

Army Regulation 381–45

Military Intelligence

Investigative Records Repository

**Headquarters
Department of the Army
Washington, DC
31 May 2013**

UNCLASSIFIED

SUMMARY of CHANGE

AR 381-45

Investigative Records Repository

This major revision, dated 31 May 2013--

- o Mandates that after 1 year, the record's hard copy version will be destroyed and the digital version will be considered the official record (para 2-8).
- o Adds an Internal Control Evaluation (app B).
- o Replaces all references to the U.S. Army Central Security Facility with 902nd Military Intelligence Group (throughout).
- o Mandates the requirement to provide digital copies of records, along with hard copy documents, for all new records retired to the Investigative Records Repository (throughout).

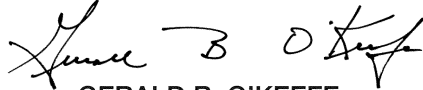
Military Intelligence

Investigative Records Repository

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:



GERALD B. O'KEEFE
Acting Administrative Assistant
to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation establishes policies for storage, maintenance, transmission, review, and scheduled reduction of, as well as access to, investigative records in the custody of the Investigative Records Repository.

Applicability. This regulation applies to the Active 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 request in activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25-30 for specific guidance.

Army internal control process. This regulation is subject to the requirements of AR 11-2 and contains internal control

provisions and identifies key internal controls that must be evaluated (see appendix B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval of the Deputy Chief of Staff, G-2 (DAMI-CDS), 1000 Army Pentagon, Washington, DC 20310-1000.

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

Distribution. This publication is available in electronic media only and is intended for command levels C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Responsibilities • 1-4, page 1

Chapter 2

Operating Procedures, page 2

Authorized files • 2-1, page 2

Accession criteria and procedures • 2-2, page 3

Transmission of materials • 2-3, page 3

File processing • 2-4, page 4

File storage and security • 2-5, page 5

Controlled dossiers • 2-6, page 5

*This regulation supersedes AR 381-45, 25 August 1989.

Contents—Continued

File review • 2-7, *page 7*

File reduction and elimination • 2-8, *page 7*

Chapter 3

Access to Investigative Records Repository Dossiers, *page 7*

Dissemination of information about U.S. persons • 3-1, *page 7*

Procurement accounts • 3-2, *page 7*

File request procedures • 3-3, *page 8*

Accountability • 3-4, *page 9*

Initial and supplemental materials • 3-5, *page 10*

Appendixes

A. References, *page 13*

B. Internal Control Evaluation, *page 15*

Glossary

Chapter 1 Introduction

1–1. Purpose

The Investigative Records Repository (IRR) is a Department of the Army (DA) Records Center that serves as the repository for intelligence, counterintelligence (CI), security investigative, and operational records; related files that meet the criteria of this regulation; and required references created by or for the DA. This regulation establishes Army policy and specific responsibilities concerning these records, by outlining the responsibilities for operation of the IRR; identifying the categories of materials authorized for IRR custody; providing policies and procedures for the storage, maintenance, transmission, review, and systematic reduction of those records; establishing the appropriate uses to be made of IRR materials; and defining the procedures by which Department of Defense (DOD) and other authorized requesters may access IRR holdings.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities

- a. The Deputy Chief of Staff, G–2 (DCS, G–2) will—
 - (1) Develop and publish procedures and specific guidance relating to the establishment, operation, and content of files received by and stored in the IRR.
 - (2) Establish access policies and restrictions on dissemination of IRR materials within DA.
 - (3) Oversee the process of setting up agreements with other government agencies for extended or permanent access to and use of IRR materials.
- b. The Commander, U.S. Army Intelligence and Security Command (INSCOM) will—
 - (1) Coordinate with the DCS, G–2 on IRR implementing guidance, as necessary.
 - (2) Facilitate coordination between INSCOM elements and the IRR.
 - (3) Provide funding and other support to maintain IRR operations and achieve the IRR mission.
 - (4) Conduct intelligence oversight inspections to ensure proper collection, retention, and dissemination rules are followed.
- c. The Commander, 902nd Military Intelligence Group will—
 - (1) Coordinate with Commander, INSCOM on IRR implementing guidance, as necessary.
 - (2) Facilitate coordination between INSCOM elements and the IRR.
 - (3) Conduct intelligence oversight inspections to ensure proper collection, retention, and dissemination rules are followed.
- d. The Director, INSCOM Freedom of Information/Privacy Office and the Chief, IRR will—
 - (1) Ensure the effective and efficient operation of the IRR.
 - (2) Manage the IRR in compliance with applicable Federal statutes, this regulation, and the guidance of the DCS, G–2; Commander, INSCOM; and Commander, 902nd Military Intelligence Group.
 - (3) Prioritize the necessary resources and other support to maintain IRR operations and achieve the IRR mission.
- e. The Chief, IRR will—
 - (1) Ensure timely response to requests from authorized requestors for investigative materials and records.
 - (2) Maintain a continuing review program to identify and transfer or otherwise reduce materials and files no longer required or authorized for IRR retention.
 - (3) Ensure appropriate security of controlled dossiers (CDs) (to include restricting and controlling of access).
 - (4) Provide direction and control for the preparation of affidavits and supporting documents required by the General Counsel when required.
 - (5) Be responsible for the daily operation of the DA Records Center. Daily operational responsibilities include the following:
 - (a) Receiving and accessioning records into the repository.
 - (b) Researching and furnishing the records, extracts, or summaries to authorized requesters.
 - (c) Reviewing records for retention under the provisions of AR 25–400–2 and AR 381–10 and ensuring that information contained in dossiers pertaining to U.S. citizens is complete, timely, accurate, and relevant in accordance with AR 340–21.
 - (d) Ensuring that supplemental materials are posted promptly and accurately to appropriate files.
 - (e) Ensuring proper identification and accountability of U.S. person information maintained at the IRR in accordance with AR 381–10.

- (f) Creating and maintaining IRR entries in the Defense Central Index of Investigations (DCII).
- (g) Accurately accounting for records maintained by the IRR.
- (h) Maintaining disclosure accounting records in accordance with AR 340–21.
- (i) Coordinating with other headquarters and agencies to facilitate the processing of files and information.
- (j) Monitoring and assisting liaison offices of non-DOD agencies accredited by the DCS, G–2.

Chapter 2 Operating Procedures

2–1. Authorized files

a. The following broad categories of materials are authorized for retention within the IRR (see Defense Privacy and Civil Liberties Office Privacy Web site <http://dpclo.defense.gov/privacy/SORNS/component/army/index.html>, for Privacy Act System notices referenced below):

(1) *U.S. Army Intelligence and Security Command investigative files.* Records relating to authorized intelligence or CI operations, missions, or investigations of persons, events, and organizations conducted by INSCOM (or predecessor DA agencies) or other DOD, Federal, State, or local investigative agencies.

(2) *Counterintelligence operations files.* Records obtained by or through agencies in paragraph 2–1a(1), in the conduct of foreign CI operations pertaining to counterespionage, counter-sabotage, countersubversion, and counterterrorism missions of the Army.

(3) *Technical surveillance index.* Records relating to persons whose conversations have been intercepted during technical surveillance operations conducted by or on behalf of the Army.

(4) *Intelligence collection files.* Records describing requirements, objectives, approvals, implementation, reports, and results of DA sensitive intelligence activities.

(5) *Department of the Army operational support activities files.* Documents concerning selected Army military members and civilian employees who have participated in Army intelligence and CI duties.

(6) *Personnel security clearance information files.* Individual case files related to Army military members and civilian employees, including retired personnel, members of 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 interest of national defense under the DOD Industrial Security Program, and persons being considered for participation in other DOD programs.

(7) *Sensitive Compartmented Information Nondisclosure Agreement.* Copies of DD Form 1847–1 (Sensitive Compartmented Information Nondisclosure Statement) or similar forms signed by military or civilian personnel, including employees of contractors, licensees, or grantees with access to information that is classified under standards put forth by executive orders governing security classification.

(8) *Intelligence and/or counterintelligence sources.* Information containing data about personnel who have been used as sources of intelligence or CI information by the Army; the details on the use or activities of a source that are necessary to confirm claims against the Army by source or heirs of the source; or to authenticate an individual was an agent.

(9) *U.S. Prisoner of War, Missing in Action, and/or detainee intelligence.* Documents relating to and containing information about U.S. personnel who have been designated Missing in Action or Prisoner of War, civilian personnel who are being held hostage, or personnel who have been recovered from hostile control and debriefed for intelligence or CI information.

(10) *Polygraph files.* Information on the results of polygraph examinations including conclusions, examination reports, briefing acknowledgements, and consent forms will be stored in the subject dossier under separate cover from other material that may be contained therein in accordance with AR 381–20.

(11) *Counterintelligence special operations files.* Information on the results of counterespionage, countersubversion, and countersabotage operations or programs conducted by or with the Army.

(12) *Human intelligence collections.* Records describing requirements, objectives, approvals, implementation, reports, and results of human intelligence (HUMINT) activities.

(13) *Other files.* Other CI, personnel security, and investigative files as directed by DCS, G–2.

b. IRR dossiers are both personal and impersonal in content and are categorized for retention purposes under the Army Records Information Management System.

c. The following types of materials will not be retained in the IRR:

(1) Personal or impersonal files of nonaffiliated U.S. persons not involved in a CI investigation, operation, HUMINT case, or personnel security investigation. (See AR 381–10 for categories of U.S. person information that may be collected and retained in intelligence databases.)

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

- (3) Impersonal files of a nonderogatory nature with last information more than 1 year old.
- (4) Enemy Prisoner of War, CI, and/or detainee files in peacetime, except detailed debriefing statements of intelligence value.
- (5) U.S. Prisoner of War, CI, and/or detainee files relating to individual U.S. prisoners (except detailed debriefing statements of intelligence value).
- (6) Records of court-martial and nonjudicial punishment administered under Article 15, Uniform Code of Military Justice, except as forwarded by the DOD Consolidated Adjudication Facility as part of a personnel security adjudicative file.
- (7) Non-sensitive compartmented information (SCI) nondisclosure agreements (NDAs), to include read-on verification and NDAs related to sensitive activities and special access programs.
- d.* Materials identified in paragraph 2-1c may be included in IRR files if those materials are exhibits or enclosures to an investigation or incident concerning a subject falling under the purview of paragraph 2-1a. Such materials will not be cross-referenced or otherwise identified in the DCII.

2-2. Accession criteria and procedures

a. Material accessed into the IRR, either initial or supplemental, will contain only one copy of each document having retention value for investigation, adjudication, security, or loyalty review, or containing information concerning persons or organizations of CI interest. All enclosures are retained as part of the transmittal document to which they are attached, even if duplicated by an original copy or identical enclosure to another document elsewhere in the file. Original documents are preferred, but if this is not possible, the best available copy will be accessed. (NOTE: All hard copy files must be submitted with a corresponding digital copy of that file provided by the submitter. Any files not sent with a digital copy of the file will be returned to the submitter.) The following are examples of qualifying documents (this is not an all-inclusive listing):

- (1) Request for CI investigation, request for personnel security investigation, or other similar documents initiating an investigation.
- (2) Background documentation concerning the subject related to initial and periodic background security clearance investigations, to include, but not limited to, the Electronic Questionnaires for Investigations Processing, or other documents containing the results of agency record examinations and digests of biographic information concerning a subject.
- (3) Investigative reports with attached exhibits.
- (4) Defense Security Service (DSS) and Office of Personnel Management inquiries supporting limited investigations or adjudications.
- (5) Case summaries prepared by control offices.
- (6) Results of intelligence interrogations, CI investigations, subject interviews, or sworn statements.
- (7) Correspondence or other documents pertaining to an investigation or adjudication when attached to a Joint Personnel Adjudication System (or system of record) incident report listing the final action.
- (8) Extracts or summaries of reports of inspector general (IG) investigations when they support a CI investigation. The authority directing an IG investigation will determine what information is to be included in the extract or summary. The dossier will not include the basic IG report of investigation. Requests for release of any portion of an IG report, including extracts or summaries there from, will be processed in accordance with the provisions of AR 20-1 (see para 3-4c(2)).
- (9) Correspondence relating to notification of denial or revocation of security clearance or access to SCI, limited access authorization, and reports submitted under provisions of AR 380-67.
- (10) DA Form 5248-R (Report of Unfavorable Information for Security Determination) with any enclosures or attachments thereto.
- (11) DD Form 1300 (Report of Casualty).
- (12) Polygraph examinations (see AR 195-6).
- (13) Electronic surveillance material (formerly wiretap, investigative, and eavesdropping activities) obtained in a manner consistent with applicable regulations and directives.
- (14) Amendments to the record.

b. Polygraph examination reports will be segregated from other dossier material, but maintained within the dossier of the individual to whom they pertain.

c. All material accessed must be certified retainable under AR 381-10 by the originator.

d. All material accessed must show appropriate declassification instructions under the provisions of current classification guidance and appropriate implementing regulations and directives.

2-3. Transmission of materials

a. All materials classified as top secret will be packaged and dispatched in accordance with the provisions of AR 380-5.

b. DA Form 3964 (Classified Document Accountability Record) will accompany each shipment of classified material. Both outer and inner envelopes will be addressed to the File Procurement Agency (FPA) (see para 3-2b). Material transferred electronically via e-mail (attachment), file transfer protocol or on digitized media will be handled at the appropriate classification level.

c. For official use only material will be mailed in an envelope addressed to the FPA (see para 3-2b). Material transferred electronically via e-mail (attachment), file transfer protocol, or on digitized media will be handled at the for official use only level.

d. At a minimum, HUMINT files will be transmitted with protections afforded secret material.

2-4. File processing

a. *Sources of files and/or materials.* The IRR will accept initial or supplemental material from the following sources only:

- (1) Case control offices with responsibility for CI activities for or on behalf of the Army.
- (2) DA agencies authorized to conduct or support intelligence or CI operations.
- (3) Agencies responsible for DA-level intelligence and CI products.
- (4) DOD Consolidated Adjudication Facility.

b. *Initiating and supplementing Investigative Records Repository dossiers.*

(1) All materials submitted for inclusion into the IRR as either initial or supplemental to an existing dossier will be evaluated under the criteria of this regulation and AR 381-10 before accession. Only material related to any of the following descriptive categories will be accepted:

- (a) Persons affiliated with DOD.
- (b) Persons, organizations, and incidents of CI or security interest to the DA.
- (c) Information concerning U.S. persons as authorized by AR 381-10.
- (d) Alien persons or organizations that are the subject of authorized investigations.
- (e) Alien persons or organizations identified in DA intelligence reports or other command intelligence reports.
- (2) Materials requiring controlled custody, as defined in paragraph 2-6, or for which a CD already exists.
- (3) Acceptable materials relating to a subject on which there is no existing file will be accessed into the IRR as a new dossier (classified as appropriate), assigned an identifying number, and entered in the DCII.
- (4) Acceptable materials on which there is an existing subject dossier will be incorporated therein.
- (a) DCII will be updated to reflect the addition of the new material.
- (b) Contents of the dossier will be purged of extraneous materials according to criteria defined in paragraph 2-7.
- (5) Cross-referencing will be accomplished only where doing so would serve legitimate intelligence, CI, or security interests. Cross-referencing will not occur where doing so would cause a person or organization, otherwise of no legitimate interest, to appear in the DCII as the subject of a file.

(6) Exhibits will be handled as follows:

(a) The chain of custody for exhibits or items of evidence developed during an investigation, and that will be used in legal proceedings, extends to the IRR. Exhibits or items of evidence will be identified, including the name of the subject, date and place of birth, social security number, and IRR record number, and will be appropriately identified with a cover sheet.

(b) Exhibits or evidence that are not required for routine investigations or adjudications normally will not be released to requestors.

(7) Initial or supplemental materials inappropriate for IRR retention will be returned to the originating agency or office. Rejection of submitted materials will be based on the following criteria:

- (a) *Substantive.* The material is outside the authority of this regulation or AR 381-10 for retention in IRR files.
- (b) *Procedural.* The submission fails to meet the requirements defined in paragraph 2-6.
- (8) All electronic materials submitted for accession to the IRR will be in the standards specified in the National Archives and Records Administration (NARA) expanding acceptable transfer requirements:

c. *Replies for requested files.*

(1) The IRR will expeditiously service requests from commanders and offices or agencies to which this regulation applies, and for which accreditation has been established. Circumstances or higher authority may require the processing of specific requests ahead of all others. Because of the disruption to IRR operations and the inevitable delays expedited processing inflicts on routine requests, expedited processing will be authorized under the most exceptional circumstances, and only by the Director, INSCOM Freedom of Information/Privacy Office and/or IRR.

(2) In the absence of a directed priority reply, the following order of precedence will be followed in processing requests for IRR files:

- (a) Statutory action (for example, Freedom of Information Act and Privacy Act requests).
- (b) Litigation actions to which the Army is a party.
- (c) INSCOM investigations.

- (d) Criminal investigations.
 - (e) Personnel security and security clearance actions.
 - (f) All others.
- (3) Depending on the nature of the request, replies may be effected by sending the dossier extract or summary thereof.
- (a) Ordinarily, only the DCS, G-2; INSCOM operational elements; and the DOD Consolidated Adjudication Facility may review an entire dossier. Case-by-case exceptions may be granted to other requesters by the Director, INSCOM Freedom of Information/Privacy Office and/or IRR on the basis of compelling justification.
 - (b) Accredited requesters, other than those listed in paragraph 2-4, will be provided, as appropriate, only a favorable response; a reproduced extract of unfavorable (derogatory) information; a summary of the requested dossier; or the response "nothing pertinent to your inquiry." Evaluation of unfavorable (derogatory) information for purposes other than file reduction or elimination, under the provisions of paragraph 2-8, is not an IRR responsibility.
 - (c) Non-DOD agencies will not be provided third-agency materials. The requester will be advised of the existence of such material and the identity of the agency having release authority.
 - (d) Financial records obtained on or after 10 March 1979 will not be disclosed outside DOD unless the requester certifies the relevance of such records in writing in accordance with applicable Army regulations. A copy of the requestor's justification and the release (or denial) authority will be permanently filed in the dossier concerned. Financial information obtained before 10 March 1979 may be released outside DOD according to existing records release procedures for ordinary records.
 - (e) The release of medical record information is governed by AR 40-66, AR 340-21, and AR 600-85, as applicable. The written consent of the subject is required and will become part of the file before release. Signed releases will be forwarded to the Chief, IRR (IAMG-C-IRR), 4552 Pike Road, Fort George G. Meade, MD 20755-5995.
 - (f) Exhibits that are not required for routine investigations or adjudications normally will not be released to requestors.

2-5. File storage and security

- a. The information contained in IRR files, even the very existence of a file, constitutes a major trust placed in the Army by the source of that information. The existence of this bank of information, therefore, constitutes a significant potential liability if an unauthorized disclosure occurs. Personnel assignments and access to and within the IRR will be made in accordance with these considerations (see AR 380-5).
- b. The volume of IRR materials and the nature of the IRR mission require extraordinary measures to safeguard those materials and not overly encumber the service mission. The IRR facility, therefore, will be maintained in its entirety as a limited access area (see AR 190-13). Detailed security procedures recognizing the peculiar circumstances of the IRR will be locally developed, approved by the Commander, 902nd Military Intelligence Group, and rigorously enforced.
- c. Investigative files within the IRR will be stored in such a way as to meet the following mission and security objectives:
 - (1) Efficient retrieval from and return to storage.
 - (2) Primary identification and storage by code number rather than subject name.
- d. Dossiers will be transmitted by any of the methods appropriate for the classification level of the materials as specified in AR 380-5.

2-6. Controlled dossiers

Especially sensitive files will be maintained within the IRR in a limited access status, physically segregated from the main body of IRR materials.

- a. The following two categories of CDs are authorized:
 - (1) *Category 1.* CDs that may be released to an authorized requester by the IRR control custodian only with the prior approval of a designating authority. The designating authorities for establishment of CD category 1 material are as follows:
 - (a) DCS, G-2.
 - (b) Commanding General, INSCOM.
 - (c) Commander, Foreign CI Activity.
 - (d) Chief of the Army CI Coordinating Authority.
 - (2) *Category 2.* CD that may be released to an authorized requester by the IRR control custodian without prior approval of a designating authority.
- b. The DCS, G-2, as control authority, will establish policy and procedures for designating and releasing CDs.
- c. Designating authorities will—
 - (1) Request control of IRR dossiers on personnel under their jurisdiction, or in whom they have an official interest, that contains material warranting stringent control requirements.
 - (2) Designate the appropriate control category for each dossier identified (see para 2-6a).

(3) Review and certify the retainability of those dossiers and any new or supplemental material thereto in accordance with the criteria set forth in AR 340–21 and AR 381–10.

(4) Respond expeditiously to release coordination requests from the IRR control custodian.

d. The Director, INSCOM Freedom of Information/Privacy Office and/or IRR as control custodian will—

(1) Be responsible for the administrative processing, safeguarding, accountability, and custodianship of CDs (except those of selected INSCOM personnel, per para 2–6*i*).

(2) Approve or disapprove all requests for release of all controlled files.

(3) Access the dossiers of all officers selected or promoted to general officer or equivalent ranks into controlled status immediately upon notification of such selection or promotion.

(4) Coordinate with designating authorities when required in the exercise of their dossier control responsibilities.

e. Dossiers and supplemental materials thereto, relating to the following individuals or categories of content, will be accorded control status as follows:

(1) IRR personnel and selected INSCOM and 902nd Military Intelligence Group personnel (CD category 1 and/or CD category 2).

(2) Persons within the commands, agencies, or departments to which this regulation applies who are authorized to request dossiers from the IRR or who have review or adjudicative functions in the personnel or industrial security program (CD category 2).

(3) Army officers (O–6 and below) and DA civilian employees assigned or detailed to another component of the U.S. intelligence community (CD category 1).

(4) All general and flag officers on active duty and for 1 year after retirement (CD category 2).

(5) General officer selectees (CD category 2).

(6) Secretary of the Army and Secretary of the Defense (CD category 2).

(7) Individuals named or material identified by the controlling authority or a designating authority (CD category 1 and/or CD category 2).

(8) Sources (potential, active, or dropped) and covert, clandestine, or confidential informants (CD category 1).

(9) Any person not otherwise specified in this paragraph who, by virtue of their assignment, might gain access to their own dossier (CD category 2).

(10) Persons listed as members of the family or as relatives in biographical listings (for example, Electronic Questionnaires for Investigations Processing), of persons listed in paragraphs 2–6*e*(1) through 2–6*e*(9) (CD category 2).

(11) Material that might reflect unfavorably upon foreign government officials (CD category 1).

(12) Electronic surveillance material (CD category 1). This material will be segregated from the dossier and access will be controlled and recorded. A cross-reference sheet will be placed in the dossier to indicate that electronic surveillance material has been removed and stored in a separate location.

(13) Reports of IG investigations, extracts, or summaries thereof, when they support a CI investigation (CD category 1).

(14) All top secret, SCI, Special Access Program, and restricted data files (CD category 1).

f. Requests for control of individual dossiers may be made by designating authorities at any time by letter or electrical message to the Chief, IRR (IAMG–C–IRR), 4552 Pike Road, Fort George G. Meade, MD 20755–5995. Each request will include the following:

(1) The category of control that is requested. Designating authorities specifying CD category 1 status for materials held in the IRR must be able to review or otherwise certify the releasability of that material to other authorized consumers within 10 days notice of such a request from the IRR control custodian.

(2) Reasons for request, as defined by paragraph 2–6*e*, with full justification whenever based on dossier content rather than the duty assignment or function of the individual.

(3) Duration of control, if known.

(4) Identification of personal data, including date and place of birth, social security number, aliases, and IRR dossier number, if known.

g. Storage and transmission procedures for paper and/or hard copy files and records are as follows:

(1) CDs will be maintained in a distinguishable blue jacket and annotated as necessary with a precautionary warning.

(2) Access to CDs will be limited only to personnel with both a top secret clearance, approved access to requisite programs, and a valid need to know. Requests for access will be processed in accordance with paragraph 2–4*c*.

(3) Transmission of CDs will be effected by any of the methods appropriate for top secret materials as outlined in AR 380–5. The inner envelope will be addressed to the receiving file procurement officer and marked “To be opened by addressee only.”

h. All digitized dossiers in controlled status will be afforded the same type of protection in any electronic records management system used by the IRR.

i. Dossiers of IRR personnel will be placed under control status by the Commander, 902nd Military Intelligence Group.

2-7. File review

a. Each dossier, document, or film on file in the IRR will be subjected to a systematic retention and security classification review each time it is retrieved from storage.

- (1) Nonretainable files will be eliminated in accordance with paragraph 2-8.
- (2) Retainable files will be purged of extraneous and duplicate materials and consolidated with existing film or document counterpart files, as appropriate.

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

2-8. File reduction and elimination

Every effort consistent with legitimate intelligence and security needs will be made to reduce the number and bulk of IRR files. Those objectives will be advanced by—

a. Elimination of duplication within retained dossiers.

b. Elimination of information within each file that is not complete, accurate, relevant, or timely in accordance with AR 340-21.

c. Elimination of nonretainable dossiers.

(1) Substantive retention criteria are established by this regulation and AR 381-10.

(2) Disposition instructions established by AR 25-400-2 will apply.

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

(1) Over aged files of potential historical value will be offered to the NARA under procedures established by AR 25-400-2.

(2) Operational, technical, or confidential source material will not be transferred without approval of the Commander, 902nd Military Intelligence Group.

(3) Overaged files of no interest to NARA will be destroyed in accordance with procedures for disposal of classified material established by AR 380-5 and in accordance with AR 25-400-2.

(4) Entries within DCII or an IRR electronic records management system will be deleted concerning transferred or destroyed dossiers.

e. Digitization of all dossiers, except for certain CDs and NDAs. Upon successful accession and digitization into the IRR electronic records management system, the original (paper) material will be maintained for 1 year after the date of receipt. After this timeframe, the original (paper) material will be destroyed in accordance with AR 25-400-2 and AR 380-5.

Chapter 3

Access to Investigative Records Repository Dossiers

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

a. The release of information concerning U.S. persons is governed by provisions of AR 340-21 and AR 381-10.

b. The most common lawful reasons for accessing an IRR dossier include the following:

- (1) To respond to requests under the Freedom of Information Act and/or Privacy Acts.
- (2) For use in current criminal or security investigations.
- (3) To provide information for authorized security and/or suitability investigations and determinations.
- (4) To provide information pertinent to the protection of persons under Title 18, United States Code, 3056 (18 USC 3056).
- (5) To provide information in judicial or adjudicative proceedings, including litigation, or in accordance with a court or Congressional inquiry.
- (6) To confirm the investigation or clearance of an individual.
- (7) To facilitate the work of the Government Accountability Office.
- (8) To determine whether a record has sufficient historical or other value to justify its continued preservation by the Government.

3-2. Procurement accounts

a. All agencies requiring access to IRR materials will establish a file procurement account according to the following general guidelines. Each account will be assigned an identifying number by the IRR and be serviced through accredited file procurement officers (FPOs). The FPA will designate an account point of contact, which may be an FPO, and provide their telephone number and e-mail address.

(1) Agencies and units requiring only occasional access to IRR files will use the account of a central office or higher headquarters to meet their needs.

(2) Ordinarily, procurement accounts will not be established below the division headquarters (military) or bureau (civilian) levels.

(3) The Chief, IRR may grant an exception for extraordinary circumstances.

b. Correspondence relating to procurement accounts, including requests to establish an account, will be addressed to the Chief, IRR (IAMG-C-IRR), 4552 Pike Road, Fort George G. Meade, MD 20755-5995.

c. Concurrent with a request to establish a file procurement account, correspondents will nominate at least one, but not more than six, individuals as FPOs. Only an FPO can serve as the sole point of contact between the accredited agency and the IRR for management of file requests and the receipt, control, and accountability of IRR files.

(1) FPO nominees must meet the following qualifications:

(a) Have the minimum rank or grade.

1. Military: Enlisted grade E-6, commissioned officer, or warrant officer.

2. Civilian: Currently assigned to a position graded no lower than GS-5.

(b) Possess a valid secret clearance and be eligible for access to top secret information based on a minimum of a favorably completed background investigation. This will be verified via Joint Personnel Adjudication System or the current system of record.

(c) Be permanently assigned to the requesting organization.

(2) FPOs of all accredited agencies will be thoroughly familiar with statutory and regulatory restrictions limiting the dissemination of CI information outside the receiving agency. This familiarization will include the following:

(a) The reading of extracts from 18 USC 793, 18 USC 794, Executive Order 10450 (EO 10450), AR 380-5, and AR 381-10 by each newly accredited representative.

(b) Instruction that disclosure of the contents, sources of information or even the existence of an IRR dossier to persons not officially entitled to such information may be made only when specifically authorized by the DCS, G-2; that material will not be added to or removed from any IRR dossier and the contents of an IRR dossier will not be altered, amended, or rearranged; and that IRR dossiers will be reviewed only in the course of official duties.

(3) A memorandum prepared on agency letterhead will list the FPO being appointed and include the following information for each:

(a) Full name.

(b) Social security number.

(c) Place of birth.

(d) Date of birth.

(e) Clearance level.

(4) A certificate of understanding (see fig 3-1 or fig 3-2, as applicable to the nominating agency) prepared on agency letterhead will be signed by each nominee and forwarded with agency FPO nominations for retention by the IRR.

d. Organizations with file procurement accounts will submit a list of their accredited FPOs to the IRR each January. Delinquency will be cause for the IRR to terminate such accounts the following April. Accounts with no history of requests for 2 consecutive years will be administratively terminated. Changes of FPO personnel will be reported as they occur to ensure continuity of access to IRR services. All correspondence relating to existing accounts will include the IRR-assigned account numbers and be addressed as shown in paragraph 3-2*b*.

3-3. File request procedures

a. Requests for IRR materials in connection with intelligence, CI, security, or litigation matters will come through the accredited FPO to the Chief, IRR (IAMG-CIC-IRR), 4552 Pike Road, Fort George G. Meade, MD 20755-5995.

b. Requests are accepted by mail on DA Form 1144 (Request for Dossier/Index Check), facsimile, or via e-mail unless otherwise specified by the Chief, IRR. Full known identifying data will be provided for personal files, including full name (include all known maiden names or aliases), date and place of birth, social security number, and all pertinent cross-references. Impersonal files will be identified to the fullest extent possible by name, location, date of incident or event, and all pertinent cross-references. Dossier numbers will be included where known. The remarks section of the form will be used for nonstandard items of identification or to indicate the type of information, justification, or review desired, and whether it is a tracer or follow-up on a previous request. Non-DOD agencies will provide the appropriate code with their request (see table 3-1).

(1) Procurement accounts outside DA may use request forms developed by their own agencies for access to IRR materials, provided essential file-identifying data, as defined above, is supplied.

(2) Facsimile or e-mail may be used if expedited service is required. Justification will be provided in all cases. The Chief, IRR will determine if priority processing is appropriate.

(3) Telephonic requests will be accepted only under the most extraordinary circumstances. Urgent requests should be made by facsimile or e-mail.

Table 3–1
Defense Central Index of Investigations accounting codes for disclosures outside of DOD

Code: 01

Purpose: For use in current criminal law enforcement investigations, including statutory violations, counterintelligence, counterespionage, and other security matters. (Disclosure not releasable to subject without coordination with the agency to which record is disclosed.)

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. (Applicable to non-DOD agencies authorized to conduct full background investigations: Office of Personnel Management, Federal Bureau of Investigation (FBI), Internal Revenue Service; U.S. Secret Service; Bureau of Alcohol, Tobacco and Firearms; U.S. Department of Homeland Security; Department of the State; U.S. Postal Service; and Central Intelligence Agency.)

Code: 03

Purpose: To provide information pertinent to protection of persons under the provisions of 18 USC 3056. (Disclosure not releasable to the subject without approval of U.S. Secret Service.)

Code: 04

Purpose: To provide information in judicial or adjudicative proceedings, including litigation, or in accordance with a court or congressional inquiry.

Code: 12

Purpose: To Federal agencies to confirm the investigation or clearance of individuals.

Code: 13

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.

3–4. Accountability

a. Each FPA and appointed FPO is responsible for safeguarding IRR information in accordance with their signed certificate of understanding.

b. Each dossier will be afforded the protection appropriate to its classification.

(1) Only persons with an appropriate security clearance and a legitimate need to know will be permitted access to IRR materials. In no case will the subject of a dossier be allowed access to their own file.

(2) Any lost IRR record or unauthorized disclosure of the contents of an IRR record constitutes a compromise of privileged, often classified information. The provisions of AR 25–55 and AR 380–5 apply. Additionally, the accountable FPO will immediately advise the Chief, IRR, who in turn will notify the Director, INSCOM Freedom of Information/Privacy Office and/or IRR of all particulars concerning the compromise. The Director, INSCOM Freedom of Information/Privacy Office will notify the appropriate security office of any compromise related to classified information and/or the Administrative Assistant to the Secretary of the Army (Records Management and Declassification Agency) for lost or compromised personally identifiable information.

c. Except where otherwise authorized by current regulations (AR 25–55, AR 340–21, AR 380–5, AR 381–10, and AR 381–20) or directives, documents may be copied, extracted, or reproduced from dossiers only to meet investigative, adjudicative, administrative, court-martial, administrative board action, and assignment requirements. Commanders of Army commands, Army service component commands, and direct reporting units and commanders of their major subordinate elements may release information from CI investigative reports to duly-constituted administrative proceedings and courts-martial convened to try individuals for activities revealed by such investigations. The identity of confidential sources or other Federal Government agencies providing information will not be disclosed without the prior written consent of the Commander, INSCOM or higher authority.

(1) Classified material may be reproduced only in accordance with provisions of AR 380–5.

(2) 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 dossier will not be provided in response to requests. Case-by-case justification must be made through the Director, INSCOM Freedom of Information/Privacy Office and/or IRR for final determination by the IG in accordance with AR 20–1.

(3) Financial records will be disseminated to non-DOD agencies only in accordance with paragraph 2–4c(3)(d).

(4) Medical records will be disseminated to non-DOD agencies only in accordance with paragraph 2-4c(3)(e).

(5) Copies, extracts, or reproductions made for DOD agencies will be marked or stamped as follows: "Information copy (extract) only. To be destroyed upon completion of action. Record copy on file at IRR, 902nd Military Intelligence Group, Fort George G. Meade, MD 20755-5595."

(6) Copies, extracts, or reproductions for agencies outside the DOD will contain no third-agency material and will be marked or stamped as follows: "This is a copy (extract) of an investigative document on file at the IRR, 902nd Military Intelligence Group, Fort George G. Meade, MD 20755-5995. It is furnished without prior permission of the Commander, INSCOM or DCS, G-2. It does not constitute a DA determination regarding the subject."

(7) FPOs are responsible for ensuring that materials are appropriately safeguarded from unauthorized disclosure and destroyed promptly following completion of the purpose for which they are produced.

d. Except as provided in paragraph 3-4c, only the IRR may modify the contents of a dossier by adding or removing material. Supplemental materials will be submitted in accordance with paragraph 3-5.

3-5. Initial and supplemental materials

a. Criteria and procedures for submission of materials are defined in paragraphs 2-1, 2-2, and 2-4b.

b. Materials for inclusion in the IRR will be forwarded to the Chief, IRR (IAMG-C-IRR), Fort George G. Meade, MD 20755-5995. Identifying data, as required by paragraph 3-3 will be included with the submission.

c. Initial and supplemental material forwarded to IRR will not contain convenience copies of investigative reports and correspondence, documents of a general administrative nature pertaining to personnel or logistical management, rough draft notes, or documents for which another DA agency is the primary office of record, unless such documents directly pertain to a CI or security investigation or to a security or loyalty adjudication.

d. Agencies other than those identified in paragraph 2-4a, wishing to include material into the IRR will route such material through one of the authorized source agencies.



AGENCY LETTERHEAD
ORGANIZATION NAME
STREET ADDRESS
CITY STATE ZIP

OFFICE SYMBOL

DATE

SUBJECT: Certificate of Understanding

1. As an accredited representative to the IRR, I have access to counterintelligence investigative dossiers of the U.S. Army.
2. The agency that I represent is a signatory to the Delimitations Agreement. As its accredited representative, I understand that in the performance of my official duties at the IRR:
 - a. I may copy, quote, summarize, and otherwise disseminate to my agency information from U.S. Army sources.
 - b. I may summarize or copy information in IRR records originated by other signatory agencies provided that the material does not contain any restrictions by the originating agency.
 - c. I may not extract, quote, summarize, or otherwise disseminate information in IRR dossiers originated by U.S. agencies that are not signatory to the Delimitations Agreement. With respect to such data, I may note the title, date, and originating office of such information.
3. I have read, understand, and will comply with the restrictions concerning the dissemination of classified defense and Privacy Act information set forth in AR 380-5 (Department of the Army Information Security Program) and AR 25-55 (The Department of the Army Freedom of Information Act Program). I will not circulate U.S. Army counterintelligence information, which I may receive in the conduct of my duties, outside my agency without the consent of the IRR.

Signature
Typed Signature
Block (to include Agency Address)

Figure 3-1. Sample certificate of understanding (DOD or FBI)



AGENCY LETTERHEAD
ORGANIZATION NAME
STREET ADDRESS
CITY STATE ZIP

OFFICE SYMBOL

DATE

SUBJECT: Certificate of Understanding

1. As an accredited representative to the IRR, I have access to counterintelligence Investigative dossiers of the U.S. Army.
2. The agency that I represent is not a signatory to the Delimitations Agreement. As its accredited representative, I understand that in the performance of my official duties at the IRR, I may copy, quote, summarize, or otherwise disseminate to my agency, only information obtained from U.S. Army sources.
3. I have read, understand, and will comply with the restrictions concerning the dissemination of classified defense and Privacy Act information as set forth in AR 380-5 (Department of the Army Information Security Program) and AR 25-55 (The Department of the Army Freedom of Information Act Program). I will not circulate U.S. Army counterintelligence information, which I may receive in the conduct of my duties, outside my agency without consent of the DCS, G-2.

Signature
Typed Signature
Block (to include Agency Address)

Figure 3-2. Sample certificate of understanding (Non-DOD or FBI)

Appendix A References

Section I Required Publications

AR 25-55

The Department of the Army Freedom of Information Act Program (Cited in paras 3-4b(2), 3-4c, figs, and 3-2.)

AR 25-400-2

The Army Records Information Management System (ARIMS) (Cited in paras 1-4e(5)(c), 2-8c(2), 2-8d, 2-8d(1), 2-8d(3), 2-8e, and terms.)

AR 340-21

The Army Privacy Program (Cited in paras 1-4e(5)(c), 1-4e(5)(h), 2-4c(3)(e), 2-4, 2-6c(3), 2-8b, 3-1a, and 3-4c.)

AR 380-5

Department of the Army Information Security Program (Cited in paras 2-3a, 2-5a, 2-5d, 2-6g(3), 2-8d(3), 2-8e, 3-2c(2)(a), 3-4b(2), 3-4c, 3-4c(1), fig 3-1, and fig 3-2.)

AR 380-67

Personnel Security Program (Cited in para 2-2a(9).)

AR 381-10

U.S. Army Intelligence Activities (Cited in paras 1-4e(5)(c), 1-4e(5)(e), 2-1c(1), 2-2c, 2-4b(1), 2-4b(c), 2-4b(7)(a), 2-6c(3), 2-8c(1), 3-1a, 3-2c(2)(a), 3-4c, and terms.)

AR 381-20

The Army Counterintelligence Program (Cited in paras 2-1a(10), 3-4c.)

Section II Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this regulation.

AR 11-2

Managers' Internal Control Program

AR 15-6

Procedures for Investigating Officers and Boards of Officers

AR 20-1

Inspector General Activities and Procedures

AR 25-30

The Army Publishing Program

AR 40-66

Medical Record Administration and Health Care Documentation

AR 190-13

The Army Physical Security Program

AR 195-6

Department of the Army Polygraph Activities

AR 381-100

Army Human Intelligence Collection Programs

AR 600-85

The Army Substance Abuse Program

EO 10450

Security requirements for Government employment
(Available at <http://www.archives.gov/federal-register/codification/>.)

EO 13526

Classified National Security Information (Available at <http://www.archives.gov/federal-register/codification/>.)

18 USC 793

Gathering, transmitting or losing defense information (Available at <http://www.law.cornell.edu/uscode/>.)

18 USC 794

Gathering or delivering defense information to aid foreign government (Available at <http://www.law.cornell.edu/uscode/>.)

18 USC 3056

Powers, authorities, and duties of United States Secret Service (Available at <http://www.law.cornell.edu/uscode/>.)

UCMJ, Art. 15

Nonjudicial Punishment (Available at <http://www.au.af.mil/au/awc/awcgate/ucmj.htm>.)

Section III

Prescribed Forms

Unless otherwise indicated below, DA Forms are available on the APD Web site (<http://www.apd.army.mil>).

DA Form 1144

Request for Dossier/Index Check (Prescribed in para 3-3b.)

Section IV

Referenced Forms

Unless otherwise indicated below, DA Forms are available on the APD Web site (<http://www.apd.army.mil>). DD Forms are available from the Office of the Secretary of Defense Web site (<http://www.dior.whs.mil>).

DA Form 11-2

Internal Control Evaluation Certification

DA Form 2028

Recommended Changes to Publications and Blank Forms

DA Form 3964

Classified Document Accountability Record

DA Form 5248-R

Report of Unfavorable Information for Security Determination

DD Form 1300

Report of Casualty

DD Form 1847-1

Sensitive Compartmented Information Nondisclosure Statement

Appendix B Internal Control Evaluation

B-1. Function

The function covered by this evaluation is the IRR.

B-2. Purpose

To ensure that prescribed policies and responsibilities are followed to allow proper accession, identification, sharing, and destruction review. The document used to accomplish the control objective is AR 381-45. This evaluation ensures that IRR 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 IRR access records in accordance with the provisions of AR 381-45?
- b.* Is an individual 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 and/or destruction eligibility in accordance with established guidelines and standard operating procedures?
- f.* Are records only released to authorized requestors?

B-5. Supersession

Not applicable.

B-6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to the Deputy Chief of Staff, G-2 (DAMI-CDS), 1000 Army Pentagon, Washington, DC 20310-1000.

Glossary

Section I Abbreviations

CI

counterintelligence

DA

Department of the Army

DCII

Defense Central Index of Investigations

DCS, G-2

Deputy Chief of Staff, G-2

DSS

Defense Security Service

DOD

Department of Defense

EO

Executive Order

FBI

Federal Bureau of Investigation

HUMINT

human intelligence

IG

inspector general

INSCOM

U.S. Army Intelligence and Security Command

IRR

Investigative Records Repository

NARA

National Archives and Records Administration

NDA

nondisclosure agreement

SCI

sensitive compartmented information

USC

United States Code

Section II Terms

Control office

The agency or organization exercising directive authority over an investigation or collection activity.

Controlled dossier

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

Cross-reference

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

Customer

A Government agency that requires IRR information either to produce other intelligence or for decisionmaking purposes. Synonymous with user, requester, and consumer.

Defense Central Index of Investigations

The automated alpha-numeric register of DOD investigations; maintained by the DSS.

Delimitations Agreement

Agreement between the Deputy Secretary of Defense and the Attorney General of the U.S. that establishes delimitation of responsibilities for CI investigations.

Designating authority

The commander or senior official of a unit, agency, or office having the responsibility for identifying specific IRR dossiers for controlled status and the degree of control.

DOD agency

Any department, office, bureau, or organization subject to the authority of the Secretary of Defense. Synonymous with "DOD component."

Dossier

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 thereof. Synonymous in this publication with "file" or "record." May be "personal" referring to an individual, or "impersonal" referring to a thing, event, or organization.

Initial material

Information on a subject for which there is no known existing dossier.

Liaison representative

An official representative of an agency accredited to request and review dossiers onsite at the IRR. Synonymous herein with "liaison office."

Litigation

Any legal proceeding to which the Government, DOD, its component departments or agencies, or any individual thereof in an official representative capacity is a party.

Retention

The maintenance of information that can be retrieved by reference to name or other identifying data (for example, dossier number). (Information on U.S. persons that is authorized for retention is defined in AR 381-10. The length of retention period is specified in AR 25-400-2.)

a. Limited retention. Material that may be stored for up to 75 years beyond the date of last information. Such material will be destroyed following the end of the prescribed holding period unless disposition is otherwise mandated or required.

b. Permanent retention. Material to be preserved indefinitely by NARA following the end of 25 years retention by DA.

Subject

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

Supplemental material

New information on a subject for which a dossier already exists. Synonymous with "additional material."

Third-agency rule

A provision of EO 13526 which 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. Intelligence community

The collective intelligence apparatus of the U.S., composed of the following:

- a.* The Central Intelligence Agency.
- b.* The National Security Agency.
- c.* The Defense Intelligence Agency.
- d.* DOD components for the collection of national foreign intelligence by reconnaissance programs.
- e.* The Bureau of Intelligence and Research, U.S. Department of State.
- f.* The intelligence elements of the military services of the U.S.
- g.* FBI.
- h.* The U.S. Department of the Treasury.
- i.* The U.S. Department of Energy.
- j.* The staff elements of the Director of Central Intelligence.
- k.* The Director of National Intelligence.

U.S. person

A U.S. citizen, permanent U.S. resident alien, any organization substantially composed of U.S. citizens or permanent U.S. resident aliens, or any organization incorporated under the laws of a State or the U.S., but not directed by a foreign government or governments. Synonymous with U.S. subjects (see AR 381–10).

Section III**Special Abbreviations and Terms****CD**

controlled dossier

FPA

File Procurement Agency

FPO

file procurement officer

UNCLASSIFIED

PIN 004117-000