BILLING C

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2025-OS-0178]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new Department-wide system of records titled, "Counterintelligence Investigations and Collection Activities (CICA)," DoD-0025. This system of records covers DoD's maintenance of records about counterintelligence (CI) investigations and collection activities. The purpose of CICA is to determine whether an individual is acting for or on behalf of foreign powers organizations, or persons, or their agents, or international terrorist organizations or activities.

This differs from the purpose of Counterintelligence Functional Services (CIFS), DoD-0010, which protects Department resources and personnel from foreign adversaries who seek to exploit sensitive information, operations, and agency programs to the detriment of the U.S. Government. It is also separate from the purpose of the DoD Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System, DUSDI 01-DoD, which addresses security functions. Additionally, DoD is issuing a Notice of Proposed Rulemaking, which proposes to exempt this system of records from certain provisions of the Privacy Act, elsewhere in today's issue of the *Federal Register*.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The Routine Uses are effective at the close of the comment period, unless comments have been received from interested members of the public that require modification and republication of the notice.

ADDRESSES: You may submit comments, identified by docket number and title, by either of the following methods:

* Federal Rulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 05F16, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Privacy and Civil Liberties Directorate, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 05F16, Alexandria, VA 22350-1700; osd.mc-alex.oatsd-pclt.mbx.pcld-sorn@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing the "Counterintelligence Investigations and Collection Activities, (CICA)," DoD-0025 as a new DoD-wide Privacy Act system of records. This system of records will ultimately replace multiple systems of records currently maintained at the component level for the same purpose. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use,

and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

CI investigations are formal investigative activities undertaken by the Military Department CI Organizations to determine whether an individual is acting for or on behalf of foreign powers organizations, or persons, or their agents, or international terrorist organizations or activities, and to determine actions required to neutralize such acts. They are investigations in which there is a reasonable belief a member of the U.S. military; a civilian employee or contractor of DoD; or an individual having access to DoD installations, personnel, or information, is engaged in spying or poses a threat to national security. CI collection activities are conducted to acquire information to answer collection requirements to determine if foreign intelligence entities present a threat to U.S. operations, personnel, organizations, or programs. These collection activities may provide the foundation for operations and activities to counter, influence, or negate these threats. They include documents review, liaisons with U.S. and foreign intelligence security, military, and law-enforcement entities.

DoD SORNs have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties Directorate website at https://pclt.defense.gov/DIRECTORATES/Privacy-and-Civil-Liberties-Directorate/Privacy/SORNs/.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: July 16, 2025.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Counterintelligence Investigations and Collection Activities (CICA), DoD-0025.

SECURITY CLASSIFICATION: Unclassified; Classified.

SYSTEM LOCATION:

A. Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations.

B. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S): The system managers for this system of records are as follows:

A. Director for Defense Counterintelligence, Law Enforcement and Security, Office of the Under Secretary of Defense for Intelligence and Security, 1000 Defense, Pentagon, Washington, DC 20301-1100, who is also responsible for implementing policy for the Counterintelligence Collection Activities and Counterintelligence Investigations programs within the Department.

B. Commander, United States Air Force Office of Special Investigations (AFOSI), Department of the Air Force (including Space Command), 27130 Telegraph Road, Quantico, VA 22134, phone number (571) 305-8044.

C. Deputy Chief of Staff for Intelligence, Headquarters, Department of the Army, 1001 Army Pentagon, Washington, DC 20310-1001.

D. Director, United States Naval Criminal Investigation Service (NCIS), Department of the Navy (Navy and Marine Corps), 27130 Telegraph Road, Quantico, 22134.

Note 1. Whereas each component conducts counterintelligence functional services, as described in Counterintelligence Functional Services (CIFS), DoD-0010, the Military Department Counterintelligence Organizations (MDCOs) are the only organizations within the DoD that may conduct counterintelligence investigations, as described in this SORN.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: National Security Agency Act of 1959, as amended (Pub. L. 86–36) (codified at 50 U.S.C. 3601 *et seq.*); the Foreign Intelligence Surveillance Act (FISA), as amended (Pub. L. 95–511) (codified at 50 U.S.C. 1801 *et seq.*); 44 U.S.C. Subchapter II (3551–3559), Information Security (Federal Information Security Modernization Act of 2014 (FISMA)); 50 U.S.C. 3381, Coordination of Counterintelligence Activities; Executive Order (E.O.) 12333, as amended, United States intelligence activities; E.O. 13526, Classified National Security Information; National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems; E.O. 9397 (SSN), as amended by E.O. 13478.

PURPOSE(S) OF THE SYSTEM:

A. To investigate alleged acts by an individual for or on behalf of a foreign power seeking to harm or undermine the security of the United States.

B. To obtain information to answer counterintelligence collection requirements and determine if foreign intelligence entities present a threat to U.S. operations, personnel, organizations, or programs. These activities may provide the foundation for operations and activities to counter, influence, or negate these threats and include document reviews, liaisons with U.S. and foreign intelligence security, military, and law-enforcement entities, and counterintelligence collection activities.

C. To support case management to include case tracking, evidence, statements, reports, and other records necessary to support appropriate administrative, disciplinary, and adjudicative action.

D. To compile statistical information to accomplish management studies, quality control, fulfill mandatory training requirements, and to ensure that completed investigations are legally sufficient.

Note 2. This differs from the purpose of Counterintelligence Functional Services (CIFS), DoD-0010, which is to protect Department resources and personnel from foreign adversaries

who seek to exploit sensitive information, operations, and agency programs to the detriment of the U.S. Government. It is also separate from the purpose of the DoD Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System, DUSDI 01-DoD, which addresses security functions.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals involved in, mentioned in, and/or supporting CI investigations and collection activities, including by not limited to complainants, sources, subjects, and witnesses; individuals within DoD's investigatory jurisdiction, including military and civilian personnel or contract employees.

CATEGORIES OF RECORDS IN THE SYSTEM: CI investigations and collection activities records include CI awareness and reporting records, threat assessment records, incident assessment records, and records produced as a result of CI specialized technical services, e.g., Technical Surveillance and Countermeasures. These records may contain the following data elements as necessary:

A. Personal information such as: names, social security numbers (SSN), DoD/ID numbers, employee identification numbers, date and place of birth, addresses, contact information, biometric information, fingerprints and retinal data, medical/psychological information, travel identification information (passport, visa, resident alien), driver's license information (state, number, and expiration date, etc.), biographic information, family and dependent information, sex, race/ethnicity, and property information.

B. Employment information such as: position/title, rank/grade, duty station; work address, email address, supervisor's name and contact information, military records, personnel security information, employment personnel files, financial information (to include tax identification information), financial reports and transaction data, and education and training records.

Note 3. Records supporting the counterintelligence mission, which safeguards Department resources and personnel against foreign adversaries seeking to exploit sensitive information, operations, and programs, potentially harming the U.S. Government are maintained under

Counterintelligence Functional Services (CIFS), DoD-0010. However, such records may become part of this system when they are necessary to accomplish the purpose of this system.

Note 4. Records supporting the insider threat program, which focuses on security functions, are maintained under the DoD Insider Threat Management and Analysis (DITMAC) and DoD Component Insider Threat Records System, DUSDI 01-DoD. However, such records may become part of this system when they are necessary to accomplish the purpose of this system.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: complainants, sources, subjects, or witnesses, government sources (Federal, state, local, tribal and foreign), social media, periodicals, newspapers, information from commercial databases, and information from classified sources to include intelligence reports, security sources, law enforcement information, and correspondence.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is relevant and necessary.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General

in conducting an audit, investigation, inspection, evaluation, or other review as authorized by the Inspector General Act of 1978, as amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

K. To third parties during the course of an authorized inquiry to the extent necessary to obtain information pertinent to the inquiry, provided disclosure is appropriate to the proper performance of the official duties of the DoD official making the disclosure.

L. To U.S. Government agencies or organizations for the purpose of notifying, coordinating, or addressing actual or potential compromises of classified information.

M. To appropriate Federal, state, local, territorial, tribal, foreign or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

N. To designated officers, contractors, and employees of Federal, state, local, territorial, tribal, international, or foreign agencies for the purpose of the hiring, detailing, licensing, or retention of an individual, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a license, grant or other benefit, to the extent that the information is relevant and necessary to the agency's decision on the matter.

O. To the DOJ and other Federal, State, or local government prosecuting or litigating agencies, for the purpose of satisfying obligations under *Giglio* (405 U.S. 150 (1972)) and *Henthorn* (931 F.2d 29 (9th Cir. 1991)), as well as the DOJ United States Attorneys' Manual, Section 9-5.100 and DoD IG Instruction 5500.1, DOJ Requirements for Potential Impeachment Information (Giglio Policy), or DoD OIG initiated notifications of similar information.

P. To the Department of State when it requires information to consider and/or provide a disclosure of information, or an informed response to a request for information, from a foreign,

international, or intergovernmental agency, authority, or organization about an enforcement, counterintelligence, or national security matter with transnational implications.

Q. To the news media and the public, with the approval of the Under Secretary of Defense for Intelligence and Security in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DoD, or when disclosure is necessary to demonstrate the accountability of DoD's officers, employees, or individuals covered by the system, except to the extent the Under Secretary determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by personal and employment data elements that may identify the individual to whom the reporting pertains, including, but not limited to, name, social security number, DoD/ID or employment identification number, and email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are maintained and disposed of in accordance with National Archives and Records Administration Schedules and authorized DoD component Records Disposition Schedules. The retention period for specific records may be obtained by contacting the system manager for the Component.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies

require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely applies administrative, technical, and physical safeguards to information systems and paper recordkeeping systems such as the following: multifactor authentication, including CAC authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption security disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access to sensitive data; identification and marking of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure, and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, email address, and date of birth of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

> If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3); (d)(1), (2), (3) and (4); (e)(1); (e)(4)(G), (H) and (I); and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2) as applicable. An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c), and (e) and published in 32 CFR part 310. In addition, when exempt records received from other systems of records become part of this system, DoD also claims the same exemptions for those records that are claimed for the prior system(s) of records of which they were a part, and claims any additional exemptions set forth here.

HISTORY: None.

[FR Doc. 2025-13582 Filed: 7/18/2025 8:45 am; Publication Date: 7/21/2025]