SYSTEM NAME AND NUMBER: Case Control System—Investigative, CIG-26. (July 1, 2020; 85 FR 39540)

SECURITY CLASSIFICATION: Classified and Unclassified.

SYSTEM LOCATION: DoD Office of Inspector General (OIG), Office of Professional Responsibility (OPR), 4800 Mark Center Drive, Alexandria, VA 22350-1500.

SYSTEM MANAGER(S): DoD OIG, OPR, 4800 Mark Center Drive, Alexandria, VA 22350-1500.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Inspector General Act of 1978, as amended; Inspector General Reform Act of 2008; Inspector General Empowerment Act of 2016; 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 141, Inspector General; and DoD Directive 5106.01, Inspector General of the Department of Defense, and Executive Order (E.O.) 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: The DoD OIG maintains this System of Records, on behalf of the Office of Professional Responsibility (OPR), in order to carry out its responsibilities pursuant to the Inspector General Act of 1978, as amended. The DoD OIG is statutorily authorized to conduct and supervise investigations relating to the programs and operations of the DoD, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Specifically, the OPR is responsible for investigating administrative and criminal misconduct alleged against DoD OIG employees and military personnel assigned to the DoD OIG. The records in this system are used in the course of such investigations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DoD OIG employees, military personnel, and contractors involved in, mentioned in, and/or subject to OPR investigations or complaints; including any complainants, sources, subjects, and witnesses.

CATEGORIES OF RECORDS IN THE SYSTEM: Individual's full name, DoD Identification Number, SSN, date of birth, email addresses, duty positions, telephone numbers, case control number, and other personal information related to investigations and inquiries.

RECORD SOURCE CATEGORIES: The individual, DoD OIG investigators, witness statements, DoD records, and law enforcement agencies' records.

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, the records contained therein 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 appropriate Federal, State, local, territorial, tribal, foreign or international agencies having jurisdiction over the substance of the allegations or a related investigative interest in criminal law enforcement investigations, including statutory violations, counter-intelligence, counter-espionage and counter-terrorist activities and other security matters for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, to include activities authorized by 6 U.S.C. 485(a)(5), Domestic Security; 6 U.S.C. 482, Facilitating Homeland Security; Intelligence Reform and Terrorism Protection Act of 2004; and E.O. 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.

c. 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 violations of law, rule, and/or regulation.

d. 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).

e. To designated officers, contractors, and employees of Federal, State, local, territorial, tribal, international, or foreign agencies 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 and that the employer is appropriately informed about information that relates to or may impact an individual's suitability or eligibility.

f. To the news media and the public unless it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

g. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation or case arising from the matters of which they complained and/or which they were a victim.

h. 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.

i. 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.

j. 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 pertinent.

k. 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.

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

m. 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.

n. 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.

o. To another Federal agency or Federal entity, when the DoD determines 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Paper records and electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by individual's name or case control number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Unfounded or unsubstantiated investigative files are destroyed 10 years from the date the report is completed. Substantiated investigative files are destroyed 10 years from the date the report is completed or 5 years after termination of employee, whichever is later. Reports are dated when completed and once a final determination has been made.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The database access is restricted to authorized Office of Professional Responsibility staff with an authenticated need to know who are properly screened, cleared, and trained. The database is safeguarded by role-based common access card permissions and an associated personal identification number, encryption, and system firewalls. Paper records are stored in a controlled facility with limited suite access protected by cipher lock and physical security to monitor areas and personnel access.

RECORD ACCESS PROCEDURES: As specified in the exemptions claimed for this system, the records in this system are exempt from certain notification, access, and amendment procedures. A request for access to non-exempt records shall address written inquiries to the DoD OIG FOIA, Privacy and Civil Liberties Office, ATTN: Privacy Act Officer, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500. For verification purposes, individuals must provide their full name and any details which may assist in locating records of the individual. The request must be signed by the requesting individual and they must provide a notarized statement or a signed declaration made in accordance with 28 U.S.C. 1746, in the following 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: The DoD rules for accessing records, for contesting contents and appealing initial agency determinations are published in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: As specified in the exemptions claimed for this system, the records in this system are exempt from certain notification, access, and amendment procedures. Individuals seeking to learn whether this system contains nonexempt information about them should address written inquiries to the DoD OIG FOIA, Privacy and Civil Liberties Office, ATTN: Privacy Act Officer, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500. For verification purposes, individuals must provide their full name and any details which may assist in locating records of the individual. The request must be signed by the requesting individual and they must provide a notarized statement or a signed declaration made in accordance with 28 U.S.C. 1746, in the following 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)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The DoD exempted records maintained in the CIG-26, from subsections (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G) through (I), (e)(5), (e)(8), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a 552a(j)(2) as records maintained by an agency or component thereof that performs as its principal function any activity pertaining to the enforcement of criminal laws. The DoD also exempted records maintained in the CIG-26, from subsections (c)(3), (d), (e)(1), and (e)(4)(G) through (I), of the Privacy Act pursuant to 5 U.S.C. 552a 552a(k)(1) and (k)(2) to the extent that such records are

properly classified pursuant to an executive order and are investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2).

This system may contain records or information compiled from or created from information contained in other Systems of Records, which may be exempt from certain provisions of the Privacy Act. To the extent that copies of exempt records from those `other' System of Records are entered into this System of Records, the DoD claims the same exemptions for the records from those `other' systems that are entered into this system, as claimed for the original primary system of which they are a part. Any exemption claimed from the originating agency will follow the record. A determination as to exemption shall be made at the time a request for access or amendment is received.

Parts of this system may be exempt pursuant to 5 U.S.C. 552a (k)(2) as applicable. However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or for which he would otherwise be eligible, as a result of the maintenance of such information, the individual will be provided access to such information except to the extent that disclosure would reveal the identity of a confidential source.

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 310.28.

HISTORY: August 9, 2011, 76 FR 48812.