**DEPARTMENT OF DEFENSE**

**Office of the Secretary**

**[Docket ID: DOD-2026-OS-0661]**

**Privacy Act of 1974; System of Records**

**AGENCY:** Office of Inspector General (OIG), Department of Defense (DoD).

**ACTION:** Notice of a modified system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the DoD is modifying and reissuing a current system of records notice titled "Case Reporting and Information Management System Records," CIG-04. The system of records is being retitled, "Inspector General Criminal Investigation Records (IGCIR)." This system of records was originally established by the DoD OIG to collect and maintain records on individuals suspected of criminal misconduct and investigated pursuant to the Inspector General Act. This system of records is being combined with CIG-06, "Investigative Files," to consolidate criminal investigative records and investigative files into a single system. A separate notice rescinding CIG-06 is being published elsewhere in today's issue of the **Federal Register**. This system of records notice (SORN) is being updated to incorporate the DoD standard routine uses and to support additional information sharing outside of the DoD in furtherance of external oversight, case management, and required reporting. The DoD is also modifying various other sections within the SORN to add exemptions, improve clarity, and update information that has changed. Additionally, the DoD is issuing a Notice of Proposed Rulemaking (NPRM), 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 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 any of the following methods:

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

* Mail: Department of Defense, Office of the Director of Administration and Management, Privacy, Civil Liberties, and Transparency Directorate, Regulatory Division, 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. Anna Rivera, Government Information Specialist, FOIA, Privacy and Civil Liberties Office, Department of Defense, Office of Inspector General, 4800 Mark Center Drive, Alexandria, VA 22350-1500; privacy@dodig.mil; (703) 699-5680.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

The Inspector General Criminal Investigation Records (IGCIR) system of records is used by the DoD OIG to carry out its responsibilities pursuant to the Inspector General Act of 1978, as amended. The DoD OIG is statutorily authorized to investigate matters relating to DoD programs and operations; to detect and deter fraud, waste, and abuse; and to help ensure ethical conduct throughout the DoD. Specifically, the CIG-04 system of records, which is now consolidated with the CIG-06 system of records, contains records of DoD OIG mission activities

such as records related to criminal investigations, crime prevention, criminal intelligence activities, and the criminal investigative process. These records include case management notes and evidence tracking. The system also provides users with the capability to record allegations and requests for assistance. Through the system, DoD OIG compiles statistical information on the data stored, provides responsive and accurate information regarding the status of ongoing cases, and provides a record of complaint disposition, actions taken, and notifications to interested parties. Subject to public comment, the DoD is updating this SORN to add the standard DoD routine uses (routine uses A through J) and to allow for additional disclosures outside DoD related to the purpose of this system of records. The DoD also proposes to claim exemptions for the system pursuant to subsection (k) of the Privacy Act. Additionally, the following sections of this SORN are being modified to include retitling the system name. The DoD OIG also restructured and updated the purpose of the system, categories of individuals, and categories of records in the system, to reflect consolidation with the CIG-06 system of records. In line with these modifications, changes have been made to the system location; system manager; authority for maintenance of the system; record source categories; policies and practices for storage, retrieval, and disposal of records; administrative, technical, and physical safeguards; and records access, contesting record, and notification procedures.

The DoD is issuing a NPRM to exempt this system of records from certain provisions of the Privacy Act, elsewhere in today's issue of the **Federal Register**. This rulemaking will seek public comment on the proposed exemptions under 5 U.S.C. 552a(k)(1) and (k)(2).

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

**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: April 7, 2026.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

**SYSTEM NAME AND NUMBER:** Inspector General Criminal Investigation Records (IGCIR), CIG-04.

**SECURITY CLASSIFICATION:** Unclassified; classified.

**SYSTEM LOCATION:** Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer, 6000 Defense Pentagon, Washington, DC 20301-6000.

**SYSTEM MANAGER(S):** DoD Office of Inspector General (OIG), Defense Criminal Investigative Service Program Manager, 4800 Mark Center Drive, Alexandria, VA 22350-1500.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 10 U.S.C. 141, Inspector General; 5 U.S.C. 4, Inspector General Act; Pub. L. 117-286; 10 U.S.C. 113, Secretary of Defense; DoD Directive (DoDD) 5106.01, Inspector General of the Department of Defense; DoDD 5106.04, Defense Inspectors General; and E.O. 9397 (SSN), as amended.

**PURPOSE(S) OF THE SYSTEM:** This system supports DoD OIG staff and investigators in support of the law enforcement investigative process and associated activities within its jurisdiction, specifically:

A. To conduct criminal investigations, crime prevention, and criminal intelligence activities that impact the health, life, safety, and mission-readiness of U.S. warfighters.

B. To coordinate with and provide information to other investigative elements of the DoD having jurisdiction over the substance of the allegations or a related investigative interest in criminal law enforcement investigations including statutory violations, counterintelligence, counter-espionage and counter-terrorist activities and other security matters.

*Note 1*: The DoD OIG may become involved in joint investigations with other investigative elements. In these situations, case records may also be maintained within a system of records of the other investigative element.

C. To support case management to include case tracking, evidence, statements, reports, and other records necessary to support subsequent actions taken as a result of a criminal investigation.

*Note 2*: Records maintained for the purpose of supporting adjudication and litigation in judicial, administrative, or disciplinary proceedings are maintained in DoD-0006, Military Justice and Civilian Criminal Case Records, or DoD-0020, Military Human Resource Records. Records from this system may also be maintained in those other systems when they are relevant and necessary to a proceeding.

*Note 3*: DoD OIG Administrative Investigation records are excluded from this system of records and instead covered by CIG-16, Inspector General Administrative Investigation Records.

D. To document and respond to requests for information for investigative reports or report disposition to include requests in accordance with a court order, attorneys general requests to provide facts and evidence upon which to base prosecution, requests to identify offenders, and congressional inquiries.

*Note 4*: Records related to reporting, tracking, and processing access requests made pursuant to the Freedom of Information Act, 5 U.S.C. 552, or subsection (d) of the Privacy Act, 5 U.S.C. 552a, are covered by DoD-0008, Freedom of Information Act and Privacy Act Records.

E. To support mandatory reporting requirements, the compilation of statistical information, and the provision of data for analysis and decision-making related to the activities described.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** Individuals covered by this system are persons who have been identified as a target, subject, or informant, as well as victims and witnesses, of the law enforcement investigative process and associated activities, to include:

A. DoD civilian personnel.

B. Military personnel and members of the Armed Forces, to include Reserve components and National Guard units.

C. DoD contract employees that are or have been the subject of a DoD OIG criminal investigation.

D. Individuals residing on, having authorized official access to, or contracting or operating any business or other functions at any DoD installation or facility.

E. Individuals not affiliated with DoD, when their activities have directly threatened the functions, property or personnel of the DoD; or they have threatened any high ranking government individual who are provided protective service mandated by the Secretary of Defense; or have engaged in or are alleged to engage in criminal acts on DoD installations, or directed at the DoD, its personnel or functions.

**CATEGORIES OF RECORDS IN THE SYSTEM:** Records in this system are from the referral of and inquiry into criminal wrongdoing. Records include Reports of Investigation, Information Reports, case summaries, and investigative information. The criminal investigative file may contain the following data points:

A. Biographic information: Full name, social security number (SSN), or driver's license number, photo, alien registration number, passport number, sex, race and ethnicity, date and place of birth, home and email address, home or cellular telephone number, and marital status.

B. Employment information: Office mailing address, office or work cellular telephone number, work email address, employer(s), date(s) of employment, and salaries.

C. Law enforcement data: Case control number, polygraph records, charts, rights waivers, polygraph waivers, interview logs, disposition and suspense of offenders, criminal intelligence reports, witness, suspect, subjects, and special agent statements, fingerprints, laboratory reports, ballistic summaries, consensual and nonconsensual monitoring, agent notes and summaries, working papers, confidential source documents, subpoenas, and Grand Jury documents.

D. Financial information: Any financial record associated to personal, corporate, and government financial accounts where criminal conduct may be documented. Financial records include, but are not limited to, monthly bank statements, signature cards, loan applications, contract payments information, electronic funds transfer documents, wire transfer instructions, Society for Worldwide Interbank Financial Telecommunication (SWIFT) international payment transactions, and credit card records.

E. Medical records: Medical records associated with suspected criminal activity involving healthcare providers, healthcare facilities, and patients where the suspected criminal activity is deemed to impact the DoD or its personnel.

F. Other records gathered during the course of the investigation that are relevant to the nature of the investigation, such as a description of physical evidence, basis for allegations, location, year and date of offense, photos of persons who are subject to electronic surveillance, special investigative techniques, and any other type of record deemed necessary to support the investigation.

**RECORD SOURCE CATEGORIES:** Records and information stored in this system of records are obtained from:

A. Special agents, private industry, non-profit organizations, internet websites, subjects, suspects, witnesses, and informants interviewed and questioned during the course of a criminal investigation.

B. Federal, State, Tribal and local agencies and departments.

**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 a breach of the system of records; (2) the DoD determines 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, in coordination with an Office of Inspector General, for the purpose of 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 other Federal Inspector General offices, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and/or other law enforcement agencies for the purpose of coordinating and conducting administrative inquiries and civil and criminal investigations, or when responding to such offices, CIGIE, and agencies in connection with the investigation of potential wrongdoing, including violations of law, rule, and/or regulation.

L. To other Federal Inspector General offices, the CIGIE, and/or the Department of Justice for purposes of conducting external reviews to ensure that adequate internal safeguards and management procedures continue to exist within the Office of Inspector General of the Department of Defense.

M. To designated officers, contractors, and employees of Federal, State, local, territorial, tribal, international, or foreign agencies, upon request, for the purpose of the hiring 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.

N. To the Office of Management and Budget for the purpose of review of private relief legislation as set forth in OMB Circular A-19 at any stage of the legislative coordination and clearance process as set forth in that circular.

O. To any individual or entity employed by or connected with an overseas Military Banking Facility who is reimbursed by the Government for certain checking and loan losses, in response to its request, for the purpose of identifying Armed Forces personnel and their last known residential or home of record address.

P. To any individual or entity when necessary to elicit information that will assist an OIG investigation, inspection, or audit.

Q. To foreign or international law enforcement, security, investigatory authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

R. To the Merit Systems Protection Board or the Office of Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the civil service and other merit systems; review of Office of Personnel Management (OPM) or component rules and regulations; investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation.

S. To OPM for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for OPM to carry out its legally authorized government-wide personnel management functions and studies.

T. To the news media and the public with the approval of the DoD Inspector General 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 Inspector General determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

U. To the Department of Justice (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 Inspector General Instruction 5500.1, DOJ Requirements for Potential Impeachment Information (Giglio Policy), or OIG initiated notifications of similar information.

V. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate governmental entity tasked with public health and safety, for the purpose of sharing such information as is necessary and relevant to the detection, prevention, disruption, and mitigation of threats to public health or safety, where a record, either alone or in conjunction with other information, indicates a violation or potential violation of administrative standards or indicates a threat or potential threat to public health and safety.

W. 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.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Records may be stored electronically or on paper in secure facilities in a locked drawer and behind a locked door. Electronic records may be stored on magnetic disc, tape, or 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 case control number, name and date of birth, social security number, driver's license number, alien registration number, and passport number.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Permanent. Retire to WNRC 3 years after case closure. Transfer to the National Archives in 5-year blocks when the newest case in the block has been closed for 25 years.

TEMPORARY. Retire to WNRC 3 years after case closure. Destroy 25 years after case closure.

**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 administrative safeguards include policies requiring the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and restrict access to those individuals who have a need-to-know and appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of incidents involving PII (breaches). DoD also employs administrative controls including mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII. Personnel, including contractors, must pass a background investigation and receive a security clearance, when necessary. Personnel must also sign nondisclosure documents. DoD routinely employs technical safeguards such as the following: multifactor authentication including presentation of a Common Access Card (CAC) and password; and use of a physical token. Other technological controls are employed such as network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities. Computerized records in a controlled area accessible only to authorized personnel.

Records are maintained in a controlled facility and physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Physical and electronic access is restricted to designated individuals having a need for access in the performance of official duties and who are properly screened and cleared for need-to-know.

**RECORD ACCESS PROCEDURES:** Individuals seeking access to their records should address written inquiries to the DoD OIG Freedom of Information Act, Privacy and Civil Liberties Office, 4800 Mark Center Drive, Alexandria, VA 22350-1500, www.dodig.mil/FOIA or foiarequests@dodig.mil. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address 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 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:** The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained within 32 CFR part 310, or may be obtained from the system manager.

**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:** Pursuant to 5 U.S.C. 552a(j)(2), portions of this system are exempt from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3) and(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f) and (g). Additionally, pursuant to 5 U.S.C. 552a(k)(1) and (k)(2) portions of this system are exempt

from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). An exemption rule for this record 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, the DoD also claims the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

**History:** June 16, 2014, 79 FR 34297; February 10, 2009, 74 FR 6587.

[FR Doc. 2026-06950 Filed: 4/9/2026 8:45 am; Publication Date: 4/10/2026]