Headquarters
Department of the Army
Washington, DC
19 April 2023

*Army Regulation 381–45

Effective 19 May 2023

Military Intelligence

U.S. Army Intelligence and Security Records Repository

By Order of the Secretary of the Army:

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

Official:

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

History. This publication is a major revision.

Authorities. The authority for this regulation is DoDM 5240.01.

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

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

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

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-dcs-g-2.mbx.dami-cd@mail.mil.

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.

*This regulation supersedes AR 381-45, dated 31 May 2013.

Contents (Listed by chapter and page number)

Chapter 1
Introduction

1–1. Purpose
The U.S. Army Intelligence and Security Records Repository (USAISRR) is a Department of the Army (DA) records center serving as the repository for intelligence, counterintelligence (CI), human intelligence (HUMINT), personnel security, questionable intelligence activity reports, and other records that meet the criteria of this regulation. This regulation establishes policy, assigns responsibilities, and establishes requirements for the operation of the USAISRR; identifies the categories of material authorized for custody in the USAISRR; provides policy and procedures for the storage, maintenance, transmission, review, and reduction of these records; establishes a requirement for digitization and automation of databases and records; and specifies procedures for the Department of Defense (DoD) and other organizations requesting access to USAISRR holdings.

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

1–3. Associated publications
Policies associated with this regulation are found in AR 25−400−2, AR 380−67, AR 381−10, AR 381−20, and AR 381−100.

1–4. Responsibilities
a. The Deputy Chief of Staff (DCS), G–2 will—

(1) Develop and publish policy on the establishment and operation of the USAISRR and designate the types of files that must be archived there.

(2) Exercise Army staff responsibility for oversight and accountability of the USAISRR.

(3) Serve as the approving official for requests to archive materials not specified in this regulation.

(4) Serve as the initial denial authority/denial authority, unless otherwise delegated, for all Freedom of Information Act (FOIA) and Privacy Act requests for intelligence and security records in accordance with AR 25–22.

b. The Commander, U.S. Army Intelligence and Security Command (INSCOM) will—

(1) Coordinate with the DCS, G–2 to develop implementing guidance on the operation of the USAISRR.

(2) Provide funding, legal, and resource support to maintain USAISRR operations.

(3) Conduct intelligence oversight inspections to ensure USAISRR follows proper retention and dissemination policies.

(4) Develop and maintain information technology solutions for the transmittal to the repository of digital records that are processed on automated systems, such as the Army Counterintelligence Operations Portal, the DoD Portico Operations Module, and the DoD Source Operations Management Module.

(5) Oversee the process of setting up agreements with other Government agencies for access to and use of USAISRR materials.

(6) Provide dedicated information technology and assurance support for the Intelligence Records Information System.

(7) Ensure that the Army Counterintelligence Coordinating Authority (ACICA) and the Army Human Intelligence Operations Center (AHOC) properly retire records to the USAISRR in accordance with AR 381–20, AR 381–47, and AR 381–100.

(8) Ensure that Army service component commands (ASCCs) retire records of HUMINT operations conducted under the authority of combatant commands in accordance with AR 381–100.

(9) Serve as the initial denial authority/denial authority, unless otherwise delegated, for all FOIA and Privacy Act requests for intelligence and security records in accordance with AR 25–55.

c. The Director, USAISRR will—

(1) Maintain the effective and efficient operation of the USAISRR.

(2) Under the direction and guidance of the DCS, G–2 and Commander, INSCOM, manage the USAISRR in compliance with applicable laws, DoD policy, and Army policy.

(3) Prioritize the necessary resources and other support to maintain USAISRR operations.

(4) Serve as the initial denial authority as delegated by the DCS, G–2 for all Privacy Act requests for intelligence and security records in accordance with AR 25–22.

(5) Authorize control of records containing material warranting restricted access.

(6) Assign a record category for all records requiring restricted access (see para 2–6).

(7) Serve as the approving authority for requests for access to restricted records.

(8) Develop security procedures as per paragraph 2–5b.

(9) Convene a quarterly review board as per paragraph 2–7c.

(10) Review and make recommendations on requests to amend records as per paragraph 3–5b.

d. The Chief, USAISRR will—

(1) Be responsible for the daily operation of the USAISRR and ensure the timely response to requests for access to intelligence materials and records from authorized users.

(2) Maintain a continuing review program to identify, transfer, and reduce materials and files no longer required or authorized for retention.

(3) Ensure that information contained in records pertaining to U.S. persons is maintained in accordance with DoDM 5240.01, AR 381–10, and AR 25–22.

(4) Ensure appropriate security for and control access to restricted records.

(5) Provide direction and control for the preparation of affidavits and supporting documents required by the General Counsel.

(6) Receive accession records into the repository and ensure that supplemental materials are posted promptly and accurately to appropriate files.

(7) Create and maintain entries in the Defense Central Index of Investigations (DCII).

(8) Maintain disclosure records in accordance with AR 25–22.

(9) Coordinate with other organizations to facilitate the processing of files and information.

(10) Coordinate with liaison officers of non-DoD organizations accredited for access to records.

(11) Fulfill additional responsibilities as listed throughout paragraph 2–3.

(12) Review requests to amend records as per paragraph 3–5b.

1–5. Records management (recordkeeping) requirements

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

Chapter 2
Accession, Retention, Transmission, Storage, and Reduction

2–1. Accession policy

Organizations creating the following types of records are required to archive them in the USAISRR in accordance with this regulation and the applicable System of Records Notice (SORN) (see table 2–1 for SORNs that are applicable to the types or records for which the USAISRR is responsible). Upon retirement of records to the USAISRR, the USAISRR will determine their disposition and retention. Records that are authorized for indexing into DCII are assigned a locator number and DCII code. The DCII codes identified in table 2–2 will be affixed at the end of the locator number to identify the record type. The retention codes identified in table 2–2 identify the threshold for which records will be retained in the USAISRR in accordance with AR 25–400–2. The USAISRR maintains the following categories of records:

a. CI investigative records. Records relating to CI investigations of persons, events, and organizations conducted by Army CI organizations (INSCOM, U.S. Army Counterintelligence Command (USACIC) and the 650th Military Intelligence Group) and other DoD, Federal, state, and local organizations. The 650th Military Intelligence Group will archive records pertaining to CI investigations of U.S. persons.

b. Restricted access CI investigative files. CI investigations that are categorized as restricted or that contain Special Access Program (SAP) material.

c. CI source files. Records obtained by or through Army organizations and other agencies in the conduct of CI source operations by or with the Army, including plans, proposals, reports, polygraph reports, and asset or source dossiers regarding CI operations, defensive source operations, investigative source operations, and CI projects. These records include details on the use or activities of sources or assets that are necessary to confirm potential future claims against the Army by them or their heirs or to authenticate that a person was an asset or source.

d. Offensive CI operations records (see para 2–1c) and asset dossiers.

e. HUMINT source records. Dossiers on sources and assets recruited for HUMINT activities. This category includes operational reports and reports containing data about personnel who have been used as sources or assets in HUMINT activities.

f. Substantiated reports of questionable intelligence activity. Reports of questionable intelligence activity rendered in accordance with AR 381–10, including investigations conducted by INSCOM and other Army commands. Substantiated reports are those in which an assessment has been made that a questionable intelligence activity was not legal or was not consistent with applicable policies.

g. Inspector General (IG) reports. Extracts or summaries of reports of IG investigations when they relate to a CI activity or a report of questionable intelligence activity. The official directing the IG investigation will determine what information is to be included in the extract or summary. The record will not include the basic IG report of investigation. Requests for release of any portion of an IG report, including extracts or summaries, will be processed in accordance with AR 20–1 (see para 3-4e).

h. CI incident reports. Initial reports regarding matters of CI interest that have not resulted in the initiation of a CI investigation.

i. Electronic surveillance records. Records relating to electronic surveillance or concealed monitoring conducted under the provisions of DoDM 5240.01 or AR 381–10 by or on behalf of the Army as part of a lawful CI investigation, including audio, video, and network records.

j. Polygraph and credibility assessment files. Information on the results of polygraph examinations and Preliminary Credibility Assessment Screening System, including examination reports, briefing acknowledgments, consent forms, and examiner conclusions will be stored in a subject's record under separate cover from other material that may be contained there in accordance with AR 381–20.

k. Screening records. Records pertaining to the CI and security screening of contract linguists, interpreters, translators, local hires, contract role players, Military Accessions Vital to the National Interest, and non-U.S. citizen enlistees, including the results of intelligence agency checks, the results of CI screening interviews, and the results of any CI investigation and polygraph examination.

l. U.S. prisoners of war. Those missing in action and detainees. Documents relating to and containing information about DoD personnel who have been held as prisoners of war; designated as missing in action; who have been held hostage by terrorist, insurgent, or other foreign entities; and personnel who have been recovered from hostile control and debriefed for intelligence or CI purposes.

m. Military Intelligence Excepted Career Program records. Records of persons managed by the Military Intelligence Excepted Career Program and those in CI or HUMINT special duty status. This includes applicants and spouses, probationary and tenure reports, and evaluation reports.

n. Personnel security clearance files. Individual case files related to Army military members and civilian employees, retired personnel, members of the Reserve Components, applicants for commission and enlistment, DoD civilian personnel and applicants for such status, persons having need for access to official information requiring protection in the interests of national security under the DoD industrial security program, and persons being considered for participation in other DoD programs. Files may include DA Form 5248–R (Report of Unfavorable Information for Security Determination) with any attachments, correspondence relating to notification of denial or revocation of security clearances or access to sensitive compartmented information (SCI); limited access authorizations, and reports submitted under the provisions of AR 380–67. Files in this category created after 1 January 2013 will not be retained by the USAISRR. Files created prior to this date will remain in the USAISRR under their prescribed retention criteria.

o. SCI nondisclosure agreements. Copies of IC Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement) or similar forms signed by military and civilian personnel, employees of contractors, licensees, and grantees with access to information that is classified as defined by Executive Order (EO) 13526.

p. HUMINT and CI collection records. Records describing requirements, objectives, approvals, implementation, reports, and results of CI and HUMINT collection activities.

q. Other intelligence files as approved by the DCS, G–2.

Table 2–1
System of Record Notices applicable to intelligence and security records

System of Records Notice number	System Name/descriptor
A0380–67 DAMI	Personnel Security Clearance Information Files
A0381-20b DAMI	Foreign Intelligence/Counterintelligence/Information Operations/Security Files
A0381-100a DAMI	Intelligence/Counterintelligence Source Files
A0381-100b DAMI	Technical Surveillance Index
A0614–115	Department on the Army Operational Support Activities

Table 2–2
Disposition and retention standards

Record type	Defense Central Index of Investigations Index code	Army Records Information Management System retention code Table 7–1, AR 25–400–2	Notes
CI investigative records	W	T25	
Restricted access CI investigative records			
CI source records (defensive and investigative)	NA	T75	
Offensive CI operations records	NA	TE	Final retention code determined based on instructions from offensive CI organization
HUMINT collection and source records	NA	T75	
Substantiated questionable intelligence activity reports	Q1	T15 T25	Extended disposition if derogatory information is included (see glossary for definition)
CI incident reports not resulting in a CI investigation	NA	T15 T25	Extended disposition if information of CI value is identified
Inspector General (IG) Records	NA	TP	Intelligence and security related records contained within an IG file, will remain under the control and release authority of this regulation.
Electronic surveillance records	NA	T25	
Polygraph and credibility assessment records	E2	T35	
Polygraph examinations of CI and HUMINT sources and assets	E	T50	
CI and security screening of Military Accessions Vital to the National Interest, contract linguists, 09L, non-U.S. citizen enlistees, and persons having access to official information requiring protection in the interest of national defense under the DoD industrial security program, and persons being considered for participation in other DoD programs.	MV TC SV	T15 T25	Extended disposition if derogatory information or information of CI value is identified
U.S. prisoner of war, missing in action, and detainee intelligence reports	NA	T50	
Personnel security clearance records	C	T15 T25	Extended disposition if derogatory information is identified

Table 2–2
Disposition and retention standards—Continued

Military Intelligence Excepted Career Program records	NA	TE15	Event is after release, separation, transfer, retirement, or resignation.
SCI nondisclosure agreements	NA	T70	
HUMINT and CI collection records	NA	T25	
Operational support records	NA	T15	15 years after last action noted in record

2–2. Records not authorized for accession

a. The following types of materials will not be accessed into the USAISRR:

(1) Personal or impersonal files on non-DoD affiliated U.S. persons who are not or who have not been the subject or source in a CI investigation, who have not been a source or asset in CI or HUMINT operations, or who have not been the subject or a source in a personnel security investigation. DoDM 5240.01 and AR 381–10 have policy related to the collection and retention of information on U.S. persons by intelligence organizations. Any questions regarding retention should be reviewed by a legal advisor.

(2) Files containing only materials originating from a non-DA agency.

(3) Impersonal files containing no derogatory information with the most recent information being more than 1 year old.

(4) Files on U.S.-held enemy prisoners of war and detainees, except detailed debriefing statements that are deemed of intelligence value.

(5) Files on enemy-held U.S. prisoners of war and detainees, except detailed debriefing statements that are deemed of intelligence value.

(6) Records of courts-martial and nonjudicial punishment administered under Article 15, Uniform Code of Military Justice, except as submitted by the DoD Consolidated Adjudications Facility as part of a personnel security adjudications file.

(7) Non-SCI nondisclosure agreements, to include those related to sensitive activities and SAP.

b. Materials identified in this paragraph may be included in USAISRR files if those materials are exhibits or enclosures to an investigative report concerning a subject defined in paragraph 2–1. These materials will not be cross-referenced or otherwise identified in the DCII.

2–3. Accession criteria and procedures

a. Material accessed into the USAISRR, either initial or supplemental, will contain only one copy of each document having retention value or containing information concerning persons of HUMINT, CI, or security interest. Commanders will submit files in an approved digital format or other digital formats as directed or required. Hardcopy files will be submitted only by exception (see para 2–4).

b. Commanders submitting records for accession will use DA Form 7808 (U.S. Army Intelligence and Security Records Repository Data Reference Form) to document the transfer of records.

c. All materials submitted for accession will be evaluated under the criteria of this regulation and must meet the retention requirements of DoDM 5240.01 and AR 381–10; submitters will certify that the retention requirements have been met.

d. The Chief, USAISRR will accept initial or supplemental material only from the following sources:

(1) The ASCCs, the Army theater counterintelligence coordinating authorities (ATCICAs), INSCOM, USACIC (including the ACICA and AHOC), the 650th Military Intelligence Group, and other Army organizations that conduct or support intelligence, HUMINT, or CI activities.

(2) Army organizations that create personnel records associated with special intelligence and CI activities.

(3) Army Intelligence Polygraph Quality Control Office.

(4) Army organizations responsible for the processing of IC Form 4414 or similar forms.

(5) DoD Consolidated Adjudications Facility.

(6) Army organizations responsible for conducting CI and security screening.

(7) Office of The Inspector General.

e. The Chief, USAISRR will accept material related to only the following categories of persons:

(1) Persons affiliated with DoD.

(2) Persons, organizations, and incidents of CI, HUMINT, or security interest to the Army.

(3) Information concerning U.S. persons that is authorized for collection and retention in accordance with the provisions of DoDM 5240.01 and AR 381–10.

(4) Foreign nationals or foreign organizations that were the subjects of investigations or who have been identified in intelligence reports.

(5) Materials requiring restricted custody, as defined in paragraph 2–6, or for which a restricted record already exists.

f. Initial and supplemental material submitted for accession will not contain extraneous copies of investigative reports or correspondence, administrative reports regarding personnel or logistical management, rough draft notes, or documents for which another Army organization is the primary office of record, unless such material pertains directly to a CI or personnel security investigation or to a security or suitability adjudication.

g. Acceptable material relating to a subject on which there is no existing file will be accessed into the USAISRR as a new record with proper security classification, assigned an identifying number, and entered into the DCII.

h. Except for nondisclosure agreements, new material will be updated in DCII in accordance with table 2–2.

i. The Chief, USAISRR will purge extraneous material according to criteria in paragraph 2–8.

j. The Chief, USAISRR will cross-reference records only when doing so would serve legitimate intelligence, CI, or security interests. It will not cross-reference records when doing so would cause a person or organization that is otherwise of no legitimate interest to appear in the DCII as the subject of a record.

k. The Chief, USAISRR will not normally release to requestors exhibits that are not required for routine investigations or adjudication.

l. The Chief, USAISRR will return to the originating organization initial or supplemental material that is inappropriate for accession.

m. The Chief, USAISRR may reject material submitted for accession based on the following criteria:

(1) Failure to include a completed copy of DA Form 7808.

(2) Records that are not complete or that have improper classification markings.

(3) The material does not meet the scope of this regulation or is not retainable as specified in DoDM 5240.01 or AR 381–10.

(4) Electronically submitted material does not meet the standards specified by National Archives and Records Administration (NARA).

2–4. Processing records requests

a. The Chief, USAISRR will expeditiously respond to requests from organizations to which this regulation applies and for which accreditation has been established. Circumstances may require the prioritizing of specific requests ahead of others. Expedited processing will be accomplished only by exception in order to minimize delays and disruption of routine operations. Expedited processing requires approval of the Director, USAISRR. In the absence of expedited processing, the following order of precedence will be followed in processing requests for USAISRR files:

(1) Statutory actions, such as FOIA and Privacy Act requests.

(2) Litigation in which the Army is a party.

(3) CI investigations.

(4) Criminal investigations.

(5) Personnel security and security clearance actions.

(6) All others.

b. The Chief, USAISRR may respond to requests with an extract from the record or a summary of the information in a record.

c. The Chief, USAISRR ordinarily authorizes reviews of entire records only by the DCS, G–2 and the Commander, INSCOM. The Director, USAISRR may approve exceptions based on a compelling need.

d. The Chief, USAISRR will provide to accredited requesters, the following types of responses: a favorable response, a reproduced extract of unfavorable or derogatory information, a summary of the information in a record, or a response that there is no record in the USAISRR. The Chief, USAISRR will not provide an evaluation of unfavorable, questionable, or derogatory information for purposes other than file retention, reduction, or elimination (see para 2–8).

e. The Chief, USAISRR will not provide third-agency materials to non-DoD organizations. The Chief, USAISRR will advise the requester that the material is on file and provide the identity of the agency that may authorize its release.

f. The Chief, USAISRR will not release financial records acquired on or after 10 March 1979 outside of DoD unless the requester certifies the relevance of such records in writing in accordance with applicable ARs. A copy of the requestor's justification and a record of the release or denial will be permanently filed in the record. Financial information acquired before 10 March 1979 may be released outside DoD according to existing records release procedures for other types of records.

g. The release of medical record information is governed by AR 25–22, AR 40–66, and AR 600–85, as applicable. The written consent of the subject is required and will be made part of the file before release. Signed releases will be forwarded to the U.S. Army Intelligence and Security Records Repository, 2600 Ernie Pyle Street, Fort George G. Meade, MD 20755–5910.

h. Exhibits that are not required for routine investigations or adjudication normally will not be released to requestors.

i. FOIA requests for SAP material or material marked "handle via special access channels only" require review and approval for release by the SAP Central Office.

2–5. File storage and security

a. The information contained in USAISRR holdings, including in some cases the very existence of a file, constitutes a major trust placed in the Army by the original source of the information. Any unauthorized disclosure may constitute a potentially significant liability. In addition, DoDI 5400.11 mandates the implementation of access controls and physical security safeguards for records containing personally identifiable information. These considerations are important factors when assigning personnel to the USAISRR and allowing access in the facility.

b. The volume of material stored in the USAISRR and the nature of its mission require extraordinary measures to safeguard these materials while not encumbering the ability to perform the mission. The USAISRR facility will be maintained as a limited access area in its entirety. The Director, USAISRR will develop detailed security procedures that will be approved by Commander, INSCOM. These procedures will be rigorously enforced.

c. Investigative files in the USAISRR will be stored in a way that meets the following objectives:

(1) Efficient retrieval from and return to storage.

(2) Primary identification and storage by code number rather than subject name.

d. Records will be transmitted by any of the methods authorized for the classification of the materials as specified in AR 380–5.

e. The Commander, INSCOM will coordinate SAP access requirements and indoctrination for select USAISRR personnel with the Army SAP Central Office, which is Army Special Programs Directorate. The Commander, INSCOM will coordinate briefings for those requiring access to alternative compensatory control measures (ACCMs) with the owner of the ACCM unless the owner has granted Commander, INSCOM the authority to approve access.

2–6. Restricted records

Especially sensitive files will be maintained in the USAISRR in a controlled access area physically separate from the main body of USAISRR materials to which only authorized personnel will be allowed access. Electronic files will be maintained in databases that only authorized personnel may view, retrieve, and distribute. The Director, USAISRR will apply physical security measures for the controlled access area and electronic files that meet the requirements for physical security of the highest level of classified material in storage. The USAISRR maintains the following two categories of restricted records:

a. Category 1 are restricted records for which the USAISRR does not have direct release authority. The originating agency will identify these records on DA Form 7808 when the record is retired. Except for SAP records, DCS, G–2; Commander, INSCOM; Commander, USACIC; Director, ACICA; or Director, AHOC must authorize release. FOIA requests for SAP material or material marked "handle via special access channels only" require review and approval for release by the SAP Central Office. Category 1 records include—

(1) HUMINT and CI sources and assets, including developmental, active, and retired assets.

(2) Material that might reflect unfavorably upon foreign governments.

(3) Electronic surveillance records. This material will be segregated from the primary record and access will be controlled and recorded. A cross-reference sheet will be placed in the record when these records are stored in another location.

(4) Reports of IG investigations, extracts, or summaries when they relate to a CI investigation.

(5) All top secret, SCI, SAP, ACCM, and restricted data files.

(6) Sensitive CI investigations.

b. Category 2 restricted records are those that are placed into an access controlled area because of the position, appointment, or duty of the persons to whom they refer. These records may be released to an authorized requester by the USAISRR control custodian. They include—

(1) USAISRR personnel and select individuals within Headquarters, INSCOM and USACIC.

(2) Persons in organizations who are authorized to request records from the USAISRR or who have review or adjudicative functions for personnel or industrial security.

(3) All general and flag officers on active duty for up to 1 year after retirement, general officer selectees, and Secretaries of the Army and Defense.

(4) Any person not otherwise specified in this paragraph who by virtue of their assignment might gain access to their own record.

(5) Persons listed as relatives in biographical listings (for example, personnel security questionnaires) of persons listed in paragraphs 2–6b(1) through 2–6b(4).

c. The Chief, Special Records Division, USAISRR will process, safeguard, account for, and maintain custody of restricted records. They will also ensure the records of military officers selected for or promoted to general officer or equivalent are stored as restricted records.

2–7. Record review

a. Each record, electronic document, or film on file in the USAISRR will undergo a retention and security classification review each time it is retrieved from storage. Electronic files will be set for automated reviews and deletion upon expiration, unless otherwise marked for archiving in NARA.

(1) Nonretainable files will be eliminated in accordance with paragraph 2–8.

(2) Retainable files will be purged of extraneous and duplicate material and consolidated in digital files.

b. The control custodian will ensure that all controlled records are reviewed while in and upon leaving controlled status.

c. Director, USAISRR will convene a quarterly review board consisting of representatives from the ACICA, the AHOC, and other organizations directed by Commander, INSCOM. The review board will identify files that are in final disposition status and recommend either retention, destruction, or archiving. The board may meet electronically and will make final determinations by the 20th day of the month following the end of each quarter. If there is no recommendation from participating agencies, the board may make disposition determinations.

2–8. Record reduction and elimination

Every effort consistent with intelligence and security requirements will be made to reduce the number of USAISRR records. Those objectives will be accomplished by—

a. Elimination of duplication in records that are retained.

b. Elimination of information that is not complete, accurate, relevant, or timely in accordance with AR 25–22.

c. Elimination of nonretainable records.

(1) Retention criteria are established by this regulation, DoDM 5240.01, and AR 381–10.

(2) Disposition instructions in AR 25–400–2 apply.

d. File elimination will be accomplished under the provisions of AR 25–400–2.

(1) Older files of potential historical value will be offered to NARA under procedures established by AR 25–400–2.

(2) HUMINT and CI source and asset records will not be transferred without written approval of Commander, INSCOM.

(3) Older files of no interest to NARA will be destroyed in accordance with AR 380–5 and AR 25–400–2.

(4) The Chief, USAISRR will delete entries in DCII or in the USAISRR electronic records management system on transferred or destroyed records.

e. Digitization of all records, except for certain restricted records. Upon successful accession and digitization into the USAISRR electronic records management system, paper documents will be destroyed in accordance with AR 25–400–2 and AR 380–5.

Chapter 3
Access to Records

3–1. Dissemination of information about U.S. persons

a. The release of information concerning U.S. persons is governed by AR 25–22, DoDM 5240.01, and AR 381–10.

b. The following are authorized purposes for requesting access to USAISRR records containing U.S. person personally identifying information:

(1) FOIA and Privacy Act requests.

(2) Use in current criminal, personnel security, and CI investigations and adjudication.

(3) To provide information pertinent to persons authorized protection by the U.S. Secret Service (see Section 3056, Title 18, United States Code (18 USC 3056)).

(4) To provide information for judicial or adjudicative proceedings, including litigation, or in accordance with a court order or inquiry from the Congress of the United States.

(5) To confirm the investigation or clearance of an individual.

(6) For use in a duly authorized CI or HUMINT operation.

(7) Government Accountability Office requests.

(8) To determine whether a record has sufficient historical value to justify its continued preservation by the Government.

3–2. File procurement accounts

a. All agencies requiring access to USAISRR materials will establish a file procurement account (FPA) according to the requirements in this paragraph. Each account will be assigned an identifying number by the USAISRR and be serviced through accredited field procurement officer (FPO). Each FPA will have a point of contact, which may be an FPO. Users will provide the telephone number and email address of FPOs to USAISRR.

(1) Organizations requiring infrequent access will use the account of a central office or higher headquarters to meet their needs.

(2) Procurement accounts will not be established below a division level or equivalent.

(3) The Director, USAISRR may grant an exception under extraordinary circumstances.

b. Correspondence relating to FPAs, including requests to establish an account, will be addressed as specified in paragraph 3–3a.

c. Concurrent with a request to establish an FPA, correspondents will nominate between one and six persons as FPOs. FPOs are the sole points of contact between their agency and the USAISRR for requesting, receiving, controlling, and accounting for USAISRR files.

d. FPO nominees must possess at least a secret security clearance, as verified by Defense Information Security System, and be permanently assigned to the requesting organization.

e. FPOs will be thoroughly familiar with statutory and regulatory policy on the dissemination of CI information to unauthorized recipients. FPOs will be knowledgeable of 18 USC 793, 18 USC 794, EO 10450, AR 380–5, DoDM 5240.01, and AR 381–10.

f. Disclosing contents, sources of information, or the existence of a record to persons not officially entitled to such information may be accomplished only when authorized by the Director, USAISRR.

g. Material will not be added or removed from any record, the contents will not be altered, amended, or rearranged, and records will be accessed only in the course of official duties.

h. Agencies will appoint FPOs via memorandum with the person’s full name, date and place of birth, and clearance.

i. A certificate of understanding (see fig 3–1) will be signed by each nominee and forwarded with agency FPO nominations to the USAISRR.

j. Organizations with FPAs will submit a list of their accredited FPOs to the USAISRR each January. The following April, the USAISRR will terminate accounts of any agency from which it does not receive a list. The USAISRR will terminate accounts in which no record requests have been made during any given fiscal year. Agencies will report changes in FPOs as they occur to ensure continuity of access.

Correspondence relating to existing accounts will include the USAISRR assigned account numbers and be addressed as in paragraph 3–3a.

k. ASCCs, ATCICAs, USACIC, and INSCOM organizations performing CI and HUMINT missions will have managed, role-based access to USAISRR records.

l. Upon approval, USAISRR will provide access to these agencies and their authorized representatives to electronic copies of USAISRR records. The files may be accessed through CI investigative or HUMINT management systems and will not be further disseminated by requestors.

m. USAISRR will not provide information in restricted records to requestors. A search for these records will result in notification that a record is available and that access is restricted. Requestors will request the file from INSCOM or the appropriate ASCC or ATCICA.

DEPARTMENT OF THE ARMY
ORGANIZATION
STREET ADDRESS
CITY STATE ZIP

[Office Symbol] [Date]

MEMORANDUM FOR

SUBJECT: Certificate of Understanding

1. I understand that, as an accredited representative of the US Army Intelligence and Security Records Repository (USAISRR), I will be granted access to Army counterintelligence and security investigative records.

2. I understand that, in the performance of my official duties, I may copy, quote, summarize, or otherwise disseminate only within my agency, information obtained from the records maintained by the USAISRR. I will not circulate counterintelligence or security investigative records outside of my agency without prior consent of the USAISRR.

3. I am responsible for ensuring that files are appropriately safeguarded from unauthorized disclosure and destroyed following completion of the purpose for which they were requested. They will be destroyed in any manner authorized for the destruction of Secret defense information as specified in DOD Manual 5200.01, DOD Information Security Program. If they are marked at a level above Secret, they will be destroyed in the manner required for that level of classification as specified by DOD Manual 5200.01.

4. I will not alter, amend, or rearrange material contained in an USAISRR file, nor may I add or remove material.

5. I have read, understand, and will comply with the restrictions concerning the dissemination of classified defense and Privacy Act information as set forth in DOD Manual 5200.01; DOD Directive 5400.11, DOD Privacy Program; and DOD Manual 5400.07, DOD Freedom of Information Act Program.

Signature
Typed Signature
Block (to include Agency Address

Figure 3–1. Certificate of understanding

3–3. File request procedures

a. Requests for USAISRR records in connection with intelligence, CI, security, adjudication, or litigation matters will be forwarded through the accredited FPO to the U.S. Army Intelligence and Security Records Repository, 2600 Ernie Pyle Street, Fort George G. Meade, MD 20755–5910.

b. Non-DoD agencies will provide the appropriate DCII accounting code in table 3–1 with requests for records. These accounting codes are used by USAISRR to account for disclosures to non-DoD agencies as required in AR 25–22.

Table 3–1
Defense Central Index of Investigations accounting codes for disclosure of records outside of the Department of Defense

Code 01
Purpose: For use in current criminal law enforcement investigations, including statutory violations, CI, counterespionage, and other security matters.
Code 02
Purpose: To provide information for ongoing security and suitability investigations being conducted by non-DoD agencies for assignment of individuals to sensitive positions or for access.
Code 03
Purpose: To provide information pertinent to protection of persons under the provisions of 18 USC 3056.
Code 04
Purpose: To provide information in judicial or adjudicative proceedings, including litigation, or in accordance with a court or congressional inquiry.
Code 05
Purpose: To respond to the Freedom of Information/Privacy Act access request.
Code 06
Purpose: To non-DoD agencies conducting pre-employment inquiries and security or suitability investigations other than those listed above.
Code 07
Purpose: To provide information relative to the presence of aliens in the U.S. under the provisions of 8 USC Chapters 12 and 13.
Code 08
Purpose: To agencies and activities not described above in response to a request accompanied by a release.
Code 09
Purpose: To Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee, any joint committee of Congress or subcommittee of any such joint committee.
Code 10
Purpose: To make statistical evaluations of investigative activities.
Code 11
Purpose: To agencies and activities when identifying information must be provided to obtain information.
Code 12
Purpose: To Federal agencies to confirm the investigation or clearance of individuals.
Code 13

Table 3–1
Defense Central Index of Investigations accounting codes for disclosure of records outside of the Department of Defense—Continued

Purpose: To the comptroller general, or any authorized representative, in the course of the performance of the duties of the Government Accountability Office.
Code 14
Purpose: To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual.
Code 15
Purpose: To NARA as a record that has sufficient historical or other value to warrant its continued preservation by the Government, or for evaluation by the NARA to determine whether or not the record has such value.
Code 16
Purpose: To make access or clearance determination when significant derogatory information has developed since the last date of the last clearance.
Code 17
Purpose: To make access or clearance determination when the individual is considered for a higher level clearance or access.
Code 18
Purpose: To make access or clearance determination when there has been a break in the individual's service of more than 2 years.
Code 19
Purpose: To make access or clearance determination if the existence of a valid DoD clearance cannot be verified.
Code 20
Purpose: To make determinations of the eligibility and suitability for entry into and retention in the armed forces.
Code 21
Purpose: Response to congressional, IG, Equal Employment Opportunity, or other complaints.
Code 22
Purpose: To provide information to DoD for ongoing security and suitability.

3–4. Accountability

a. Each FPO is responsible for safeguarding USAISRR information in accordance with the certificate of understanding in figure 3–1.

b. Records will be safeguarded and handled in accordance with their classification. Only persons with the proper security clearance and a legitimate need to know will be permitted access to USAISRR records. In no case will the subject of a record be allowed access to their own file.

c. Loss of classified USAISRR records, unauthorized access to personally identifiable information, or the unauthorized disclosure of the contents of a record constitutes a compromise of restricted and classified information. The accountable FPO will immediately notify the Chief, USAISRR. The Chief, USAISRR will notify Director, USAISRR, who will inform the appropriate security office and the Records Management and Declassification Agency for compromised personally identifiable information.

d. Users are authorized to copy and extract material from records only to meet investigative, adjudicative, administrative, courts-martial, board actions, and assignment requirements. Commanders of Army commands, ASCCs, and direct reporting units and commanders of their major subordinate elements are authorized to release information from CI investigative reports to duly constituted administrative and courts-martial boards that are convened relative to matters identified in the reports. The identity of confidential sources, active and terminated CI and HUMINT sources and assets, or other agencies providing information will not be disclosed without the prior written consent of the Commander, INSCOM or Commander, USACIC.

e. Copying, extracting, reproducing, or releasing information from IG reports is subject to the provisions of AR 20–1. Ordinarily, IG materials constituting a portion of a record will not be provided in response to requests. Requests for IG reports must be approved by the appropriate IG office in accordance with AR 20–1.

f. Financial records will be disseminated to non-DoD agencies only in accordance with paragraph 2–4f.

g. Medical records will be disseminated to non-DoD agencies only in accordance with paragraph 2–4g.

h. The Chief, USAISRR will not provide third-agency material to a non-DoD organization. The Chief, USAISRR will mark copies or extracts for release to non-DoD agencies as follows: "This is a copy (extract) of an investigative or security record on file at the USAISRR, Fort George G. Meade, MD 20755–5995. It will not be provided to another agency and will be destroyed upon completion of the purpose for which it was requested."

i. FPOs are responsible for ensuring that materials are appropriately safeguarded from unauthorized disclosure and destroyed following completion of the purpose for which they were requested.

j. Except as provided in paragraph 3–4d, only the Chief, USAISRR may modify the contents of a record by adding or removing material. Supplemental materials will be submitted in accordance with paragraph 3–5.

3–5. Amendment of records

a. Policy. An amendment of CI investigative and security records is appropriate when such records are established as being inaccurate, irrelevant, untimely, or incomplete. Amendment procedures are not intended to permit challenging an event that actually occurred. Requests to amend reports will be granted only if the individual submits new, relevant, and material facts that are determined to warrant their inclusion in or revision of content in the record. The burden of proof is on the individual to substantiate the request. Requests to delete a person's name from the title block will be granted only if it is determined that there is not probable cause to believe that the individual committed the offense for which they are listed as a subject. It is important to note that the original decision to list a person's name in the title block of a CI investigative or security record is an investigative determination that is independent of whether or not subsequent judicial, nonjudicial, or administrative action is taken against the individual. In compliance with DoD policy, the person's name will remain entered in the DCII to track all reports of investigation.

b. Procedure.

(1) The Chief, USAISRR will review amendment requests. Upon receipt of a request for an amendment of a CI investigative or security record 5 or fewer years old, the chief will gather all relevant available records on file at the USAISRR. They will coordinate a review with the Army agency that generated the report and forward a recommendation to either approve or deny, along with the rationale for denial, to the Director, USAISRR. The director will conduct a secondary review and provide a final recommendation for approval or justification for denial to the DCS, G–2 for a final determination. If DCS, G–2 decides that a report should be amended, the director will task the originating agency to prepare an amended supplemental report. The originating agency will return the supplemental report to Chief, USAISRR with the amendment request as an enclosure. The chief will ensure that both the supplemental record and the original record are archived with a copy furnished back the requestor.

(2) The USAISRR will follow the same process for requests for amendments for CI investigative and security related records that are older than 5 years. In these cases, the Director, USAISRR will serve as the final approval or denial authority.

Appendix A

References

Section I

Required Publications
Unless otherwise indicated, all Army publications are available on the Army Publishing Directorate website at https://armypubs.army.mil. DoD publications are available on the Executive Services Directorate website at https://www.esd.whs.mil.

AR 25–22
The Army Privacy and Civil Liberties Program (Cited in para 1–4a(4).)

AR 25–55
The Department of the Army Freedom of Information Act Program (Cited in para 1–4b(9).)

AR 25–400–2
Army Records Management Program (Cited in para 1–3.)

AR 380–5
Army Information Security Program (Cited in para 2–5d.)

AR 380–67
Personnel Security Program (Cited in para 1–3.)

AR 381–10
The Conduct and Oversight of U.S. Army Intelligence Activities (Cited in para 1–3.)

AR 381–20
The Army Counterintelligence Program (Cited in para 1–3.)

AR 381–47
Offensive Counterintelligence Operations (Cited in para 1–4b(7).)

AR 381–100
The Army Human Intelligence (HUMINT) Collection Program (U) (Cited in para 1–3.)

DoDI 5400.11
DoD Privacy and Civil Liberties Programs (Cited in para 2–5a.)

DoDM 5240.01
Procedures Governing the Conduct of DoD Intelligence Activities (Cited in the title page.)

EO 13526
Classified National Security Information (Cited in para 2–1o.)

Section II

Prescribed Forms
Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil/).

DA Form 7808
U.S. Army Intelligence and Security Records Repository Data Reference Form (Prescribed in para 2–3b.)

Appendix B

Internal Control Evaluation

B–1. Function
The function covered by this evaluation is the USAISRR.

B–2. Purpose
The purpose of this evaluation is to ensure that USAISRR procedures are properly established and followed.

B–3. Instructions
Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, and simulation). Answers that indicate deficiencies must be explained and the corrective action identified in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Test questions
a. Does the USAISRR access records in accordance with the provisions of AR 381–45?

b. Is the Director, USAISRR appointed to implement and monitor these procedures and oversee these responsibilities?

c. Are provisions of AR 381–45 concerning separation and control of controlled records implemented and followed?

d. Are certificates of understanding on file for all FPOs?

e. Are files reviewed for retention or destruction eligibility in accordance with established guidelines and standard operating procedures?

f. Are records only released to authorized requestors?

B–5. Supersession
This evaluation replaces the evaluation previously published in AR 381–45, dated 31 May 2013.

B–6. Comments
Help make this a better tool for evaluating internal controls. Submit comments to the DCS, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Glossary of Terms

Asset
A recruited source.

Controlled record
Files of a particularly sensitive nature due to substantive content or method of collection that are physically segregated from the body of ordinary materials.

Counterintelligence coordinating authority
A staff element that is responsible for mission management of CI activities, whether at Army level (ACICA), theater level (ATCICA), or task force level (task force counterintelligence coordinating authority).

Cross-reference
The identification of the subject of one record with the subject of another by virtue of an alias or some association or activity of legitimate intelligence or CI significance.

Defense Central Index of Investigations
The automated alpha-numeric register of DoD investigations; maintained by the Defense Counterintelligence and Security Agency.

Department of Defense agency
Any department, office, bureau, or organization subject to the authority of the Secretary of Defense.

Impersonal files
Files based on a thing, event, or location.

Record
An official file of investigative, intelligence, or CI materials collected by or on behalf of the Army. It may consist of documents, film, magnetic tape, photographs, digital images, or a combination of these. May be used interchangeably in this publication with “file.” Records may be personal, referring to an individual; or impersonal, referring to a thing, event, or organization.

Retention
The maintenance of information in either hard copy or electronic format regardless of how the information was collected or how it was disseminated.

Source
A person, thing, or activity from which information or services are acquired.

Subject
The person, organization, event, or thing to which a record pertains.

Third-agency
A provision of EO 13526 that stipulates that “classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order. For purposes of this section, the DoD will be considered one agency.”

U.S. person
A United States citizen; an alien known by the defense intelligence component concerned to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the Unites States, is not a U.S. person. A person or organization in the United States is presumed to be a U.S. person, unless specific information to the contrary is obtained. Conversely, a person or organization outside the United States, or whose location is not known to be in the United States, is presumed to be a non-U.S. person, unless specific information to the contrary is obtained (see DoDM 5240.01).

SUMMARY of CHANGE

AR 381–45
U.S. Army Intelligence and Security Records Repository

This major revision, dated 19 April 2023—

- Changes the title of the regulation from Investigative Records Repository to U.S. Army Intelligence and Security Records Repository (cover page).
- Requires the implementation of automated recordkeeping, management, and transmission of records between the repository and organizations requesting access (chap 2).
- Updates the categories of records that may be accessed into the U.S. Army Intelligence and Security Records Repository (para 2–1).
- Prescribes a new form, DA Form 7808 (U.S. Army Intelligence and Security Records Repository Data Reference Form) (para 2–3b).
- Requires quarterly review of holdings by a board to identify records for retention, destruction, or archiving (para 2–7c).
- Establishes policy for the amendment of records (para 3–5).