in a comment, be advised that the entire comment—including PII—may be made publicly available at any time. While one may ask in a comment to withhold PII from public view, the USPTO cannot guarantee that it will be able to do so.

Justin Isaac,

Information Collections Officer, Office of the Chief Administrative Officer, United States Patent and Trademark Office.

[FR Doc. 2026–01229 Filed 1–22–26; 8:45 am]

BILLING CODE 3510–16–P

DEPARTMENT OF DEFENSE

Department of the Army

[Docket ID: USA–2026–HQ–0100]

Privacy Act of 1974; System of Records

AGENCY: Department of the Army, Department of Defense (DoD).

ACTION: Rescindment of a System of Records Notice.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of the Army is rescinding a System of Records Notice titled, Controlled Accountable Document Inventory System, A0001 DAMI. This system was established to conduct periodic inventory of classified documents and to determine or validate custodial accountability of those documents.

DATES: The rescindment of this SORN is effective January 23, 2026.

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 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. Joyce Luton, Department of the Army, Records Management Directorate, Attention: Army Privacy and Civil Liberties Office, 9301 Chapek Road (Building 1458), Fort Belvoir, VA 22060–5605 or by calling (571) 515–0213.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of the Army system of records Controlled Accountable Document Inventory System, A0001 DAMI (February 22, 1993; 58 FR 10002) was established to conduct periodic inventory of classified documents and to determine or validate custodial accountability of those documents. The Army is rescinding A0001 DAMI because the records are now maintained as part of the A0 0001 DAMI, U.S. Army Security and Foreign Disclosure Files, published elsewhere in today's issue of the **Federal Register**.

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

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 alien lawfully admitted for permanent residence.

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 SORN rescindment to OMB and Congress.

SYSTEM NAME AND NUMBER:

Controlled Accountable Document Inventory System, A0001 DAMI.

HISTORY:

February 22, 1993; 58 FR 10002.

Dated: January 20, 2026.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2026–01235 Filed 1–22–26; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Department of the Army

[Docket ID: USA–2026–HQ–0067]

Privacy Act of 1974; System of Records

AGENCY: Department of the Army, Department of Defense (DoD).

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of the Army is modifying and reissuing a current system of records notice (SORN) titled ''Personnel Security Clearance Information Files,'' A0380–67 DAMI. The SORN is being retitled ''U.S. Army Security and Foreign Disclosure Files,'' with a new identifier of A0 0001 DAMI. Originally established to facilitate the processing of personnel security clearance actions, the SORN also documented clearances granted or denied and confirmed eligibility for access to classified information or assignment to sensitive positions. A separate notice rescinding Army SORN A0001 DAMI, ''Controlled Accountable Document Inventory System,'' is being published elsewhere in this issue of the **Federal Register**. This update incorporates the DoD standard routine uses and supports additional information sharing outside of the DoD. It also expands the authorities for maintaining the system, integrates records previously managed under the Controlled Accountable Document Inventory System, addresses records maintained across all general intelligence security disciplines, and expands on the purposes of such uses. Additionally, the update revises system locations and managers. These changes align the SORN with modernized automation systems and ensure compliance with applicable regulatory requirements.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before February 23, 2026. 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. Joyce Luton, Department of the Army, Records Management Directorate, Attention: Army Privacy and Civil Liberties Office, 9301 Chapek Road (Building 1458), Fort Belvoir, VA 22060–5605 or by calling (571) 515–0213.

SUPPLEMENTARY INFORMATION:

I. Background

The Headquarters, Department of the Army, Office of the Deputy Chief of Staff, G–2 (ODCS G–2) is making a comprehensive update to its Personnel Security Clearance Information Files system of records. This modification consolidates and supersedes existing Army personnel security-related notices aligning them under G–2's integrated lines of effort designed to prevent unauthorized disclosures or compromises of Army information, such as classified data, and to support the clearance, training, and protection of personnel in accordance with national security priorities. This update expands the authorities governing system maintenance and integrates records previously managed under both the Personnel Security Clearance Information Files and the Controlled Accountable Document Inventory System. The consolidation groups all similar security-related under a single notice, eliminating redundant notices and covering all Army records maintained across security disciplines that require the collection and retention of personnel identifying information. It also encompasses records maintained across all general intelligence security disciplines and broadens the scope of permissible uses. In addition, the system's locations and responsible managers have been revised to reflect current operational structures. These changes ensure the system is consistent with modernized automation systems and compliant with applicable regulatory requirements.

Records within the Army Security and Foreign Disclosure Records Systems are not centrally stored in a single information technology (IT) capability. Instead, the term ''system'' collectively refers to all security records, both analog and digital, maintained at security offices across the Army. These records support Army security vetting, facility and information system access, and other security-related functions. The system integrates IT capabilities to comply with regulatory requirements related to initial and continued employment; to determine eligibility for access to Army information (*e.g.,* controlled unclassified information (CUI), classified information), IT systems, facilities, research, technologies, or programs; identify, mitigate, and process adverse personnel information.

This system supports the Army's operational administration, management, accountability, and oversight of its security functions which includes Information Security, Personnel Security, Industrial Security, Education and Awareness, Communications Security, Sensitive Compartmented Information (SCI) protection, Research and Technology Protection, Special Access Programs (SAPS), and Foreign Disclosure management.

Subject to public comment, the Army proposes to update this SORN by adding the standard DoD routine uses (A through J) and authorizing additional disclosures outside the DoD consistent with the system's purpose. The update also includes retitling the SORN name, incorporating and expanding routine uses, and revising the following sections: system location, system manager, authority for maintenance, record source categories, policies and practices for storage, retrieval, and disposal, safeguards, and procedures for accessing, contesting, and receiving notification about records.

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

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 the 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: January 20, 2026.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER:

U.S. Army Security and Foreign Disclosure Files, A0 0001 DAMI.

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 (CIO), 6000 Defense Pentagon, Washington, DC 20301–6000.

SYSTEM MANAGER(S):

The system manager is the Senior Security Advisor, Headquarters, Department of the Army (HQDA), Office of the Deputy Chief of Staff (ODCS), G–2, 1000 Army Pentagon, Washington, DC 20310–1000.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

National Security Act of 1947, as amended, 50 U.S.C. 3036; 5 U.S.C. 9101, Access to Criminal History Records for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence and Security; 10 U.S.C. 504, Persons Not Qualified; 10 U.S.C. 505, Regular components: Qualifications, term, grade; 10 U.S.C. 3013, Department of the Army; Public Law 108–458, The Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 401 note); Public Law 114–92, Section 1086, National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016, Reform and Improvement of Personnel Security, Insider Threat Detection and Prevention, and Physical Security (10 U.S.C. 1564 note); Public Law 114–328, Section 951 (NDAA for FY2017), Enhanced Security Programs for Department Defense Personnel and Innovation Initiatives (10 U.S.C. 1564 note); Public Law 115–91, Section 925, (NDAA for FY2018) Background and Security Investigations for Department of Defense Personnel (10 U.S.C. 1564 note); Executive Order (E.O.) 10865, as

amended, Safeguarding Classified Information Within Industry; E.O. 12333, as amended, United States Intelligence Activities; E.O. 12829, as amended, National Industrial Security Program; E.O. 12968, as amended, Access to Classified Information; E.O. 13467, as amended, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 13488, as amended, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust; E.O. 13526, Classified National Security Information; E.O. 13549, as amended, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities; E.O. 13741, Amending Executive Order 13467, To Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters; E.O. 13764, Amending the Civil Service Rules; National Security Presidential Memorandum 33 (NSPM–33) on National Security Strategy for United States Government—Support Research and Development; DoD Instruction (DoDI) 1400.25, Volume 731, DoD Civilian Personnel Management System: Suitability and Fitness Adjudication for Civilian Employees; DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); DoD Manual 5200.02, Procedures for the DoD Personnel Security Program (PSP); Homeland Security Presidential Directive 12 (HSPD–12), Policy for a Common Identification Standard for Federal Employees and Contractors; Federal Information Processing Standard (FIPS) 201–2, Personal Identity Verification (PIV) of Federal Employees and Contractors; Army Regulation (AR) 380–5, Army Information Security Program; AR 380–10, Foreign Disclosure and Contacts with Foreign Representatives; AR 380–13, Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations; AR 380–28, Army Sensitive Compartmented Information Security Program; AR 380–49, Industrial Security Program; AR 380–53, Communications Security Monitoring; AR 380–67, Personnel Security Program; AR 380–381 Special Access Programs (SAPs) and Sensitive Activities; AR 381–45, Investigative Records Repository; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM:

This system of records supports the Department of Army's operational administration, management, accountability, and oversight of its security functions such as Information Security, Personnel Security, Industrial Security, Education and Awareness, Communications Security, Sensitive Compartmented Information, Research and Technology Protection, Special Access Programs (SAPs), and Foreign Disclosure and Security Screening and Vetting programs. This system will be used:

A. To comply with regulatory requirements related to initial and continued employment; to determine eligibility for access to Army information including Controlled Unclassified Information (CUI) and classified information, as well as information technology systems, facilities, research, technologies, or programs.

B. To support the Army's intelligence missions, including assessing the fitness of personnel applying for or selected for an Army award, such as a grant or cooperative agreement, or a legal agreement, such as a contract, and performing work for or on behalf of the U.S. Army.

C. To identify areas in personnel security, fitness, and military accessions field warranting more intense security screening; to conduct personnel security, vetting, and fitness pilots, projects, and programs.

D. To protect the agency's operations, data, personnel, facilities, and systems by using administrative, security, and investigative functions to detect actual or potential insider threats and security risks; to identify and initiate needed follow-on inquiries and/or investigative activity; to enable security professionals and Commanders to assess an individual's continued eligibility and access and take appropriate actions; to evaluate and improve Army personnel security, insider threat, and other personnel or security procedures, programs, and policies.

E. To support the conduct of security pilots and projects related to Army programs, with a focus on research and development.

F. To document training and education, to evaluate and improve Army personnel security, insider threat, and other personnel or security procedures, programs, and policies; to assist in providing training, instruction, and advice on security-related functions, and to conduct statistical analyses and track, report, and evaluate the effectiveness of Army Security programs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. Any individual affiliated with the U.S. Army by assignment, employment, or contractual relationship, as the result of an inter-service support agreement, or other form of affiliation, on whom a security screening and vetting request or check has been submitted, or an adjudication or determination has been completed or may be pending.

B. Family members, dependents, relatives, and individuals with a personal, professional, employment, or other association to an individual described above.

C. Individuals and entities with access to CUI or classified information, including contractors, government employees, military personnel, and other authorized persons.

D. Individuals, including government personnel, private-sector individuals, contractors, volunteers, and visitors, who have or are seeking access to Army facilities, installations, information, and systems, as well as those who may pose a potential threat to Army personnel, installations, operations or research, technology, and development programs and activities.

E. Individuals who support the Army by executing security functions and/or who utilizes technology to synchronize and normalize security-relevant data to improve security administration, management, performance, reporting, and mission readiness.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal information, including names (current, former, alias, and alternate names), social security number (SSN), DoD/ID number, biographical information (date and place of birth, contact information, biometric information, sex, race, addresses, telephone number, personal and work email addresses, family and dependent information, to include names of relatives, associates, and references with their contact information, citizenship information and travel information, immigration, and passport information and records, military records and discharge information, medical and mental health history, records related to drug and/or alcohol use, financial information, information from the Internal Revenue Service pertaining to tax returns, bureau of vital statistics records (*e.g.,* birth certificate, death certificate, marriage application and license), copies of identity source documents, credit reports, prior security clearance and investigative information, types and dates of DoD affiliation and separations, employing activity, current and former employment and

professional experience, position sensitivity, educational history (*e.g.,* degrees earned, institutions attended, conduct records), records, or academic experiences, security management office data, personnel security investigative basis, adjudicative actions and determinations, and corresponding dates, security clearance and investigative information eligibility status and access (*e.g.,* status, level(s), corresponding dates, and agencies that granted), self-reported information, adverse personnel information, eligibility recommendations or decisions made by an appellate authority, briefings and agreements (*e.g.,* inadvertent disclosure, North Atlantic Treaty Organization (NATO) non-disclosure agreements and execution dates, indoctrination date(s), level(s) of access granted, briefing/debriefing date(s) and reasons for briefing/debriefing, or other biographical information required or obtained during personnel vetting (*e.g.,* background investigation, continuous vetting, enhanced security screening and vetting), and/or information obtained through the administration of security functions.

B. Records of investigations, determinations, and adjudications conducted by investigative organizations including the including U.S. Office of Personnel Management (OPM), Federal Bureau of Investigation, and the Defense Counterintelligence and Security Agency.

C. Employment information, includes pre-/post-employment screening reports, including counterintelligence or security screening, military, accessions, applications or agreements for Army funding, linguist screening and vetting; appointment orders, employment activities and conduct information, personnel actions (adverse, remedial, or corrective), duty assignments and experience, background investigations results, continuous vetting, counter insider threat, counterintelligence screening, security incident resolution, or program access requests.

D. Information required through National (*e.g.,* Trusted Workforce, Security Executive Agent Directive), DoD, or Army policies, such as: insider threat-related information, security incidents/violations, user activity monitoring, internal misconduct investigations and disciplinary actions taken, self-reported information, third party information, and concerning behavior or conduct found in: Law Enforcement reports (final), Inspector General Reports of Investigation, and Equal Employment Opportunity violation.

E. Information detailing agency or Command investigation, such as Commander's inquiry, formal and informal investigations (*e.g.,* Army Regulation 15–6), administrative investigations, and security incident investigations including information or reports on incidents, infractions, violations, to include the potential compromise or unauthorized disclosure of CUI and/or classified information), records include type of investigation, tracking codes, and requesting officials' final determination and contact information.

F. Polygraph reports, polygraph charts, polygraph tapes, and recordings in other forms, and notes from polygraph interviews or activities related to polygraph interviews.

G. Biometric information including, but not limited to, images, fingerprints, voice samples and criminal and civil fingerprint history information.

H. Criminal information and investigative data, including records from local, state, military, Federal and foreign criminal records, local, state, military, Federal civil and criminal court records; judicial, and administrative proceedings, appeals, and local command investigations. Criminal intelligence or information about affiliation with known international criminal and/or terrorist organizations.

I. National Intelligence Agency Check records which includes information about known or suspected links to foreign government(s), foreign intelligence agencies, and/or international terrorist organizations.

J. Records concerning civil or administrative proceedings, (*e.g.,* bankruptcy, liens, records, civil lawsuits, Merit System Protection Board, appeals), including information contained in local, state, military, Federal, and foreign courts, and agency records.

K. Information furnished to or obtained by the Army, including other DoD components, Intelligence Community members, other federal government agencies, industry, and other agencies or organizations about individuals who may pose an insider threat. This information includes payroll information, travel vouchers, benefits, and performance evaluations; disciplinary files, training records, and records of law enforcement action, records of substance abuse and mental health records treatment; personal conduct records, including improper political activity and prohibited personnel practices, reports of harassment or discrimination, records of government telephone uses, including call logs and summaries of potential insider threats.

L. Information collected through user activity monitoring, such as information may include keystrokes, screen captures, and content transmitted via email, chat, and data import or export.

M. Information, data, (transiting or stored), in part or in combination, collected through network monitoring, cyber security, and information assurance, information security or any related activity conducted for network or information protection activities on DoD owned or operated systems, networks, endpoints, cloud infrastructure, and devices. This includes personnel usernames and aliases, levels of network access, audit data, information about and evidence of unauthorized use or misuse of information technology systems, logs of printer, copier, and facsimile machine use, and information pertaining to the accountability, safeguarding, and disposition of classified and CUI material.

N. U.S. and foreign finance and real estate information, including financial institutions names, account information and balances, real estate information, such as address, year of purchase and price, capital investment costs, lease or/rental information, asset information including year of lease or rental, monthly payments, deeds, lender/loan information and foreclosure history, information on owned and leased vehicles, boats, airplanes, and other U.S. and foreign assets that include type, make, model, and year, U.S. and foreign mortgage, loans, and liability information, including that consist of type of loan, names and addresses of creditors, original balance, monthly and year-end balance, monthly payments, and payment history, financial disclosure filings, information pertaining to U.S. and foreign affiliations, cooperate relationships, partnerships, and research collaboration, including sponsor, partner and affiliate information, and documents involved in academic or contractual solicitation.

O. Information pertaining to contracts, licenses, grants, and other government contracting activities. This includes data on pre-contract, post-contract, and continuous monitoring activities, as well as facility clearance records, foreign ownership or influence, and business identifiers listed on records relevant to contracts (including those contracts that are unclassified but may be considered sensitive due to insight they may provide into federal government activities in conjunction with data from other federal contracts),

as it pertains to all phases of the contract. Information also includes reviews and decisions made by the Committee on Foreign Investments in the United States, business identifiers, and other information related to industrial security.

P. Facility or installation access records, including entry badges or passes, badge issuance and expiration date, government sponsor, facility identification, vehicle, and permit data, and visitor information, to include dates and times of individual access to secure areas.

Q. Any information that may call into question an individual's suitability for federal employment, contractor fitness, trustworthiness, loyalty, or acceptability for access to CUI and/or classified information.

R. Publicly and commercially available information about or generated by an individual including public records, civil court records, licenses and filings, social media content, news articles, publications, streaming or broadcasted media, conferences and symposia, technical data, grey literature, and web blog information.

S. Name, date and place of birth, social security number, citizenship information, criminal history, and prior security clearance and investigative information for current and/or former spouse or cohabitant(s), the name and marriage information for current and/or former spouse(s), citizenship information, name, date, and place of birth, contact information (*e.g.,* phone numbers, email addresses), and address for relatives.

T. Foreign contact, affections, associates to include family members, friends or social contacts), travel, and activities information, including names of individuals known, dates, citizenship information, countries of residence, type and nature of contact. This includes travel records, such as destinations, travel dates, and purposes, as well as information on foreign financial interests, assets, and affiliations, including awards, honors, and positions held. Additionally, it includes passport and visa information, U.S. border crossings, and loyalty to the United States, and information on visits, authorized access, participation, sponsorship, affiliation, and/or employment with Army, financial interests, assets, benefits from foreign governments, foreign awards, honors, commendations, recognitions, or positions held, U.S. border crossings information, traveler data, trip information to include destination, travel dates, purpose), and other travel related records, passport and visa relevant information, association records, information on loyalty to the United States.

RECORD SOURCE CATEGORIES:

Records and information stored in this system of records are obtained from:

A. Individuals, interviews, and polygraphs.

B. Government databases and other DoD databases and component program offices, to include: Defense Enrollment Eligibility Reporting System, Defense Civilian Personnel Data System, Electronic Military Personnel Record System, DoD Insider Threat Management and Analysis Center and DoD Component Insider Threat Records System, DoD contractor databases, internal and external sources including counterintelligence and security databases and files, DoD component human resources databases and files, Office of the Chief Information Officer and information assurance databases and files.

C. DoD and Federal investigative or adjudicative facilities/organizations.

D. Federal, State, local, or tribal government entities, including information from criminal or civil investigations, courts, law enforcement agencies, agencies authorized to collect information concerning citizenship, probation officials, prison officials, information technology officials, and security representatives.

E. Publicly available information sources, commercial data providers (*e.g.,* credit reporting companies and online news sources), including commercially available subscription databases containing public records; past and present employers, personal references and associates, relatives, neighbors.

F. Information collected through user activity monitoring, government telephone usage records.

G. Inspector General reports of investigations, available U.S. Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.

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 to litigation.

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 and necessary 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 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 the Office of Personnel Management and other Government agencies responsible for conducting background investigations and continuous vetting to provide them with information relevant to their inquiries and investigations.

L. To the elements of the U.S. Intelligence Community as identified in E.O. 12333, as amended, for use in intelligence, counterintelligence, and/or security activities for the purpose of protecting the United States National Security.

M. To contractors whose employees require fitness determinations, or eligibility for access to classified national security information for the purpose of ensuring that the employer is appropriately informed about the status of the employee's application for a fitness determination.

N. To Original Classification or Declassification Authorities, to determine whether information obtained while processing the background investigation, is or should be classified.

O. A record from this system may be disclosed as a routine use outside the DoD or the U.S. Government for the purpose of counterintelligence, counterterrorism, and homeland defense activities authorized by U.S. Law or Executive Order or for the purpose of enforcing laws which protect the national security of the United States; this includes disclosure to Executive Branch Agency insider threat, counterintelligence, and counterterrorism officials to fulfill their responsibilities under applicable Federal law and policy, including but not limited to E.O. 12333, E.O. 13587, Sharing and Safeguarding of Classified Information, and the National Insider Threat Policy and Minimum Standards.

P. To any Federal, State, Tribal, local, territorial, foreign, multinational agency or task force, or any other entity or person, to include contractors, who support the Army by executing security functions, and/or who utilizes technology to synchronize and normalize security-relevant data to improve security administration, management, performance, reporting, and mission readiness.

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. The 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 SSN, DoD ID number, case control number, name, date of birth, state and/or country of birth, citizenship documentation, biometric data, passport number, employer name, or some combination thereof.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

A. System records are retained and disposed of according to Army records maintenance and disposition schedules and the requirements of the National Archives and Records Administration. Destruction of records will be by shredding, burning, or pulping for paper records; magnetic erasing for computerized records; purging digital files, or other means, as described in AR 380–5, and other applicable policy.

B. Unless otherwise prescribed in policy, decentralized segments of security files are either (1) destroyed upon termination of access, (2) destroyed 1 year from the individual's date of transfer or separation, or (3) forwarded to the gaining organization.

C. Historic (prior to 12 Dec 2012) personnel security investigations and adjudicative records of a routine nature are retained in the active file until no longer needed; retired to the U.S. Army Intelligence and Security Records Repository (AISRR) and retained for 15 years after last action reflected in the file. Files which contain derogatory information and/or resulted in adverse action(s) against the individual are destroyed after 25 years.

D. Records pertaining to counterintelligence polygraph examinations will be maintained in the active file until no longer needed and then disposed of after the final quality control review as follows: (1) for counterintelligence scope polygraph examinations, 90 days for favorably resolved cases or 15 years for other than favorably resolved cases, (2) for polygraph examinations conducted incident to a counterintelligence investigation, 35 years, and (3) for polygraph examinations of counterintelligence assets and human intelligence sources, material is transferred to the U.S. Army Investigative Records Repository, incorporated into an operational dossier, and disposed of 35 years from the date of the last action.

E. Original copy of signed Sensitive Compartmented Information Agreements will be sent the AISRR and destroyed when the record is 70 years old. Local Security professionals will retain a copy for one year after the individual departs the agency.

F. Records pertaining to information related to DoD and non-DoD affiliated persons and organizations, threating the security, or involving the disruption or subversion of DoD military and civilian personnel, function and activities, installations, information, communications, equipment and supplies, will be kept in a local security file for one year, then retired the United States AISRR, Fort Meade, MD, 20755–5995 for inclusion in the individual's/organization's dossier. Dossiers are maintained no longer than 15 years from date of last entry unless significant adverse information is present, in which case retention is 25 years. The AISRR will transfer records to the National Archives 25 years after the event.

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 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 using 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 to determine whether information about themselves is contained in this system of records should address written inquiries to the U.S. Intelligence and Security Command Freedom of Information and Privacy Act Office, 2600 Ernie Pyle Drive, Fort Meade, MD 20755–5995. Signed written requests should contain the requestor's full name (and any alias and/or alternate names used), SSN, DoD ID Number (if available), and date and place of birth. In addition, the requestor, must provide either a notarized statement or an unsworn 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).''

Note: Information generated, or authored, or compiled by another Government agency that is relevant to the purpose of the record may be incorporated into the record. In such instances, that information will be referred to the originating agency for direct response to the requestor or contact information and record access procedures for the other agency will be provided to the requestor.

CONTESTING RECORD PROCEDURES:

The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 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 should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Department of Defense has exempted records maintained in this system from subsections 5 U.S.C. 552a(c)(3); (d)(1), (2), (3), and (4); C(1), C(4)(G), (H), and (I); and (f) of the Privacy Act, pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(5). 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 system(s) of records from which they originated and claims any additional exemptions set forth here. 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), and (c), and published in 32 CFR part 310.

HISTORY:

February 22, 1993, 58 FR 10002

[FR Doc. 2026–01236 Filed 1–22–26; 8:45 am]

BILLING CODE 6001–FR–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD–2026–HA–0101]

Proposed Collection; Comment Request

AGENCY: The Office of the Assistant Secretary of Defense for Health Affairs (OASD(HA)), Department of Defense (DoD).

ACTION: 60-Day information collection notice.

SUMMARY: In compliance with the *Paperwork Reduction Act of 1995,* the Defense Health Agency (DHA) announces a proposed public information collection and seeks public comment on the provisions thereof. Comments are invited on: whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; the accuracy of the agency's estimate of the burden of the proposed information collection; ways to enhance the quality, utility, and clarity of the information to be collected; and ways to minimize the burden of the information collection on respondents, including through the use of automated collection techniques or other forms of information technology.

DATES: Consideration will be given to all comments received by March 24, 2026.

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

Federal eRulemaking Portal: http://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, Mailbox #24, Suite 05F16, Alexandria, VA 22350–1700.

Instructions: All submissions received must include the agency name, docket number and title 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 *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: To request more information on this proposed information collection or to obtain a copy of the proposal and associated collection instruments, please write to Defense Health Agency, 7700 Arlington Blvd., Falls Church, VA 22042, Amanda Grifka, 703–681–1771.

SUPPLEMENTARY INFORMATION:

Title; Associated Form; and OMB Number: Department of Defense Active Duty/Reserve Forces Dental Examination; DD Form 2813; OMB Control Number 0720–0022.

Needs and Uses: The information collection requirement is necessary to obtain and record the dental health status of members of the Armed Forces. This form is the means for civilian dentists to record the results of their findings and provide the information to the member's military organization. The military organizations are required by Department of Defense policy to track the dental status of its members.

Affected Public: Business or other for-profit institutions; individuals or households.

Annual Burden Hours: 37,500.

Number of Respondents: 150,000.

Responses per Respondent: 5.

Annual Responses: 750,000.