the statement an official statement.

(2) SAs will administer an oath of truthfulness prior to a source or subject signing the affidavit section of the sworn statement (DA Form 2823). To administer the oath, the agent should ask the witness or subject to stand and raise their right hand, then ask the witness or subject, "Do you swear or affirm the information you provided in this statement is the truth, the whole truth, and nothing but the truth?"

(3) If the witness or subject lies in an official statement, the witness or subject may be punished for providing a false statement under UCMJ, Article 107 (for military personnel) or 18 USC 1621 (for civilians), regardless of whether or not a conviction is obtained based upon the original allegations being investigated by ACI. The maximum punishment under UCMJ, Article 107 is dishonorable discharge, forfeiture of all pay and allowances, and confinement for no more than 5 years. The maximum punishment under 18 USC 1621 is a fine and imprisonment for no more than 5 years.

9–2. Legal documents

SAs must have an understanding of the purpose and how to execute all the legal documentation required in support of a CI investigation. These documents include sworn statement (DA Form 2823), DA Form 3881, the Privacy Act of 1974, secrecy affirmation, perjury warning, and consent to search forms.

a. DA Form 2823.

(1) Sworn statements (DA Form 2823) are permanent records of the testimony of accused persons, suspects, victims, complainants, and witnesses. They may be used in court as evidence attesting to what was told to investigators.

(2) Typewritten sworn statements are one method for recording and preserving statements from victims and witnesses. Statements are typically recorded on DA Form 2823. A statement typed by the SA should generally be brief, concise, and well written. The statement should address all the pertinent facts concerning the incident being reported. Typewritten statements can be taken in conjunction with handwritten statements and interview sketches.

b. DA Form 3881. The SA should use DA Form 3881 as a guide when advising a subject of their rights. SAs should never attempt to recite the advisement based on memory. If the appropriate forms are not readily available, the SA should delay the interview until the forms are available. The SA should keep a printed copy of DA Form 3881 along with other supporting investigative documentation. The SA should read directly from the form or card without deviation every single time. For example, when informing someone of their rights, DA Form 3881 includes specific verbal instructions to recite to the subject. Following the same methodology every time helps ensure statements will be admissible.

c. Privacy Act of 1974.

(1) The Privacy Act of 1974 was enacted to protect personal-type information from unwarranted and unreasonable disclosures. The Privacy Act of 1974 requires that each individual interviewed who must provide personal-type information (for example, full identifying data, to include SSN) must be advised of the provisions of the act. The Privacy Act of 1974 advisements serve to document that sources and subjects of an investigation understand their rights under the Privacy Act, as well as the voluntary nature of furnishing any personal information to CI.

(2) SAs are required to advise investigative sources and subjects of investigations of the provisions of the Privacy Act of 1974 prior to the start of any interview or debriefing. Whenever possible, agents should provide interviewees with a written advisement and obtain a signed copy acknowledging receipt. The signed copy of the Privacy Act advisement is maintained in the local case file and is not forwarded as an exhibit to be archived with the ROI.

(3) The Privacy Act advisement may be given verbally or in writing and must cover the following four key points:

(a) The authority by which the information is being collected.

(b) The principal purpose for which the information will be used.

(c) The routine uses of the information.

(d) The voluntary nature of disclosing information.

(4) The fact that source or subject is advised of the provisions of the act will be annotated in the agent's notes section of the corresponding CIR or ACOP ROI entry.

(5) There is no regulatory requirement to advise non-U.S. persons of the provisions of this act. When a Privacy Act advisement is not needed, such as for interviews with foreign nationals in overseas areas, no entry will be made in the resulting CIR or ACOP ROI entry.

d. Secrecy affirmation.

(1) The secrecy affirmation serves to document a source's or subject's understanding that the disclosure of the nature or existence of a CI activity is prohibited without the express approval of U.S. Army intelligence.

(2) At the conclusion of an interview concerning an alleged or actual CI incident, the SA will request that the interviewee sign a secrecy affirmation or nondisclosure agreement. If the source refuses to sign the agreement, the SA will administer a verbal warning that the information is evidence in a national security investigation and will not be disclosed to third parties.

(3) The secrecy affirmation is maintained in the local case file and is not forwarded as an exhibit to be archived with the ROI.

(4) The fact that a source or subject refused to sign the secrecy affirmation will be annotated in the agent's notes section of the corresponding CIR or ACOP ROI entry.

(5) There is no regulatory requirement for non-U.S. persons to sign a nondisclosure agreement. SAs will instead administer a verbal reminder to not discuss the nature or existence of the CI activity.

(6) When an interview requires the use of a linguist or translator, SAs will require the linguist or translator to sign a secrecy affirmation before the start of the interview. When preparing the corresponding CIR or ACOP ROI entry detailing the contents of the interview, SAs will identify the fact that the interview was conducted with the assistance of an interpreter and will fully identify the interpreter in the agent notes.

e. Perjury warning. The perjury warning serves to inform an investigative source or subject of an investigation of the penalties associated with willfully providing false information. Before questioning the subject concerning the allegations, SAs will inform the subject of the provisions of 18 USC. SAs will use the following statement: "I need to inform you of Title 18, United States Code. Should you willfully provide false information, you could be subject to a

$5,000 fine, up to 10 years in prison, or both." SAs will provide the perjury warning to sources of information regarding a potential incident of CI interest after fully debriefing the source.

f. Consent to search computer and electronic equipment.

(1) A standardized consent form is utilized when requesting consent to seize and search personal computer and electronic equipment. The seizure and search of U.S. Government computer and electronic equipment will be conducted in accordance with established policies and procedures.

(2) The consent to search computer/electronic equipment form can be utilized in two ways—

(a) The individual provides the computer or electronic equipment.

(b) The individual consents to the removal and search of computer or electronic equipment from their personal living space, residence, or other location.

Note. Evidence will be controlled and accounted for in accordance with AR 381–20 and AR 195–5.

(3) To prepare the consent to search personal computer form—

(a) Use letterhead for the unit of the preparing SA.

(b) The form should be typed when possible so all information is clearly legible and may not be discounted when scrutinized by legal authorities. However, it may be handwritten as long as all the information is legible.

(c) In paragraph 1, provide the full name of the person consenting to the search.

(d) In paragraph 2, provide the full name of the SA conducting the search in the first blank space. Provide detailed information concerning all personal computers or electronic equipment to be searched by the SA in the lined, blank space. This should the device or media make, mobile, serial number, any specific markings that can be used to fully identify the device or media. The SA will complete a DA Form 4137 for all items obtained. If this section is not used, "not used" will be written and the individual consenting to the search will initial beside the words "not used." Provide the complete physical address for a consensual search or seizure in the blank space titled "address." The address will also include any specific room, apartment, or building number. Do not draw through, black out, or cross out any item in the paragraph. This is written to allow seizure of all potential digital media or devices, accessories, and associated material or items, which may be at the location. The SA will complete DA Form 4137 for all items obtained at the address. If this section is not used, "not used" will be written and the individual will initial next to it.

(e) Paragraphs 3 through 5 should be read one at a time by the individual providing consent. Once a paragraph is read, the SA will read aloud the paragraph and then have the consenting person initial in the space provided at the end of the paragraph.

(f) Paragraph 6 ensures the individual understands the language being used. In the blank space, write the language used by the SA to brief and read the form to the individual.

(g) The individual providing consent will complete and sign the left signature block. The SA executing the consent form will complete and sign the right signature block. The SA will include their badge and credential number after their name. The date and time for both blocks will be legibly handwritten. Date will be DD/MMM/YY. Time will be in 24-hour format.

9–3. National security crimes

Crimes under U.S. ACI jurisdiction are contained in 18 USC and Federal criminal law. All crimes contain elements that must be proven in a court of law to prove a violation of said law.

a. Elements of crime.

(1) In any investigation, it is always important to understand and stay focused on the elements of the crime. It is a smart practice to periodically review the elements of the crime and ensure all investigative actions are tied to establishing one or more of the elements. If the SA cannot articulate how an investigative act will help prove one of the elements of the crime, seriously consider if that action is required. SAs must also be cognizant that other crimes may be present, view their case file for other possible applicable crimes, and coordinate with other law enforcement and intelligence community agencies as appropriate.

(2) Every crime has specific elements, all of which must be proven beyond a reasonable doubt to obtain a conviction. Elements are a set of facts assigned to a crime. While some Federal crimes have the elements explicitly listed in the Federal criminal code, others are derived from multiple sources, including case law, EOs, and regulations. SAs must gather evidence to prove each element of the crime happened or is present.

(3) The first rule is no crime occurred without relevant law. Hand-in-hand in this proven premise is the fact that the U.S. Government punishes people for their act, rather than thoughts or speech, unless that act constitutes a failure to act, an attempt to commit a criminal act, or conspiring to commit a criminal act. This rule can be defined as "no crime without a criminal act."

(4) Finally, a crime cannot occur without intent. This rule is key in espionage investigations. Intent relates to the state of mind of the individual committing the act. Intent can be difficult to prove, but evidence may be an email, blog, or witness interview where the subject advocates violence against the U.S. Government. Paragraphs 9–3*a*(4)(*a*) and 9–3*a*(4)(*b*) detail how the rule (a crime cannot occur without intent) applies to ACI investigations, specifically investigations involving suspected espionage. Espionage (18 USC 794(a)) contains the following critical elements, which must be satisfied to prove the crime:

(a) Anyone owing allegiance to the United States who provides aid and comfort to our enemies or to a foreign government, faction, agent, representative, citizen with the intent, reason, or reason to believe that the information will be used to the injury of the United States.

(b) Anyone communicating, delivering, transmitting, or attempting to communicate, deliver, or transmit national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense to a foreign government, faction, agent, representative, citizen, and others (recognized or unrecognized) with the intent, reason, or reason to believe that the information will be used to the injury of the United States or to the advantage of a foreign nation. Evidence is the national defense information or information connected to national defense that was communicated, delivered, transmitted, or attempted to be communicated, delivered, or transmitted. Other evidence may be an official passport from a foreign government, something that shows connection to a foreign government.

(5) The following are examples that investigators can look for to assist in proving the elements of a crime:

(a) Contact or communication: Are records available proving contact or communication with the FIE? Does source reporting indicate subject is associating or communicating with a suspected or confirmed agent of a foreign power? Approved electronic mail review can also assist with this element.

(b) Collection: Was the subject of the investigation collecting information to pass to FIE? Did FIE install malicious software on a U.S. Government computer system to facilitate remote access and control? This key point includes conspiring to commit a criminal act. Is there evidence that subject removed classified material from a Government facility?

(c) Tradecraft: Has the subject of the investigation utilized special means of contact, plans, meetings, or routes with FIE elements? In the cyber world, has subject used advanced tools to hide or encrypt information? This point assists with proving the criminal act and intent.

(d) Travel: Is there electronic or other evidence of travel to foreign countries? A FIE may require travel to neutral countries to facilitate meetings. This element again helps prove criminal intent.

(e) Motive or reward: Can Army intelligence gather evidence of unexplained wealth, bank accounts, and hidden funds? Why did subject commit this act? Was the motive money or ideology? Current analysis suggests espionage acts are committed to fit ideological viewpoints, rather than monetary desires.

b. Crimes within counterintelligence jurisdiction.

(1) SAs should bear in mind that not all crimes are solely within CI jurisdiction. In some cases, the SA will be limited to investigating only CI aspects of the crime or may be required to conduct the investigation jointly with another agency or even with the chain of command.

(2) Table 9–1 lists crimes under the USC within ACI jurisdiction (see ATP 2–22.2–1 for specific elements of these crimes or consult with supporting legal counsel).

(3) Table 9–2 lists crimes under the UCMJ within ACI jurisdiction (see ATP 2–22.2–1 for specific elements of these crimes).

Table 9–1
United States Codes within counterintelligence jurisdiction

Treason and treason-related offenses
Treason, levying war (18 USC 2381)
Treason, aid and comfort (18 USC 2381)
Misprision of treason (18 USC 2382)
Espionage and espionage-related offenses
Espionage (18 USC 794(a))
Espionage in time of war (18 USC 794(b))
Entering places connected with national defense (18 USC 793(a))
Gathering defense information (18 USC 793(b))
Unlawfully receiving defense information (18 USC 793(c))
Transmitting national defense information to unauthorized persons (18 USC 793(d))

Table 9–1
United States Codes within counterintelligence jurisdiction—Continued

Unauthorized retention of national defense information (18 USC 793(d) and 18 USC 793(e))
Negligent loss of national defense information (18 USC 793(f))
Failure to report the loss of national defense information (18 USC 793(f))
Photographing and sketching defense installations (18 USC 795)
Use of aircraft to photograph defense installations (18 USC 796)
Publication and sale of photographs of defense installations (18 USC 797)
Disclosure of classified communications information to unauthorized persons (18 USC 798)
Disclosure of classified communications information, general (18 USC 798)
Subversion-subversion-related offenses
Subversion (18 USC 2387)
Distribution of subversive literature to the military (18 USC 2387)
Subversion in time of war (18 USC 2388)
Subversive statements in time of war (18 USC 2388)
Sedition and sedition-related offenses
Rebellion or insurrection (18 USC 2383)
Seditious conspiracy (18 USC 2384)
Sedition (18 USC 2385)
Seditious literature (18 USC 2385)
Seditious organizations, organizing (18 USC 2385)
Seditious organizations, membership (18 USC 2385)
Sabotage and sabotage-related offenses
Sabotage, destruction of war material (18 USC 2153)
Sabotage, production of defective war material (18 USC 2154)
Sabotage, destruction of national defense material (18 USC 2155)
Sabotage, production of defective national defense material (18 USC 2156)
Terrorism and terrorism-related offenses
Terrorism, murder (18 USC 2332(a))
Terrorism, attempted murder (18 USC 2332(b))
Terrorism, providing material support to terrorist organizations (18 USC 2339B)
Terrorism, financing terrorism (18 USC 2339C(a))
Terrorism, concealing information pertaining to the financing of terrorism (18 USC 2339C(c))

Table 9–2
Uniform Code of Military Justice articles within counterintelligence jurisdiction

Defection, modeled from desertion (UCMJ, Art. 85)
Desertion with intent to remain away permanently (UCMJ, Art. 85)
Absence without leave (UCMJ, Art. 86)
Security violation, information security or violation of a regulation (UCMJ, Art. 92)
Security violation, failure to report CI incident or violation of a regulation (UCMJ, Art. 92)
Attempted mutiny (UCMJ, Art. 94)
Failure to prevent and suppress mutiny or sedition (UCMJ, Art. 94)
Failure to report mutiny or sedition (UCMJ, Art. 94)
Mutiny by refusal (UCMJ, Art. 94)
Mutiny by violence (UCMJ, Art. 94)
Sedition (UCMJ, Art. 94)
Aiding the enemy (treason) (UCMJ, Art. 104)
Aiding the enemy, harboring or protecting the enemy (treason) (UCMJ, Art. 104)
Aiding the enemy, giving intelligence to the enemy (treason) (UCMJ, Art. 104)
Aiding the enemy, communicating with the enemy (UCMJ, Art. 104)
Spies (UCMJ, Art. 103)
Espionage (UCMJ, Art. 103a)
Destruction of military property (UCMJ, Art. 108)

9–4. Evidentiary procedures

Evidence is anything that helps to ascertain the truth of a matter or gives proof of a fact in an investigation. Evidence may be physical or testimonial. Physical evidence includes any object, material, or data gathered to establish facts relevant to a specific crime or incident. Testimonial evidence includes documented written or verbal statements typically collected during CI investigative activities. Various individuals will control, store, or transmit evidence along a chain that can stretch over time and distance and the integrity of the evidence must be assured.

a. The company commander will—

(1) Appoint on orders a primary and alternate evidence custodian (EC) for the AO and each separate remote ACI FO or Military Intelligence Detachment (MID). The appointed primary and alternate EC at each location must be a credentialed SA with a minimum 1 year of investigative experience and must be a commissioned officer, warrant officer, noncommissioned officer, or DA Civilian in the grade GS–7 or above. CI agents still on probation will not be appointed as a primary or alternate EC. The remote FO or MID commander or SAC will never be appointed as the primary or alternate EC since the commander or SAC will perform and record monthly inventories of all evidence holdings. A copy of all current EC appointment orders will be kept on file in local the evidence files (see AR 195–5 for sample appointment orders).

(2) Supervise the EC.

(3) Perform monthly inventories of all evidence and associated documentation in possession of the EC serving the AO and ensure proper handling and processing of evidence. Each monthly inventory will be recorded on the next available line in the evidence ledger as required by AR 195–5. The following statement will be used to record the inventory details and both the commander or SAC and EC will sign the ledger following the written statement, "We, the undersigned, certify that on Day Month Year, in accordance with AR 195–5, a joint inventory of the evidence room was conducted. All evidence was properly accounted for with no exceptions (or with the following exceptions)." Immediately below this line, both the commander or SAC and the EC will list their names, grades, and positions and sign above their names.

(4) Conduct a monthly inventory. During a monthly inventory of an evidence room, if an item of evidence cannot be located, the EC and the commander or SAC, as appropriate, will have up to 5 working days to try to resolve the problem before an official inquiry is initiated. The apparent missing evidence could simply have been misplaced within the evidence room or there could have been a lack of proper documentation on the collection, processing, or transference of the items. If the problem cannot be resolved by the end of the fifth working day, an inquiry will be initiated as specified in AR 195–5. In case of lost evidence or breach of security, the commander will assign a senior SA to perform a complete evidence inventory and procedure review to locate the missing items. This inventory will be conducted by the person assigned to conduct the inquiry and will be conducted in the presence of the primary EC (or alternate EC if the primary is not available). Any corrective actions made to resolve the problem will be fully documented in an MFR. The MFR will be attached to the appropriate DA Form 4137.

(5) Ensure contract employees and all non-SA personnel do not issue receipts for evidence in a CI investigation via DA Form 4137. Once evidence is initially seized, only SAs may sign DA Form 4137 and handle evidence collected as part of a CI investigation. CI contract analysts and other non-SA personnel will not handle evidence while under the organization's control. In the case of electronic media, contractor analysts may handle working copies only. When needed and appropriate, a discipline counterintelligence threat assessment-trained SA will, using forensically sound methods, create a working copy of the media for the analyst to peruse. If special hardware is required (that is, a Serial Advanced Technology Attachment (ATA) write-block device), then the SA digital forensic examiner will assist.

b. All remote FO or MID commanders or SACs will—

(1) Perform monthly inventories of all evidence and associated documentation in their possession to ensure proper handling and processing of evidence has occurred. The monthly inventory will be performed jointly by the FO or MID commander or SAC (or acting commander or SAC only when on assumption of command orders) and primary EC (or alternate EC when the primary EC is absent). Each monthly inventory, no matter where performed or by whom, will be recorded on the next available line in the local evidence ledger. The following statement will be used to record the inventory details and both the commander or SAC and EC will sign the ledger following the written statement, "We, the undersigned, certify that on Day Month Year, in accordance with AR 195–5, a joint inventory of the evidence room was conducted. All evidence was properly accounted for with no exceptions (or with the following exceptions)." Immediately below this line both the commander or SAC and the EC will list their names, grades, and positions and sign above their names.

(2) Each FO or MID commander or SAC will also document monthly inventory results in MFR format and transmit a signed copy of the MFR via SIPRNET email message to the designated company level office. The MFR will list all items first by their local evidence ledger document number, from newest to oldest. The MFR will also include the associated date the item was received, its status (active, pending analysis, pending disposal determination, and so

forth), CI case control number, and brief description of the evidence items. Digital media evidence items temporarily shipped elsewhere for analysis (that is, two hard drives temporarily shipped between companies within the same battalion for digital media forensics) are still considered on-hand or "active" at the company and their status will be listed in the MFR as "pending analysis at: (list where the evidence was sent)." When items are permanently transferred from one EC to another, the losing element will complete the final disposition entries in their evidence ledger, file a copy of the updated DA Form 4137 showing the permanent transfer in inactive files, and will no longer list that item on monthly inventory MFR documents sent to unit operations. This normally will only apply to the EC located in unit headquarters who will temporarily receive items from the FO or MID and then later permanently return all items after completing digital media analysis.

c. These are procedures for the SA establishing chain of custody—

(1) This individual will be thoroughly familiar with requirements of AR 195–5, able to preserve potential evidence, and properly execute DA Form 4002 (Evidence/Property Tag) and DA Form 4137 when needed.

(2) Mark for identification (MFID) the seized items if reasonable and appropriate. MFID consists of time, date, and initials. Consider carefully how and where identification marks are placed upon items. Unnecessary damage or destruction of items of personal property that may ultimately be returned to the owner is prohibited (for example, using a permanent marker or scratching the required MFID details on the top or face of a computer tower system recovered during execution of a search warrant of an espionage subject). Consideration should also be given when marking items that may require future laboratory examination for latent prints. To avoid defacing or damaging such items, identification markings should be as inconspicuous as possible or the item should be placed in a container that is sealed and the container marked for identification.

(3) Put the evidence in an evidence container that is sealed and marked for identification if marking the evidence itself is not possible due to reasons such as value, size, or quantity. All evidence is permitted to be placed into containers that are sealed and marked for identification if so desired by the first SA receiving the evidence or the EC. Use of an evidence container is not mandatory, however, before evidence is sealed for reasons other than to protect it from cross contamination or to preserve evidence, the evidence will be jointly inventoried between the SA and the EC to ensure accuracy. The MFID marking will consist of time and date of acquisition and the initials of the person who assumed initial custody of the evidence. If an evidence container is used, all openings, joined surfaces, and edges of the evidence container will be sealed with paper packaging tape or with tape specifically designed for sealing evidence which will show signs of tampering if a seal is broken. A self-adhering DA Form 4002 will be affixed to the evidence container. The individual who sealed the evidence container will write their initials or signature on the seals in several different locations. The writing will be visible on both the tape and the evidence container. An evidence container designed by the manufacturer to seal evidence with built-in features to readily identify any signs of tampering may also be used. When a sealed container is breached, it will be resealed when appropriate. The individual resealing the container will write their initials or signature and time and date of resealing across the new seals.

(4) Properly complete DA Form 4002. A self-adhering DA Form 4002 will be attached to each item of evidence or evidence container at the earliest opportunity to identify and control it. When items are grouped together (for example, a box containing tools) and listed as one item on the DA Form 4137, only one DA Form 4002 will be used. The DA Form 4002 will be attached directly to the item of evidence or the evidence container or affixed to a blank shoe tag, which is attached to the item. Do not affix DA Form 4002 directly to a hard disk drive as it will cover the manufacturer's data plate or exposed circuitry. Instead, place the hard drive inside a non-static bag and label the bag. Do not use zipper storage bags to protect digital media as they will generate and hold static electricity. The CI case control number (CIR, LCA, PI, or FF case number) will be entered into the field titled "MPR/CID Control Number."

Note. Only the EC may complete the "Document Number" field located at the bottom right of the form. All other appropriate fields will be filled in by the agent taking custody of the evidence. The EC will enter the "Document Number" when the EC receives the evidence and verifies DA Form 4137 has no mistakes or errors. All fields on the DA Form 4002, except the "Document Number" field, will be completed by the SA who seizes the item (see AR 195–5 for an example).

(5) Obtain legible DA Forms 4137 for use. If using a carbon-copy version of DA Form 4137, then ensure the bottom copy is legible before it is detached and handed as a receipt to the person releasing the evidence. The use of a computer-generated DA Form 4137 is authorized; however, it must be prepared as a two-sided document with a vertical flip whenever reasonably possible.

(6) Execute one original and two carbon copies of each DA Form 4137. The original will be surrendered to the EC. The second copy will be retained in the agent's case file. The third copy will be provided to the owner or source as a receipt of the items seized. If carbon-copy forms are not available and if a copier machine is not available, then two additional two-sided blank vertical flip blank forms must be generated by hand to ensure the original DA Form 4137

and two copies exist. If handwritten copies are generated, the word "Copy 1" and "Copy 2" will be printed by hand in the top margin to clearly differentiate any copy from the original DA Form 4137.

(7) Ensure a CI case control number (CIR, LCA, PI, or FF case number) is recorded on the DA Form 4137 into the top right field titled "MPR/CID Sequence Number." The "Description of Articles" field will describe the item of evidence accurately to individualize the item to the exclusion of any other item. Descriptions will include only descriptive information and not include phrases based on supposition or suspicions. Descriptions should be limited to permanent characteristics. If serial numbers are available for an item of evidence, they will be recorded on the DA Form 4137. The words "Last Item" will be placed in capital letters after the last listed item on the next line below that final listed item. The words will be centered and lines or slashes will be drawn or typed from the centered words to the left and right margins. The "Reason Obtained" field will normally be "Evaluation as Evidence." When evidence is received from a consenting owner or during the execution of an authorized search, the last copy (Copy 2) of the signed DA Form 4137 will be provided as a receipt to the person releasing the evidence to the SA. When evidence is not obtained directly from a person's hand, the original and copies of the DA Form 4137 will be turned over to the EC for processing and distribution. After the EC has reviewed the original and all mistakes have been identified and corrected by the submitting SA, the EC will enter the next available document number on each form. The EC will then provide the CI agent with a new, updated Copy 2 for the SA's case records.

Note. Only the EC may complete the "Document Number" field on DA Form 4002 and DA Form 4137 since it is known only by the EC.

(8) Use a second DA Form 4137 when extra pages are necessary for listing additional items of evidence. All secondary pages will contain the same case control number, receiving activity, location, and person from whom received as entered on the first page of the DA Form 4137.

(9) If evidence items listed on a chain of custody document change hands enough times so that both the front and back side custody lines are filled up, then prepare another DA Form 4137 containing the same case control number, receiving activity, location, and person from whom received as entered on the first page of the DA Form 4137. Then make the following entry placed in the middle of the "Description of Articles" field: "Continuation of Chain of Custody, dated (enter last date shown on chain of custody on page 2 where the preceding chain of custody page ended)." The newly created additional chain of custody will be stapled to the original DA Form 4137 and used until evidence is disposed of (see AR 195–5 for an example DA Form 4137 continuation page should one become necessary).

(10) Distribute copies as follows: Normally Copy 2 (the bottom copy) will be provided as a receipt to the person who released the evidence to the CI agent and the other forms are surrendered to the EC. If Copy 2 is not provided as a receipt at time of seizure, the original DA Form 4137, along with all copies and the evidence itself, will be surrendered to the EC who will verify that all forms were correctly completed. Once verified or after any required corrections are made, the CI agent will release the evidence to the EC via signature. The EC will receive it via signature and enter the next available ledger document number onto both the DA Form 4002 (top field) and on the original DA Form 4137 (bottom right field). The EC will then destroy the old Copy 2 and create two new copies. Copy 1 will be stapled to the original DA Form 4137 and filed in the EC's evidence files. The new, updated Copy 2 will be provided to the agent for creation of an electronic copy (normally a .pdf file) for uploading as an attachment to the agent's report in ACOP.

(11) Release all physical evidence to the EC no later than the first working day after it is acquired, except in unusual circumstances. Evidence acquired during nonduty hours will be secured in a temporary storage container according to classification, in accordance with AR 195–5 and AR 380–5. The evidence will be controlled by the person securing it until released to the EC. For example, if the duty agent receives evidence on a Thursday (when Friday through Monday are a designated long weekend holiday period), the duty agent may secure the evidence in a lock-bag, retain all keys to it, and place the lock-bag in a General Services Administration security container until Tuesday, the next duty day, when the evidence is surrendered by the duty agent to the supporting EC (or shipped via U.S. Postal Service Registered Mail to a remote EC). Transmittal procedures outlined in AR 195–5 and AR 380–5 will be followed.

(12) Special instructions applicable to Federal grand jury materials held as evidence are detailed in AR 195–5.

d. The primary EC will—

(1) Account for, preserve, safeguard, and dispose of, when authorized, all evidence received in the evidence room or repository in a timely manner.

(2) Maintain an evidence ledger book in accordance with AR 195–5 for all evidence.

(a) The evidence ledger will be a bound book. Pages will not be removed by tearing, slicing, or any other means.

(b) The cover of the ledger book will identify the organization (such as, "ACICT, D Company, 308th MI Battalion") and dates spanned by the entries. If only one ledger exists at the element, the start date will be shown on the cover with a blank end date (that is, "15 July 2015 to…"). For ledgers that have been retired, their covers will reflect

a start and end date. The end date will be the date of final disposition of the last evidence item disposed of in the ledger.

(c) The ledger will be prepared in the same manner as depicted in AR 195–5 and will contain only the following six columns in the following order: (1) Document Number/Date Received, (2) CI Case Control Number, (3) Description of Evidence, (4) Date of Final Disposition, (5) Final Disposition, and (6) Remarks. These columns will span two facing pages when the book is opened.

(d) The first page of the ledger and the first page of each new calendar year will show column headings. Additional pages used during each calendar year may also show the column headings, if desired.

(e) Both vertical and horizontal lines will be used to separate each ledger entry.

(f) Black or blue ink will be used for entries. Only red ink will be used to draw a slanting line through a "Document Number/Date Received" column when items from that DA Form 4137 are completely disposed of or permanently transferred to another EC.

(g) There will be no blank pages or blank lines between ledger entries. If one or more line spaces were left between two entries, they will be lined through with the word "void" annotated in the space with the initials of the EC.

(h) Erroneous entries will be voided with one horizontal line drawn through the entry (but still leaving it legible) and initialed by the EC. No erasures, covering label, liquid correction product, or other correction product of any kind may be used to correct erroneous entries.

(i) The horizontal lines separating entries may be of a different color than the item entries to easily determine separation of entries. Evidence data entries are made in black ink and horizontal lines are drawn in blue ink.

(j) Whenever entries require signatures (such as monthly inventories, temporary absence of EC, or return or permanent change of EC), the entry will be handwritten and will extend across both pages of the ledger beginning on the next available line below the most recent entry. As many lines as needed may be used for the entry. Immediately above and immediately below this handwritten entry, horizontal lines will be drawn to clearly separate this handwritten area from the preceding and following DA Form 4137 evidence item entry.

(k) For ledger entries, complete the "Document Number/Date Received" column as follows: enter the next available document number on the next available line in the ledger. Immediately below it, enter the date the evidence was received by the EC.

Note. When all items pertaining to one document number entry are disposed of, a diagonal line (preferably in red ink) will be drawn across this column entry to visibly denote it as permanently closed. A document number consists of a sequential number followed by a hyphen followed by the two-digit calendar year (for example, "001–18" would be the first document number issued in calendar year 2018).

(l) For ledger entries, complete the "CI Case Control Number" column as follows: enter the full case number (that is, CIR BFH–18–029 or PI–18–902–BSA–012) at the time the evidence was received. If the case number is later changed (LCA elevated to PI), then the EC may, if desired, add the new PI number on the next available line directly underneath the existing case number entry.

(m) For ledger entries, complete the "Description of Evidence" column as follows: The item number from the corresponding DA Form 4137 will be entered followed by the item's description. Computer service tag number or hard disk drive make, model, and serial number whenever possible will be entered here. When DA Form 4137 lists more than one item number, each item and a brief item description will be listed in order in the ledger on separate lines starting with the first item number as listed on the DA Form 4137.

(n) For ledger entries, complete the "Date of Final Disposition" column as follows: enter the date the evidence was disposed of as shown in the "Chain of Custody" section of the DA Form 4137. If DA Form 4137 reflects multiple items and those items were disposed of on separate dates, then enter the corresponding disposal date opposite each item's description in the ledger.

(o) For ledger entries, complete the "Final Disposition" column as follows: enter a brief note on the means of final disposition opposite each item description. When all items in an entry are disposed of in the same manner at the same time, the means of disposal will be listed once and preceded or followed by the words "All Items" (that is, "all items returned to owning commander on 25 December 2018").

(p) In the "Remarks" column of the ledger entry, enter any information the EC deems necessary.

(q) Finally, after the last entry in the ledger at the end of every calendar year, the following statement will be entered in the ledger: "This ledger pertains to DA Forms 4137 from 001 through XXX (enter final document number) for calendar year (enter year)." The next ledger page will be used to list the column headings for the new year. A ledger book will normally be filled before starting a new one. Ledger books may be used for multiple years if a limited amount of evidence is collected by that element.

(r) Retired evidence ledgers will be retained in the evidence files and may be disposed of 3 years after the date the last item of evidence listed within the ledger was disposed or it may be held indefinitely as deemed appropriate. A notation will be made on the retired ledger cover annotating the last document number disposed of from that ledger and the date of that item's final disposition.

e. On return from temporary absence, the EC must ensure that all entries on all records from evidence taken in, released, or disposed of by the alternate EC are correct and accurate. If the absence was 30 calendar days or less, there is no firm requirement to conduct a 100-percent inventory between the returning EC and the alternate EC who maintained the records. At their discretion, the EC may perform a 100-percent inventory before resuming EC duties.

Note. Under alternate EC duties as described in paragraph 9-4r, in the primary EC's absence, the alternate EC may act as the primary EC and perform intake and disposal actions. Before that occurs, the alternate EC must write the following statement into the ledger and sign it to officially assume temporary duty as the primary EC, "I, (full name), on (date), assume all duties of the primary evidence custodian during the temporary absence of the regularly appointed custodian. I accept responsibility and accountability for all evidence in the evidence room." The alternate EC then must sign their name into the ledger following the statement and draw a horizontal line underneath it to separate it from the next entry made in the ledger.

(1) Upon return from temporary absence, after ensuring that all records are correct and all evidence is accounted for and properly documented, the primary EC will enter and sign the following statement in the evidence ledger immediately below the last entry: "I, (name), on (date), resume my position as primary evidence custodian and accept responsibility and accountability for all evidence in the evidence room. (Signature of primary EC)."

(2) If the EC finds that the alternate EC made an incorrect entry while they were away, they will immediately inform the local commander or SAC. The primary EC will prepare an MFR outlining the error and all corrective action taken. If the error occurred on DA Form 4137, then the MFR must be filed with (stapled or attached to) that DA Form 4137 for the life of the document. If the error was not on DA Form 4137 (that is, it was in the ledger), the MFR will be stored in an evidence file folder with copies provided to the lead SA for storage in the appropriate case jacket. Errors discovered on DA Form 4002 are immaterial as they are simply an administrative document and may be recreated at will if a mistake is noted. Because DA Form 4002 is simply an administrative form, no MFR need be generated when an erroneous form is replaced with a corrected version.

f. When permanently departing the position of primary EC, the departing and incoming primary EC will conduct a joint physical inventory. If the outgoing primary EC is unavailable (and will not become available), then the alternate EC will stand in to perform the joint inventory. All evidence records will be carefully checked to ensure proper documentation and accountability of all items. The outgoing EC will resolve all discrepancies to the satisfaction of the incoming EC before transfer of accountability.

(1) To officially make the transition, in accordance with AR 195–5, the statement in paragraph 9–4*f*(2) must be written into the ledger and signed by both the incoming and outgoing ECs on the next available line to complete the transfer of authority.

(2) Change of EC inventories will be entered in the evidence ledger immediately below the last entry. Both the incoming and the outgoing primary ECs will sign them as follows: "I, (name), assume the position of primary custodian and accept responsibility for all evidence shown on evidence custody documents in the evidence document files. A joint inventory was conducted on (date), with (name), the outgoing evidence custodian. Any discrepancies have been resolved to my satisfaction. (Signature of incoming primary EC) (Signature of outgoing primary EC or appointed person)."

g. On satisfactory completion of the change of custody inventory, each DA Form 4137 in the document files will be annotated and signed to show the outgoing EC released each item of evidence to the incoming EC. For evidence items temporarily sent elsewhere and not present to be inventoried, the incoming EC will check the file copies of DA Form 4137 in the suspense files to ensure they reflect the following:

(1) Authorized courier service or Registered Mail receipt number, if sent to company headquarters, United States Army Criminal Investigation Laboratory, or other agency.

(2) Proper signature, if released for court-martial, for investigations under UCMJ, Article 32 or other official purposes.

h. Maintain an evidence file section named "Active" that contains all active DA Forms 4137 for all evidence on-hand.

(1) A folder containing the 50 most recently received DA Forms 4137 (with the first copy attached to each), as determined by the assigned document number, will be stored in the same folder and sorted by the highest document number to the lowest document number. If more than 50 DA Forms 4137 exist for on-hand evidence items, then a second folder labeled "Active" may be used to hold the next 50 DA Forms 4137 and so on.

(2) Maintain an evidence file section named "Suspense" immediately behind the "Active" file section. Utilize three folders in the "Suspense" section that will temporarily hold the first copy of DA Form 4137 for an evidence item temporarily signed out by the EC. Temporary sign-out could entail, for example, shipping an evidence hard drive from the Army Counterintelligence General Counsel (ACIGC) EC to the company EC for digital forensic analysis in another location. Until that evidence item and its original DA Form 4137 are returned to ACIGC, the first copy will be maintained in suspense at ACIGC. Another example of a suspense action may be when the original DA Form 4137 and evidence are provided to supporting trial counsel for use in a courts-martial. Another example is just the original DA Form 4137 document is provided or sent to the supporting trial counsel for final disposal authority signature.

(3) At least three labeled suspense folders will be kept as follows:

(a) "Analysis" will contain Copy 1 of all original DA Forms 4137 for evidence temporarily transferred to headquarters or elsewhere for digital media examination.

(b) "Adjudication" will contain Copy 1 of all original DA Forms 4137 for evidence on temporary release to AR 15–6 investigating officers or UCMJ, Article 32 investigating officers, courts, trial counsel, civilian prosecutor, or other persons for legal proceedings.

(c) "Pending Disposition Approval" will contain Copy 1 of all original DA Forms 4137 of evidence when the original DA Form 4137 was sent to the trial counsel or civilian prosecutor for approval of disposition signature.

i. Maintain an evidence file section labeled "Inactive" immediately behind the "Suspense" file section containing folders labeled with the month and year evidence was finally disposed of. These folders will each contain original DA Form 4137 and related documents that have been properly disposed of during that month and year. These inactive files will be maintained in the evidence room and destroyed 3 years after the date they became inactive. Once original DA Forms 4137 have been placed in appropriately labeled inactive folders, duplicate copies may be destroyed with the exception of any duplicates that document transfers of the evidence not annotated on the original. Those that differ will remain together with the original custody document.

j. An updated first copy of the DA Form 4137 noting disposition of the evidence will be placed in the appropriate inactive DA Form 4137 file in the absence of the original if one of the following conditions exists:

(1) The original DA Form 4137 is entered as a permanent part in the record of trial.

(2) The original DA Form 4137 accompanies evidence released to an external agency.

(3) The original DA Form 4137 is not available for other reasons.

k. Ensure all DA Forms 4137 are completed correctly before accepting them and associated evidence from a collecting SA. If errors are detected on the form, the SA in possession of the evidence must make corrections in ink on DA Form 4137 and initial them. Because the DA Form 4002 is an administrative form only, these may simply be rewritten and replaced as necessary if an error is noted.

(1) If an error is noted on a DA Form 4137 after intake, the EC will make a good faith effort to locate the local SA responsible for the errors and have that SA correct their own errors and initial each in ink. The correcting SA will then prepare an MFR describing the errors they made and corrective action taken. The original signed MFR will be permanently attached to the original DA Form 4137 and a copy filed in the SA's case jacket.

(2) If the EC cannot reasonably locate the SA who originally made the errors, the EC will make required changes in ink, initial each, and document corrective actions taken in an MFR. The original MFR will be permanently attached to the original DA Form 4137 and a copy will be provided to the commander, FO or MID commander or SAC, and case SA for their case jacket. This circumstance may arise when a remotely stationed SA or EC mails evidence and associated original forms via authorized courier service or U.S. Postal Service to another EC and one or more mistakes are discovered after the shipment is received.

l. When evidence is temporarily released from the evidence room for any reason (that is, sent to a lab for analysis or provided for a UCMJ, Article 32 hearing or court-martial), the original DA Form 4137 will accompany the evidence. A new, updated Copy 1 of DA Form 4137 (updated to reflect this new transfer including the authorized courier service or U.S. Postal Service tracker number or signature of recipient) will be retained in the appropriate suspense folder until the evidence is returned to the evidence room. When the evidence and original DA Form 4137 are returned and updated with signatures reflecting return of the item, a new Copy 1 will again be created via copier machine and kept with the original form (the older, outdated Copy 1 that was held in suspense until the item was returned may then be destroyed). Always maintain an exact copy of the current DA Form 4137 with the original form. Whenever an original DA Form 4137 is updated, shred the current Copy 1 file and make a new one to staple to the original.

m. When transferring just one item from a DA Form 4137 that has multiple items listed on it, the original DA Form 4137 will accompany the transferring item. The Copy 1 document will be updated to reflect the transfer and stored in the suspense folder. For example, to transfer only item 4 of 6 via authorized courier service or U.S. Postal Service from ACICT to another location for digital media examination, the shipping ACICT EC will enter "4" in the next available Chain of Custody "Item Number" field, enter the date, complete the "Released By" field by signing it, and

complete the "Received By" field by entering the name of the authorized courier service or Registered Mail and the associated tracking number. The EC will then make a new Copy 1 and store it as the suspense copy in the ACICT evidence suspense files until item 4 and the original DA Form 4137 are returned. The receiving EC will line through the existing ACICT document number and add a new document number underneath the existing ACICT assigned document number because it must be entered into the evidence ledger of the receiving organization and is assigned a document number. When Item "4" and the original DA Form 4137 are later returned to ACICT, the old Copy 1 held in suspense at ACICT will be shredded and an updated Copy 1 will be created, attached to the original DA Form 4137, and stored in the active folder pending further disposition of the items.

n. When evidence is permanently forwarded to another office, the updated original and first copy of the DA Form 4137 will be provided to the gaining unit with an updated Copy 2 placed in the shipping EC's inactive file. If disposing of the item locally, update the original, make two copies, and file the original and one copy in the appropriate inactive file folder. The EC will provide the second completed copy to the case's lead agent for inclusion in the case folder and ultimately for inclusion into the official ROI. The disposition instructions and Date of Final Disposition columns in the ledger for that particular document number will then be completed for each item. If the document number contained multiple items that were disposed of on different dates, then the disposal date of each item will be entered onto the corresponding where the item description was entered. A diagonal line (preferably in red ink) will then be drawn from the top left to the bottom right in the "Document Number/Date Received" field for that entry in the evidence ledger to visually signify the assigned document number entry was terminated and all evidence disposed of.

o. Seek guidance from supervisors, fellow ECs, or appropriate trial counsel when unusual circumstances or situations arise about the evidence processing, handling, or final disposition that are not addressed within this pamphlet or AR 195–5. The unusual situation or circumstance and responding guidance will be written in a MFR or electronic mail correspondence that will be printed and attached to the original copy of the evidence document or with the appropriate investigative case file.

p. Evidence may be disposed of only after ACICA has approved the lead agent's proposed disposition method for each item collected in the case. When disposal is approved by ACICA, the EC will follow the disposal instructions detailed in this paragraph. The EC will ensure the appropriate disposition information is recorded in the "Final Disposal Action" and "Final Disposal Authority" sections on the back of the original DA Form 4137 before it is provided to the lead agent for presentation to the disposal approval authority (SJA) or Assistant United States Attorney (AUSA) for signature. The EC will create and file an updated Copy 1 in the suspense folder while the original DA Form 4137 is awaiting disposal signature. Normally, the original evidence custody document will be hand carried by the lead agent to the SJA or AUSA. If the evidence is no longer needed, the trial counsel or the civilian prosecutor will complete the final disposal authority portion of the evidence custody document by signing it and return it to the lead agent for return to the EC. When some evidence must be retained (for example, during the appeal process after an espionage conviction), the "Final Disposition Authority" section of DA Form 4137 will not be completed. A brief statement giving the reason for retaining the evidence will be furnished to the EC on separate correspondence.

q. Procedures for the alternate EC are as follows:

(1) Assume the duties and responsibilities of the primary EC during temporary absence. A temporary absence is more than 1 working day and not more than 30 consecutive days. Before performing any evidence intake operation, the alternate EC will enter and sign the following statement in the evidence ledger immediately below the last entry in accordance with AR 195–5: "I, (name), on (date), assume all duties of the primary evidence custodian during the temporary absence of the regularly appointed custodian. I accept responsibility and accountability for all evidence in the evidence room. (Signature of alternate EC)." This statement is required to be entered into the ledger before the alternate EC accepts and in-processes newly acquired evidence items and before any existing evidence already under control in the evidence room is transferred or disposed.

(2) A joint inventory need not be conducted between the primary EC and the appointed alternate EC if the alternate EC replaces the primary EC for 30 consecutive calendar days or less. However, if it is known that the primary EC will be gone for more than 30 consecutive calendar days, the alternate EC will be appointed on orders as the primary EC and a joint inventory will be conducted before the EC departs. If the alternate EC becomes the primary EC due to death, extension of absence beyond 30 calendar days, sudden illness, or emergency transfer of the primary EC, then a joint inventory will be conducted by the alternate EC and a person appointed by the CI commander.

r. Digital media forensic examiner SA evidence procedures are as follows:

(1) Receive, inventory, and sign for each evidence item in the Chain of Custody "Received By" field on the corresponding DA Form 4137 before taking physical control of digital media evidence. The original DA Form 4137 will remain in the possession of the digital media forensic examiner while they retain possession of the evidence item. The suspense copy of the DA Form 4137 (Copy 1) will be placed by the issuing EC into the evidence suspense folder

"pending examination" until the item is returned. Contractor employees and non-SA personnel are not authorized to sign DA Forms 4137 or possess evidence that is part of a CI investigation.

(2) Sign the DA Form 4137 "Released By" field when returning evidence to the EC or when transferring an item of evidence to another person, even if only for a brief period (that is, restroom or lunch break). Positive chain of custody control must never be broken.

(3) Make every effort to ensure digital media evidence is reasonably protected against static electricity and physical shock. Write-block devices will be used when connecting to or accessing seized digital media storage devices such as traditional Serial ATA laptop hard disk drives, Universal Serial Bus thumb drives, Secure Digital cards, micro eXtreme Digital cards, and so forth. Because cellular telephone handsets and other devices (that is, Global Positioning System) cannot be protected utilizing a traditional write-block device, alteration of data residing on these devices is unavoidable in most cases and thus permissible provided each step of the examination and the results of those steps are thoroughly documented and permanently maintained in the SA digital media examiner's case notes.

(4) Implement the hash-image-hash method when possible. This process will not be followed when dealing with random access memory imaging, cell telephone handsets, discrete "Black bag" imaging jobs, or other data collection operations such as when the original data to be imaged will be copied from across a network connection from a file server or when a hard drive to be imaged will be placed back into use after imaging.

(5) Hash-image-hash method.

(a) Write-block the original digital media device and establish its digital fingerprint hash value (that is, MD5, SHA1, or SHA256). Note the resulting hash value.

(b) Keep the original device write-blocked and create a duplicate image. Note the resulting hash value of the duplicate image file and verify that it matches the original item's value before continuing. Repeat the process to resolve any inconsistency or, if necessary, to verify the device being imaged is suffering hardware failure and data sectors may not be properly read. Thoroughly document duplication results and sectors that cannot be read.

(c) After duplication, keep the original device write-blocked and perform another hash of the original device to verify that duplication processes did not change one bit of data on the original device. Note the results and all three steps in the resulting investigative MFR.

(6) Take precautions when imaging data across a network connection because a typical write-block device cannot be used. For example, if the mission is to successfully copy a subject's user account profile folder from a computer, a specific folder located on a file server, or possibly a subject's home directory stored on another network server, then a network-capable capture tool that will preserve target folder and file date and time stamps and all metadata should be used (such as the graphic user interface-based AccessData Corporation Forensic Toolkit Imager v.3.2 or the Windows-based command-line tool robocopy.exe with mirroring, timestamp, and ownership preservation switches).

(7) Once an original digital media evidence item has been successfully duplicated or imaged and saved to a destination storage drive, this duplicate image will be referred to as the backup copy/best evidence (BCBE). A second copy of the duplicate image must then be created and verified that its hash value matches the original evidence item's hash value. This second copy will be used for examination. The SA digital forensic examiner who creates the BCBE copy will place it under chain of custody control via DA Form 4137. Once generated, the DA Form 4137 and the BCBE copy storage media will be released to the EC for storage. The second copy may then be examined by the SA digital media forensic examiner.

(a) When original digital media evidence is returned from the EC to the requesting office's EC (that is, a collected hard drive that was shipped from ACIGC to a receiving office for analysis), the corresponding BCBE image storage drive will normally remain with the receiving office until disposition occurs.

(b) If the originally seized digital media item is subsequently damaged, destroyed, or lost, the BCBE image copy may be introduced in court under the best evidence rule provided its chain of custody remained unbroken and its hash value verified it matched that of the original digital evidence item when the duplication occurred. Normally, when no longer needed as evidence, the hard drive holding the BCBE duplicate copy will be disposed of by data wiping while the original hard drive is returned to its owner or wiped, if appropriate. If the BCBE copy was saved to a digital versatile disc (DVD) or other type of removable media that cannot be wiped, then that media will be destroyed. This is common for email records obtained from DISA, who stores them on CDs or DVDs and provides them for examination. Each original BCBE evidence DA Form 4137 reflecting disposal, along with an updated Copy 1, will be filed in the inactive evidence files after the ledger entry for that item is closed and the "Document Number" column is lined out.

(c) Sample DA Form 4137 entries for a BCBE item placed under chain of custody control include—

1. The "Name, Grade and Title of Person from Whom Received" field will contain a checkmark in the "Other" box and reflect "(Unit) Forensics Computer."

2. The "Address" field will be left blank.

3. The “Location from Where Obtained” field will normally reflect, for example, “Forensic Computer, Room 310D, Building 1070, 4720 Gorgas Circle, Fort Generic, State, ZIP Code.”

4. The “Reason Obtained” field will reflect: “To preserve a duplicate copy” (or something similar).

5. The “Description of Articles” field will reflect data similar to this: “BCBE. Seagate 2-Terabyte Hard disk drive, bearing Serial Number 11223344 containing a duplicate image of Western Digital 500GB Hard drive with Serial Number: 99887766, comprised of 47 files named 99887766.E01 through 99887766.E47 and with MD5 Hash Value: 2edc45901fa45dce32109320edc123456.”

6. The “Released By” signature block will reflect: “N/A.”

7. The “Released By” name, grade or title field will reflect: “Forensic Computer.”

(8) Additional BCBE images of other digital media items seized as part of the same case may be added to an existing BCBE storage hard drive that has already been placed under chain of custody control. If this is the case, and the BCBE storage drive has enough empty space to hold one or more additional BCBE image files, the BCBE storage drive will be retrieved from the EC and additional BCBE images will be added to the storage drive. The existing DA Form 4137 description of the storage drive will not be altered to reflect the addition of data to the BCBE storage drive. Rather, the SA digital media forensic examiner who copied one or more additional BCBE images to the storage drive will simply generate an unclassified signed MFR on each occasion and staple or attach it to the BCBE storage drive’s DA Form 4137. The unclassified MFR contents should reflect an entry such as the following: “(MFR Subject) (Case Number PI–19–902–BSA–001): Addition of Data to Existing BCBE Storage Hard Drive.” “(MFR Body) On 19 December 2018, an image of Seagate 500GB hard drive, bearing serial number YTG340HG, comprised of 79 file slices named YTG340HG.E01 through YTG340HG.E79, was added to BCBE Seagate 2TB Hard disk Drive, Serial Number 11223344, which contained one or more duplicate images of digital media items previously seized during this investigation. The image file slices were copied into a subfolder named \YTG340HG and verified to match the original item’s MD5 hash value: 1234567890abcdef1234567890abcdef. (Signed) (Title).”

9–5. Authorization for final disposal of evidence

Property seized or held as evidence, other than contraband property which cannot legally be returned, will be returned to its rightful owner when it is determined that the property has no evidentiary value or when legal proceedings have concluded and the time to initiate appeals has passed. Personally-owned digital media storage devices known to contain present or deleted classified defense information will not be returned to private owners, but will be retained in the possession of Army or other Government officials authorized to retain or store those classified items. All final disposition of evidence actions will be documented in evidence ledgers and corresponding DA Forms 4137 which will be kept in the inactive file for 3 years. This requirement applies even if the lead SA determined that seized evidence is of no evidentiary value to the investigation and approval is obtained to return the item before case closure.

a. Procedure to obtain disposal approval.

(1) Evidence under the control of SAs will not be permanently transferred to another DOD agency (that is, Air Force Office of Special Investigations or Naval Criminal Investigative Service) without prior approval from the Army Counterintelligence Coordinating Authority-Program Manager (ACICA–PM). Send an alert in the ACOP system requesting approval of the transfer. Action will not be taken until ACICA officially approves or concurs with the request.

(2) Evidence under the control of SAs will not be permanently transferred to another Federal agency (that is, the FBI) without prior approval from ACICA–PM. Coordination to permanently transfer evidence that was collected in a closed case or collected during an open, on-going, joint PI or FF case to the FBI (or other Federal agency) must occur between the lead agent and the ACICA–PM prior to the transfer of evidence. Copies of digital media may be provided to the joint agency as part of information sharing during these joint investigations, but original evidence items may not be provided until permission is first obtained from ACICA.

(3) The lead case agent is responsible for coordinating disposal of all evidence collected in each case. The lead case agent will confer with the local FO or MID operations officer and commander or SAC and then the operations staff to determine prospective appropriate disposal instructions for each item (return to owner, destroy, and so forth). When recommending disposal of each specific evidence item, the lead agent must remember to include the identity and disposition plan for all items held in evidence and not just the evidence held in the lead agent’s FO or MID office.

(a) Once decided, the lead case agent or FO or MID operations officer will submit an alert in ACOP notifying all operational control levels (FO, operations, and ACICA) of the proposed disposal decision for each item of evidence. After ACICA concurrence, disposal action may be taken.

(b) If an item held as evidence is deemed to be of no evidentiary value to the case and if the ACICA has authorized disposal, the FO or MID commander or SAC may sign as disposal authority on the back of the DA Form 4137. The EC then performs disposal, updates the DA Form 4137, closes out the evidence ledger entry, and files the original DA Form 4137 with an updated Copy 1 in the local inactive evidence files for 3 years. If the disposed of item at the FO

or MID was a digital media storage device (that is, NIPRNET hard drive), a corresponding BCBE image copy of that item will normally be stored in the company operations main evidence room and under separate chain of custody control. Because of this, each FO or MID should notify the unit EC whenever any evidence disposition has been authorized to ensure all original evidence and corresponding BCBE copies are disposed of. If original or BCBE copies of evidence are held at the unit's headquarters main evidence room, the EC will pull the original DA Form 4137, enter the anticipated disposal actions onto the back side, scan them, and send them via email to the lead agent. The lead agent will then print both sides of the updated DA Form 4137 and take to the supporting Judge Advocate General prosecutor (if a military subject) or AUSA (if a civilian subject) for disposition approval signature. Once signed, the lead agent then scans and emails back page 2 bearing the disposal approval signature. The EC then prints a copy of the signed page 2 and attaches it to the original DA Form 4137, then performs the disposal.

Note. At the discretion of unit operations, even if original items are deemed not pertinent to the case, not needed, or returned to the owner (that is, a NIPRNET hard drive returned to the command), then the corresponding BCBE image may not be destroyed, but instead may be retained as active evidence until the case is closed and disposition of remaining evidence in the case occurs.

(c) At the end of an investigation, if an item held as evidence is deemed of potential evidentiary value for prosecution, and if unit operations and ACICA–PM concurs, then the case agent will coordinate with the supported unit's trial counsel to determine whether the unit intends to take adverse administrative or UCMJ action against the subject and if the evidence item to be disposed of is pertinent to the charges or may be destroyed or returned to owner. If no adverse action will be taken by the unit or a civilian court, then the items may be disposed of after the trial counsel signs the DA Form 4137. However, if adverse action is pending by the unit involved (or if civilian court proceedings are anticipated), the items held as evidence will not be disposed of until the unit's trial counsel (or civilian prosecutor) approves and signs the disposal authority section on the DA Form 4137.

(d) If ACICA–PM concurs with the lead case agent's recommended disposal actions for each item, the lead case agent will comply with ACICA–PM directives or instructions. For example, if the lead case agent deemed an item collected in the case has no evidentiary value and wants permission to dispose of it immediately, the ACICA–PM may disagree and direct the evidence item be retained under chain of custody control until the case is closed. If such a decision occurs, another disposal request must be made to ACICA–PM upon case closure. The CG, INSCOM has a responsibility for determining what information obtained during an investigation is to be included in an ROI and permanently retained in the investigative file when the ROI is sent to the USAIRR. In such instances, the ACICA–PM will make that determination and communicate it to the field. Normally this will occur at the end of a case after the lead case agent confers with the unit's operations and submits a request for evidence disposal with a recommended action for each item collected (return to owner, destroy, include in ROI or USAIRR, and so forth). Normally the lead agent submits an alert in ACOP containing the proposed disposition of items. Once ACICA replies affirmatively, disposal occurs.

Note. ACICA–PM may direct an evidence item be included in attached to the ROI.

b. Authorization for disposal in unfounded, unsolved, and transferred cases.

(1) Evidence in a closed, unfounded investigation may only be disposed of after obtaining ACICA–PM concurrence as described in paragraph 9–5*a*. The release authority will be the local FO or MID SAC or commander.

(2) Evidence in an unsolved investigation, with two exceptions listed in paragraphs 9–5*b*(2)(*a*) and 9–5*b*(2)(*b*), may be disposed of after receiving concurrence ACICA–PM and after the unit trial counsel reviews and approves the release by completing the "Final Disposal Authority" section of DA Form 4137. Three months after completion of the investigation, the FO or MID SAC or commander may, without trial counsel approval, review, and approve the release by completing the "Final Disposal Authority" section of DA Form 4137.

(a) Exception 1. The trial counsel (or civilian prosecutor) and the FO or MID SAC or commander must exercise caution with cases involving other serious crimes when there is a chance that a currently unknown subject may be identified later. Evidence should be retained for a reasonable amount of time in instances of repetitive unknown subject cases that may have been committed by the same person.

(b) Exception 2. Evidence involving other serious unsolved cases may be retained indefinitely, as deemed appropriate. The FO or MID SAC or commander will prepare a memorandum explaining the reason for retaining the evidence. The memorandum will be maintained in the case file with a copy attached to the original DA Form 4137 and a copy provided to the unit's operations element.

(3) When evidence is permanently transferred to a non-DA law enforcement or intelligence agency, the "Final Disposal Authority" section of DA Form 4137 will be completed by the FO or MID commander who controls that evidence.

c. Authorization for disposal of evidence following judicial proceedings. Evidence released to trial counsel, a civilian prosecutor, or their designated representative for judicial proceedings will be returned as soon as possible to the EC for final disposition. When evidence is released to trial counsel, the EC or intermediary releasing SA will ensure the trial counsel or prosecutor is familiar with the requirements of AR 195–5. The trial counsel or prosecutor will be made aware the evidence must be returned to the controlling EC as soon as the evidence is no longer required at the conclusion of the court proceeding, unless the evidence is entered as a permanent part in the record of trial. The trial counsel or appropriate prosecutor will maintain adequate custody of the evidence to ensure its integrity and to prevent its loss or damage. If an item of evidence is made part of the trial record, the trial counsel should immediately notify the EC so DA Form 4137 can be properly annotated. This will be considered final disposition.

9–6. Procedures for final disposal of evidence

a. Final disposal procedures. Evidence will be expeditiously disposed of after it has served its purpose or has no further evidentiary value. When witnessing the destruction of evidence, the witness will physically view the items designated for destruction prior to the destruction and not just the container in which the items are contained. When a legal issue concerning methods of disposal arises, the trial counsel will provide legal advice. All completed DA Forms 4137 reflecting final disposition has occurred will be provided to the lead SA for inclusion in the official ROI and case jacket.

b. Personal property other than firearms, ammunition, or explosives. Personal property that is not contraband, as determined by the trial counsel, will be released to the rightful owner.

c. United States Government property, firearms, ammunition, and explosives. Any U.S. Government property, firearms, ammunition, or explosives seized as evidence will be returned to the proper military unit.

d. Classified items, information, or material. Items of evidence that are classified or contain classified information or material will be disposed of in accordance with AR 380–5.

9–7. Loss of evidence

a. During an inspection or inventory of an evidence room, if an item of evidence cannot be located, the EC and the CI supervisor, as appropriate, will have up to 5 working days to try to resolve the problem before an official inquiry is initiated. The apparent missing evidence could simply have been misplaced within the evidence room or there could have been a lack of proper documentation on the collection, processing, or transference of the items. If the problem cannot be resolved by the end of the fifth working day, an inquiry will be initiated as specified in accordance with AR 195–5. Any corrective actions made to resolve the problem will be fully documented in a MFR. The MFR will be attached to the appropriate DA Form 4137.

b. If evidence is lost or security of the evidence room is breached, a 100-percent inventory will be conducted and an inquiry or investigation will be performed in accordance with AR 15–6. Inquiries or investigations will be initiated by the appropriate CI commander. All losses or breaches of security and the start of inquiries will be reported to Army G–2X, 1000 Army Pentagon, Washington, DC 20310–1000, as appropriate.

c. If the inquiry fails to account for or recover the evidence, relief for accountability of the evidence must be granted. For CI units, relief will be granted by the Army G–2X. The relief from further accountability for lost evidence—

(1) Permits the closure of DA Form 4137.

(2) Has no bearing on administrative or judicial action taken against those responsible for the loss or breach.

d. Upon receipt of packaged evidence, if evidence appears to be missing after the parcel has been inventoried, then the appropriate local CI supervisor will be notified immediately by the primary or alternate EC. On verification of missing evidence from the parcel, the sender will be notified immediately and requested to search for the missing items. If the sender cannot locate the missing evidence, an inquiry will be conducted in accordance with AR 15–6.

9–8. Evidence storage

In accordance with AR 381–20, SAs are authorized to store evidence classified up to secret pertaining to CI investigations in a security container or secure room authorized for the storage of classified material classified up to secret. Access to the security container will be restricted to the primary and alternate EC. Storage and chain of custody control of evidence items classified at a higher level must be coordinated on a case-by-case basis with the supporting SSO. For example, coordination could result in the SSO temporarily providing exclusive use of a one-drawer safe that can then be used hold special access or top secret evidence materials and maintain chain of custody.

a. Evidence room or security container. The evidence room or security container will be locked at all times when not occupied by the primary or alternate EC. Authorized personnel will have access to the evidence room or security

container only when accompanied by the responsible EC. The EC will accompany all personnel in the evidence room or security container at all times.

b. Key and combination control.

(1) Only primary and alternate ECs will know the combinations of locks in the evidence room or security container. However, copies of all combinations will be recorded on SF 700 (Security Container Information). The sealed SFs 700 will be kept sealed and stored in a safe controlled by the EC's supervisor, senior CI operations officer, and commander or SAC at each location.

(2) Each key-operated lock used to secure an evidence room or container will have two keys with the exception of the high security padlock, which is supplied with three keys (two operator keys and one control key). The primary EC will always keep one key to each lock. The duplicate key for each padlock and control key for high security padlock will be put in a separate sealed envelope and secured in the safe of the appropriate supervisor.

(3) Lock combinations will be changed whenever the primary or alternate EC changes. All combinations and key locks will be changed upon possible compromise.

(4) Keys will be transferred from the primary to the alternate EC, only if the primary EC is to be absent for more than 1 working day.

(5) Master key padlocks or set locks will never be used in the evidence room.

Appendix A

References

Section I

Required Publications

AR 195–5
Evidence Procedures (Cited in para 2–44*r*(1).)

AR 380–5
Army Information Security Program (Cited in para 1–7*d*(3)(*e*).)

AR 381–10
U.S. Army Intelligence Activities (Cited in para 1–5*b*(2)(*p*).)

AR 381–12
Threat Awareness and Reporting Program (Cited in para 1–5*e*(2).)

AR 381–20
Army Counterintelligence Program (Cited in title page.)

Army Counterintelligence Security Classification Guide
(Cited in para B–4*a*.) (Available from CG, U.S. Army Intelligence and Security Command (IACG), Fort Belvoir, VA 22060–5246.)

ATP 2–22.2–1
Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U) (Cited in para 1–6*i*.)

ATP 2–22.2–2
Counter Intelligence Volume II: Operations and Collection Activities (Cited in para 1–6*i*.)

ATP 2–22.2–3
Counterintelligence Techniques, Volume III: Investigations Handbook (Cited in para 1–6*i*.)

ATP 2–22.33
2X Operations and Source Validation Techniques (Cited in para 1–6*i*.)

ATP 3–39.12
Law Enforcement Investigations (Cited in para 2–44*r*(3).)

DOD 5240.01–R
Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons (Cited in para 1–8*h*.)

DODD 5240.02
Counterintelligence (CI) (Cited in para 1–6*i*.)

DODM 5240.01
Procedures Governing the Conduct of DOD Intelligence Activities (Cited in para 1–5*e*(1).)

EO 12333
United States Intelligence Activities (as amended by EO 13470) (Cited in para 1–6*i*.) (Available at https://www.archives.gov/.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. DOD material is available at https://www.esd.whs.mil/. USC material is available at https://uscode.house.gov/.

ADP 1–02
Terms and Military Symbols

Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation
(Available in the ACOP library.)

AR 15–6
Procedures for Administrative Investigations and Boards of Officers

AR 25–2
Army Cybersecurity

AR 25–30
Army Publishing Program

AR 25–400–2
The Army Records Information Management System (ARIMS)

AR 190–6
Obtaining Information from Financial Institutions

AR 380–28
Army Sensitive Compartmented Information Security Program

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities

AR 381–47
Offensive Counterintelligence Operations

DOD Dictionary of Military and Associated Terms
Department of Defense Dictionary of Military and Associated Terms (Available at https://www.jcs.mil/.)

DODI 3025.21
Defense Support of Civilian Law Enforcement Agencies

DODI 5400.11
DOD Privacy and Civil Liberties Programs

DODI 5400.15
Guidance on Obtaining Information from Financial Institutions

Federal Rules of Evidence
(Available at https://www.rulesofevidence.org/.)

JP 2–01.2
Counterintelligence and Human Intelligence in Joint Operations (Available at https://www.jcs.mil/.)

Manual for Courts–Martial United States (2019 Edition)
(Available at https://jsc.defense.gov/.)

PL 91–508
Federal Deposit Insurance Act, amendments (Fair Credit Reporting Act) (Available at https://www.govinfo.gov/.)

PL 99–508
Electronic Communications Privacy Act of 1986 (Available at https://www.govinfo.gov/.)

PL 103–359
Intelligence Authorization Act of 1995 (Available at https://www.govinfo.gov/.)

PL 107–56
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Available at https://www.archives.gov/.)

U.S. Reports: Miranda v. Arizona, 384 U.S. 436 (1966)
(Available at https://www.loc.gov/.)

31 CFR Chapter X
Financial Crimes Enforcement Network, Department of the Treasury (Available at https://www.ecfr.gov/.)

5 USC 303
Oaths to witnesses

5 USC 552
Public information; agency rules, opinions, orders, records, and proceedings

5 USC 552a
Records maintained on individuals

5 USC 552a(b)
Conditions of Disclosure

10 USC
Armed Forces

12 USC
Banks and Banking

12 USC Chapter 35
Right to Financial Privacy

12 USC 3401
Definitions

12 USC 3412
Use of information

12 USC 3414(a)
Access to financial records for certain intelligence and protective purposes

15 USC Chapter 41 Subchapter III
Credit Reporting Agencies

15 USC 1681f
Disclosures to governmental agencies

15 USC 1681u
Disclosures to FBI for counterintelligence purposes

15 USC 1681v
Disclosures to governmental agencies for counterterrorism purposes

18 USC
Crimes and Criminal Procedure

18 USC 793
Gathering, transmitting or losing defense information

18 USC 794
Gathering or delivering defense information to aid foreign government

18 USC 795
Photographing and sketching defense installations

18 USC 796
Use of aircraft for photographing defense installations

18 USC 797
Publication and sale of photographs of defense installations

18 USC 798
Disclosure of classified information

18 USC 1621
Perjury generally

18 USC 2153
Destruction of war material, war premises, or war utilities

18 USC 2154
Production of defective war material, war premises, or war utilities

18 USC 2155
Destruction of national-defense materials, national-defense premises, or national-defense utilities

18 USC 2156
Production of defective national-defense material, national-defense premises, or national-defense utilities

18 USC 2332(a)
Homicide

18 USC 2332(b)
Attempt or conspiracy with respect to homicide

18 USC 2339B
Providing material support or resources to designated foreign terrorist organizations

18 USC 2339C(a)
Offenses

18 USC 2339C(c)
Concealment

18 USC 2381
Treason

18 USC 2382
Misprision of treason

18 USC 2383
Rebellion or insurrection

18 USC 2384
Seditious conspiracy

18 USC 2385
Advocating overthrow of Government

18 USC 2387
Activities affecting armed forces generally

18 USC 2388
Activities affecting armed forces during war

18 USC 2703(f)
Requirement to preserve evidence

18 USC 2709
Counterintelligence access to telephone toll and transactional records

31 USC 5311
Declaration of purpose

31 USC 5318(g)(2)
Notification prohibited

32 USC
National Guard

50 USC Chapter 44
National Security

50 USC 1806(b)
Statement for disclosure

50 USC 1825(c)
Statement for disclosure

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the APD website (https://armypubs.army.mil).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 2805
Polygraph Examination Authorization

DA Form 2823
Sworn Statement

DA Form 3697–R
Subvoucher for Distribution from Confidential Funds

DA Form 3881
Rights Warning Procedure/Waiver Certificate

DA Form 4002
Evidence/Property Tag

DA Form 4137
Evidence/Property Custody Document

SF 86
Questionnaire for National Security Positions

SF 700
Security Container Information

SF 1034
Public Voucher for Purchases and Services Other Than Personal

Appendix B

Format Rules for Counterintelligence Reports

Conducting investigative activity and producing evidence are only part of the investigative process. SAs must be also be adept at documenting and transmitting their findings to decision makers and adjudicators via the many CI reports. Each CI report has a specific purpose and guidelines that must be observed when documenting a CI investigation. All CI reporting will put into ACOP.

B–1. Overview

Quality reports depend on the writer and reviewer's attention to detail and to addressing the basic investigative interrogatives. The SA's report will become the sole source of information on that particular investigative activity. Reports must be accurate, clear, impartial, and complete. The following is a step-by-step guide, integrating all current guidance for the preparation of CI reports.

B–2. Principles of report writing

a. Finalized intelligence reports provide the Commander, ACICA and legal counsel with a tangible product that influences their decision-making process and helps to shape investigations and prosecution procedures. Operational intelligence and technical reporting documents the conduct of ongoing investigations and allows operational management elements to conduct technical authority and oversight of CI investigative activities.

b. Effectively communicating information collected during an investigation is a skill that takes time, repetition, and mentorship to master. CI investigative reports not only have to reflect the information collected during an investigation, but also must often anticipate the Commander, ACICA or legal counsel's questions concerning lack of detail or information gaps that must be addressed through investigative activity. The basic tenets of CI reporting include the following:

(1) *Accuracy.* The investigative report must accurately convey the information obtained from an interview, records check, or special investigative technique by transcribing it into a protected investigation report. The report writer should never embellish, draw conclusions, infer, or otherwise interpret a source's meaning or understanding of the information provided to the SA. If a source or subject expresses an opinion or belief, it must be reported as such and not written as fact.

(2) *Concise and complete.* Cover only the facts or information provided by the source. Reports must answer the six basic interrogatives: who, what, when, where, why, and how. Leave no unanswered questions for the reviewer. The Commander, ACICA and legal counsel have a large volume of information to synthesize to form their assessments. Reports should not be wordy. The information conveyed should be to the point, while providing the full depth of the information. Any lack or failure to obtain information should be explained in the report (for example, Source did not know).

(3) *Clarity.* The report will be organized and understandable. SAs must write sentences clearly to avoid any possible misinterpretation of the facts. Convey the information in as simple wording as possible. Writers should use short sentences and logically arrange the information so that the report does not confuse the reader. Each investigative report must stand on its own.

(4) *Timeliness.* Disseminate the information through investigative channels in the most expedient manner possible. While written reports are preferable, the perishability and time sensitivity of the information may dictate the use of voice communications with a followup written report. When in doubt, CI agents should discuss reporting options with their SAC.

B–3. Quality control

Quality control is the oversight of reports production to ensure that a quality product is disseminated from the investigative element to the Commander, ACICA and legal counsel. Administrative quality control ensures writers adhere to applicable regulatory guidance and unit SOPs for format, verbiage, and other administrative criteria that are required in the reports. Information quality control analyzes the information content to identify inconsistencies, information gaps, or unfounded conclusions within the report that conflict with other credible and corroborated reporting or will raise questions by the Commander, ACICA and legal counsel.

B–4. Classification and classification authority

a. Classification. Reports may range from unclassified/for official use only to top secret according to content. CIRs and investigative reports in open investigations are classified from for official use only to top secret depending on content. Refer to the Army Counterintelligence Security Classification Guide (SCG), AR 381–12, and AR 381–20

for specific guidance. Per the SCG, investigative plans, procedure requests, and requests for CI technical support are classified secret, as they reveal methods of operation. Reports will be marked in accordance with AR 380–5. Date of submission, case control numbers, and signature blocks are unclassified. The signature block for memorandum format reports will not be portion marked. Occasionally, specific units and activities or programs utilize other approved SCGs. When using this specialized guidance, ensure that it is appropriately cited.

b. Classification authority. Per Army SCG, the following classification authority is required for all classified reports dealing with counterespionage investigations:

(1) Classified by: (Name and title of derivative classifier).
(2) Derived from: ACI SCG.
(3) Declassify on: (Enter declassification instructions from appropriate table using YYYYMMDD format).

B–5. Preparation of counterintelligence reports

a. SAs will write their own reports. Supervisors may edit these reports for grammar and clarity, but only the SA can alter the basic meaning and intent.

b. CI reports are written in narrative style, third person. Agents will write in the active voice except when quoting the source, indicating a state of mind or condition, or when describing attachments.

c. The use of simple, direct, standard English facilitates understanding and reduces the risk of misinterpretation. The SA must avoid slang expressions, colloquialisms, vulgarisms, and technical or trade terms, except when their use, in direct quotes from source or subject, will add to an understanding of the information reported or to an assessment of the source and the information.

d. The SA must not use expressions that reflect approval or disapproval about the occurrence, persons, or objects being described. Statements will be written so that they can be verified through independent investigation by checking records or other credible sources. The detailed techniques and procedures used to develop the information are not described in the report. They may be made a matter of local record through operational reporting procedures. The unit commander may establish the operational reporting and procedures for each element.

B–6. Identity of persons

Because it has a very specific legal meaning, the word "suspect" is not an appropriate term when referring to the subject of a CI investigation. Instead, the term "subject" will be used in all CI investigative reporting. In the introductory paragraph of the ACOP ROI entry, identify the subject by full name, rank or grade, SSN, and DPOB. Sources will be identified by full name, rank or grade, SSN, DPOB, and unit or place of employment. After subject and source have been identified by name, refer to them as "SUBJECT" or "Source" as appropriate.

a. All names will be written in the normal order. Write the surname (last name) of the subjects in uppercase letters (for example, "Paul Michael SMITH" or "WALKER, Robert C." (only in SUBJECT block)).

b. Within the text of the report, the word "SUBJECT" written in uppercase letters will be used (for example, "SUBJECT traveled to Austria monthly" or "SUBJECT purchased the car").

c. However, the word "SUBJECT" cannot be used in the first sentence of the introductory paragraph. In the introductory paragraph, use the subject's full name.

d. When personal pronouns are used to refer to the subject, write the pronouns in uppercase letters (for example, "SUBJECT and HIS wife moved to Alabama").

e. In the case of multiple subjects, use the terms SUBJECT 1, SUBJECT 2, and so forth. Avoid the use of personal pronouns when there are multiple subjects.

f. When using the pronoun "they" to refer to the subject and another person, follow normal capitalization for the pronoun (for example, "They were friends" or "Jones first met SUBJECT when they attended ANCOC together").

g. For clarity, use two singular subjects in the sentence instead of a plural form of the surname or plural pronoun (for example, "SMITH and HIS family moved to Europe").

h. Avoid using the relative pronouns "who" and "whom" when writing about subjects of investigations.

i. When showing the possessive and using the word "SUBJECT," the possessive "s" is always capitalized (for example, "SUBJECT'S car was parked on the street in front of HIS house").

B–7. Witnesses of information

a. Write the names of persons that are not subjects with normal capitalization (for example, "Frank Wallace met SUBJECT in college. Wallace tutored HIM on history").

b. After fully identifying the person being interviewed, this person may be referred to as "Witness" except for CIRs where the source will be referred to by last name throughout the report. This will help in sanitizing the ACOP ROI

entry later. Witness's name should be used in the narrative portion only when essential for clarity (for example, "Steve S. Smith provided that SUBJECT often traveled to Germany. Witness traveled with SUBJECT on several occasions").

c. Avoid use of phraseology such as "Witness stated," "Witness provided," "Witness said," and so forth throughout the text of the ACOP ROI entry. This phraseology should be used only in the introductory paragraph. Further use would be redundant since the narrative text of an ACOP ROI entry pertaining to the interview of a source is limited to information stated or provided by that source.

d. Whenever the word "Witness" is used to refer to the interviewee, the "W" will always be uppercase (for example, "SUBJECT told Witness a funny story" or "SMITH visited Source daily").

e. The first letter of a personal pronoun referring to the source will be uppercase (for example, "He was SUBJECT'S friend. SUBJECT visited source at His home").

B–8. Other identified persons

All persons, other than subject and witness, mentioned in investigative reports will be fully identified to the best of source's ability, the first time by their first, middle, and last name; rank or grade (if DOD affiliated); social security account number, DPOB, and duty position; and unit of assignment (if DOD affiliated) or employment (if non-DOD affiliated). If identification is incomplete, use not further identified (NFI). After identifying a person, they will be referred to thereafter only by surname without any titles such as mister (Mr.), mistress (Mrs.), Doctor (Dr.), or Professor (Prof.), unless there is more than one person with the same surname in the same report. For example—

a. One person: "SUBJECT associated with Prof. John R. Talbot. SUBJECT worked for Talbot at Antioch. Talbot was HIS supervisor."

b. Two persons: "SUBJECT was associated with Dr. Andrew L. Goodman and Carol M. Goodman. SMITH worked for Dr. Goodman at County General Hospital. HE saw Carol Goodman at social functions."

c. Names are written according to the custom of the person's native country (for example, Asian names are written with the surname first). This fact will be noted in the agent's notes.

B–9. Names of persons that cannot be fully identified

a. When the SA can report only the surname of an individual in a report, no punctuation will precede the surname. The term first name unknown (FNU) can be used. Do not write FNU within quotation marks or parentheses. When using the term FNU or when the first name can be either male or female, use an honorific title or common noun indicating the sex of the person. For example—

(1) *Right.* "SUBJECT associated with Mr. FNU Martin" or "HIS teacher was FNU Stewart, a male." "SUBJECT associated with Miss Leslie Ward" or "HIS teacher was Leslie Hampton, a female."

(2) *Wrong.* "His teacher was female, (FNU) Malone." "HE knew Mr. "FNU" Singletary."

b. When the SA can report only the first name of an individual, use the term last name unknown (LNU) written in uppercase letters. Do not write LNU within quotation marks or parentheses. For example—

(1) *Right.* "LAPD arrested SUBJECT and Stanley LNU" or "Mr. Stanley LNU was HIS supervisor."

(2) *Wrong.* "SUBJECT and Mary "LNU" dated frequently" or "SUBJECT and Walter (LNU) were friends."

c. Do not use the terms FNU and LNU together. If a person or place is unknown, use terminology such as, "SUBJECT visited a man, name unknown, in Baltimore. After high school, HE left for an unidentified college in the Midwest."

d. The short title for no middle name (NMN) will not be used except in SUBJECT blocks of reports when listing the identification of the subject as indicated on the ACICA case opening message. Enclose these short titles in parentheses. If the source provides the name of an individual, but cannot spell the name, the SA will spell the name phonetically and so indicate by the word (phonetic) in parentheses and in lowercase letters immediately after the spelling (for example, "HIS supervisor was Morris Munopoulos (phonetic) while HE worked at the Esmoflaies (phonetic) Supermarket").

e. Use the term "NEE" written in uppercase letters followed by a colon to indicate maiden names in the ACOP ROI entry. Do not use NEE if the maiden name is unknown. For example—

(1) *Right.* "SUBJECT was married to Martha Smith, NEE: Brown, a U.S. citizen."

(2) *Wrong.* "SUBJECT was married to Martha Smith, NEE: Unknown."

B–10. Coded sources

Coded sources should not be identified as such in a CIR or ACOP ROI entry. Do not refer to CISOCs in the CIR or subsequent ACOP ROI entries. Fully identify the sources with the pertinent information, but keep all references to counterintelligence operations concept, CISOCs, or special projects out of the report. Investigative reports are kept within Army intelligence channels and not released to outside agencies without prior ACICA approval.

B–11. Report caveats

a. Specific caveats are placed on CI investigative reports to ensure that report recipients afford proper protection to those reports and the information contained in them. The most common caveats are Privacy Act caveats. However, information protected by statute and subject to the third-party rule may also be preceded by caveats. Third-party doctrine maintains that people who voluntarily provide information to third parties (such as banks, phone companies, internet service providers, and email servers) have no reasonable expectation of privacy. These caveats are descriptive in nature and reflect the type of information contained in the report.

b. No caveat is needed for SIs, as a Privacy Act advisement is included in the introductory paragraph.

c. Usually, only one caveat pertains to a single report. Exceptions are the LHM and ROI, which require the inclusion of all pertinent caveats.

d. Report caveats are not to be confused with standard protective markings required to protect classified defense information contained within reports (see AR 380–5).

B–12. Abbreviations and short titles

Keep abbreviations to a minimum. Civilian abbreviations, as listed in dictionaries, are authorized. The following include general rules for abbreviations:

a. Spell the word out the first time. Thereafter, use the abbreviation for the remainder of the report. Do not use an abbreviation or short title as part of an official title (for example, "SUBJECT was assigned to Fort Huachuca (FH), Arizona. HE was interviewed at Fort Huachuca Field Office, FH").

b. Do not use periods with abbreviations for rank (for example, CPT or SFC).

c. Use periods with civilian titles. The exception, Miss, does not require a period (for example, Mr., Mrs., or Dr.).

d. Do not abbreviate the names of foreign countries. Use the DIA two-letter country code. The first time a country is mentioned, spell it out in full. Thereafter, use the official country code in the remainder of the report.

e. Spell out the names of states the first time they appear in a report. Subsequently, abbreviate the state name using the two-letter U.S. Postal Service abbreviation in upper case.

f. When referred to alone, the state may be abbreviated.

g. Civilian titles preceding surnames may be abbreviated (for example, Dr. John Casey).

h. Do not abbreviate military ranks standing alone (for example, "Upon graduation from college, SUBJECT was commissioned as a Second Lieutenant in the U.S. Army").

i. Military rank follows the name of the individual and is abbreviated (for example, Alan Thompson, SFC and John Smith, CPT).

j. Abbreviate junior (Jr.) and senior (Sr.) when used as part of a name (for example, Jack Daniels, Sr. and Robert Burns, Jr.).

k. Spell out the month in full and always use the full year (for example, 14 December 1985 and 9 November 1974).

l. Three-letter abbreviations for months may be used in tabulated entries.

m. Construct short titles by taking the first letter of each proper noun in the long title and enclosing them in parenthesis immediately after the long title. Once a short title is established, use it without parentheses as a substitute for the long title for the remainder of the report. Short titles may be used for schools, units, military installations, and multiple-word cities.

n. Omit periods and spaces after initials used as short titles (for example, FBI, CIA, and DIA).

o. Never use short titles for names of people. Do not create short titles if they are not used again in the report.

B–13. Quotes, contractions, hyphen, and commas

Avoid using quotation marks, contractions, and hyphens. Apply the following rules:

a. Do not use quotations marks for common nicknames except when used with the whole name (for example, Dizzy Dean or George Herman "Babe" Ruth).

b. Do not use quotation marks with the names of newspapers and magazines. They should be underlined.

c. Do not use contractions such as isn't, for, is, not, and, didn't, for, did, not, unless contained in a direct quote.

d. Do not use the dash (two or more hyphens) when constructing sentences. Use commas instead.

e. Use the hyphen only in tabulated reports to indicate the omission of words (for example, Height: 5'10"-6'0" and Weight: 150–160 pounds).

f. Use a comma between city and state and after the state when it is not the last word of the sentences (for example, "HE resided in Covington, Kentucky, until 1965").

g. Use a comma to set off absolute phrases (for example, "Jones, the richest man in town, collected stamps").

h. Use a comma to offset long, dependent adverbial clauses coming first in the sentence (for example, "Although my hours have been shortened, I still have too much to do").

i. Use commas to offset dates from the body of the sentence (for example, “In June 1980, SUBJECT enlisted in the U.S. Army”).

B–14. Foreign terms

Underline foreign words and phrases, titles of books, plays, magazine names, and names of ships. When using foreign terms, place the English translation within parentheses following the first usage (for example, “HE worked at the Arbeitsamt (Labor Office). HE read a copy of Pravda (Truth), (the Soviet National newspaper)”).

B–15. Physical descriptions

a. When it is necessary to physically describe individuals, present a complete physical picture of the individual. The information and characteristics for identifying persons lend themselves well to tabulation (see table B–1 for example).

Table B–1
Physical description

Sex:	Male
Skin color:	White
Complexion:	Fair
Age:	37–42
Height:	5’11”-6’1”
Weight:	170–180 pounds
Build/posture:	Medium and stooped
Hair:	Blond
Eyes:	Blue
Dress:	Battle dress uniform
Distinguishing features:	3-inch scar, right cheek

b. The standards for estimates are—

(1) Age, 5-year spread.

(2) Height, 2-inch spread.

(3) Weight, 10-pound spread.

c. Other specific information or physical characteristics may be used or added when available. In addition, if an Identikit was used, the montage codes can be tabulated so that other agencies can reassemble the composite likeness of the subject. All the montages used in the composite must be listed.

B–16. Capitalization guidance

a. Knowing when to capitalize is as important as knowing when not to capitalize. The capitalization of keywords in a sentence or report allows the reviewer to key in on important information. Similarly, the lack of capitalization will keep the reader from being distracted or focusing on unnecessary topics.

b. Capitalize—

(1) The first letter of the first word in every sentence.

(2) The first letter of the word “Source” and the first letter of personal pronouns referring to source.

(3) The first letter of the names of persons (for example, John Adams or Watson family), places (for example, Rome), countries (for example, Italy), races (for example, Caucasian), language (for example, Spanish), months (for example, January), and days of the week (for example, Monday).

(4) All letters of the surnames of the subject (for example, Robert E. WILSON).

(5) All Privacy Act caveats and warning notices.

(6) The word “SUBJECT” when substituted for the surname of the subject.

(7) All security classifications or clearances appearing in the body of the report (for example, HE had a SECRET document).

(8) Personal pronouns when substituted for the surname of the subject (for example, HE was in McDonalds).

(9) Names of all political parties and organizations (for example, the Republicans).

(10) All titles preceding names, if required.
(11) Titles of rank, office, or profession following the name, if given formally and in full.
(12) Names of regions, localities, and geographic features (for example, the West, the Midwest, Far East, or Orient).
(13) Common nouns or adjectives forming a proper name (for example, Colgate Avenue or Hoover Dam).
(14) The plural form of a common noun capitalized as part of a proper name (for example, Seventh and Oak Streets or Potomac and James Rivers).
(15) The names of formally structured organizations and their short titles (for example, FBI).
(16) The terms referring to members and supporters of formally structured organizations to distinguish them from words used merely in a descriptive sense (for example, Communist, Boy Scout, and Democrat).
(17) Seasons of the year when written with a specific year (for example, Winter 1996).
(18) Names of schools (for example, Princeton University).
(19) College degrees (for example, Bachelor of Arts).
c. Do not capitalize—
(1) Names of classes (for example, HE took a math class).
(2) Names of studies except languages (for example, HE majored in sociology).
(3) High school, college, and university when used indefinitely (for example, HE went to high school in 1978).
(4) Seasons of the year when no specific year is written (for example, HE left sometime last spring).
(5) Descriptive terms to denote direction or position (for example, HE was on the north side of the room).

B–17. Numeric guidance

a. In general, numbers from one to ten are spelled out while numbers above 10 are written as numerals.
b. Use numerals in—
(1) Sums of money (for example, $20).
(2) Street numbers (for example, 114 East Street).
(3) Room and apartment numbers.
(4) Scores, degrees or temperature, telephone numbers, automobile licenses, distances, prices, percentages, and dimensions (for example, 10–4; 100 degrees; 301–677–4444; Maryland license number, 123–456–789; 10 miles; $14; 25 percent; or 10 feet by 4 feet).
c. Quantities and measurements are almost always written in figures (for example, 2 gallons or 25 feet).
d. Do not use numerals to begin a sentence, in a fraction that stands alone, or in numbers used as part of a title.

B–18. Military verbiage

a. Use the military style for time. For clarity, follow the time with the word “hours” (for example, 1440 hours).
b. Use the military sequence of day, month, and year for dates (for example, 14 May 1997).
c. Write military units of squads, platoons, companies, battalions, and so forth with abbreviations of ordinal numbers. List unit designations from smallest to the largest element (for example, 1st Squad or 2nd Platoon).
d. Write corps designations in Roman numerals (for example, I Corps).
e. Spell out Armies (for example, Third U.S. Army).

B–19. Identifying subjects

There are two subject identification methods for CI investigative reporting—
a. Single subject.
b. Multiple subjects.

Appendix C

Counterintelligence Investigative Aids

No two investigations are ever the same, but each requires SAs to rely on their experiences and employ best practices to achieve investigative goals. This appendix includes some investigative aids developed to focus investigative activity, employ investigative resources, and manage and analyze collected information.

C–1. Proof sheet

National security crimes and allegations consist of "elements of the crime," which are used to develop investigative activity to collect against. The proof sheet is utilized to identify which elements of a national security crime or allegation the investigation has produced evidence in support of or against, as well as which elements have yet to be addressed. It further helps SAs in identifying the strength of the evidence by identifying the existence or lack of corroborating evidence. Using the proof sheet ensures that an investigation is as complete as possible within the means available to CI. Other evidence may still exist that can only be obtained through joint investigative activity, the use of more intrusive investigative techniques, CI collection operations, or by handing off the investigation to other agencies. Table C–1 provides an example of a blank proof sheet.

Table C–1
Example proof sheet

Allegation/Crime	Evidence	How acquired	Notes

C–2. Searching patterns

Searching for evidence requires attention to detail and a methodical approach. Each search technique has advantages and disadvantages that depend highly on the area to be searched, available personnel, available time, and level of intrusiveness that will be exercised. The following include the most common search patterns:

a. Circle search pattern. The circle search pattern consists of concentric circles expanding from a fixed point. The search can be conducted outward from the fixed point or inward towards the fixed point. This search method is generally employed when searching small areas either indoors or outdoors.

b. Grid search pattern. The grid search pattern requires that the search area be divided into grid squares approximately 4 feet wide. The searcher begins at one end and moves from one grid square to the next until complete. This search method is generally employed when searching large outdoor areas.

c. Zone and sector search pattern. The zone and sector search pattern are two similar approaches to searching large or complex areas. They can be employed when searching large outdoor areas or the interior of multi-room structures.

(1) The zone method requires that the search area be divided into zones. The first zone would be the immediate area of importance (that is, where the subject left the classified documents). Zones 2, 3, 4, and 5 would be the areas adjacent to zone one.

(2) The sector method requires the search area to be separated into sectors, numbering each either one, two, or three, depending on the area of importance. Therefore, the most immediate area of importance (that is, where the subject left the classified documents) would be labeled with the number one. Contiguous areas would be labeled with the number two. Finally, all other areas would be labeled with the number three. The searcher begins at one end and moves from one area to the next until complete.

C–3. Analytical tools

a. SAs and supporting analysts make use of four basic analytical techniques (tools) to visualize large amounts of data in graphic form and enable link analysis of relationships that surface during a CI investigation or when analyzing human intelligence-related problems. These tools are—

(1) Time event chart.
(2) Matrices.
(a) Association matrix.
(b) Activity matrix.
(c) Link analysis diagram.

b. These analytical techniques can be used to present briefings and evidence or to store information concisely and understandably within a database. However, they are only tools used to arrive at a logical and correct solution to a complex problem. The techniques themselves are not the solution and do not replace SOPs, standard reporting procedures, or standard database files (see ATP 2–22.2–1 for a detailed discussion of these analytical techniques).

Glossary

Section I

Abbreviations

ACCN
Army case control number

ACI
Army counterintelligence

ACICA
Army Counterintelligence Coordinating Authority

ACICA–PM
Army Counterintelligence Coordinating Authority-Program Manager

ACIGC
Army Counterintelligence General Counsel

ACOP
Army Counterintelligence Operations Portal

ACRC
Army Crime Records Center

ADP
Army Doctrine Publication

AIPP
Army Intelligence Polygraph Program

AKO
Army Knowledge Online

ANCOC
Advanced Noncommissioned Officers' Course

AO
area of operations

AR
Army regulation

ARC
Airline Reporting Corporation

ATA
Advanced Technology Attachment

ATP
Army Techniques Publication

AUSA
Assistant United States Attorney

BCBE
backup copy/best evidence

BSA
Bank Secrecy Act

CAP
covering agent program

CBP
Customs and Border Protection

CCD
Consular Consolidated Database

CD
compact disc

CFR
Code of Federal Regulations

CG
commanding general

CI
counterintelligence

CIA
Central Intelligence Agency

CID
Criminal Investigation Division

CIR
counterintelligence incident report

CISOC
counterintelligence special operations concept

CLEAR
Consolidated Lead Evaluation and Reporting

CLIP
Contract Linguist Information Program

CPT
captain

CSPE
counterintelligence scope polygraph examination

DA
Department of the Army

DCII
Defense Central Index of Investigations

DCS
deputy chief of staff

DCSA
Defense Counterintelligence and Security Agency

DEE
Department of Defense Enterprise Email

DIA
Defense Intelligence Agency

DISA
Defense Information Systems Agency

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense

DODM
Department of Defense manual

DPOB
date and place of birth

DVD
digital versatile disc

EC
evidence custodian

EO
Executive order

EXSUM
executive summary

FBI
Federal Bureau of Investigation

FF
full-field investigation

FIE
foreign intelligence entity

FinCEN
Financial Crimes Enforcement Network

FISA
Foreign Intelligence Surveillance Act

FM
field manual

FNU
first name unknown

FO
field office

FOIA
Freedom of Information Act

GS
general schedule

HQDA
Headquarters, Department of the Army

ICF
intelligence contingency funds

INSCOM
U.S. Army Intelligence and Security Command

JP
joint publication

JPAS
Joint Personnel Security Adjudication System

JSIP
joint subject interview plan

LAPD
Los Angeles Police Department

LCA
limited counterintelligence assessment

LCCN
local case control number

LECI
Law Enforcement and Counterintelligence

LES
law enforcement sensitive

LHM
letterhead memorandum

LNU
last name unknown

MFID
mark for identification

MFR
memorandum for record

MI
Military Intelligence

MID
Military Intelligence Detachment

MIR
monthly investigative report

MPR
military police report

NAC
national agency check

NCIC
National Crime Information Center

NCR
National Comprehensive Report

NFI
not further identified

NIPRNET
Non-Secure Internet Protocol Router Network

NMN
no middle name

NRO
National Reconnaissance Office

NSA
National Security Agency

OPSEC
operations security

PAO
public affairs office

PI
preliminary investigation

PL
Public Law

PMO
provost marshal office

RFA
request for assistance

ROI
report of investigation

SA
special agent

SAC
special-agent-in-charge

SAP
special access program

SAR
suspicious activity report

SCG
security classification guide

SCI
sensitive compartmented information

SCIF
sensitive compartmented information facility

SF
standard form

SFC
sergeant first class

SI
subject interview

SIA
standing investigative authority

SIP
subject interview plan

SIPRNET
Secret Internet Protocol Router Network

SJA
staff judge advocate

SOP
standing operating procedure

SSN
social security number

SSO
special security office

TARP
Threat Awareness and Reporting Program

UCMJ
Uniform Code of Military Justice

USACIDC
U.S. Army Criminal Investigation Command

USAIRR
U.S. Army Investigative Records Repository

USC
United States Code

USCIS
U.S. Customs and Immigration Service

Section II

Terms
This section contains no entries.