SYSTEM NAME AND NUMBER: Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System, DUSDI 01 DoD. (March 22, 2019; 84 FR 10803)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Primary location: Defense Security Service (DSS), 27130 Telegraph Rd., Quantico, VA 22134–2253. Secondary and Decentralized locations: Each of the DoD Components including the Departments of the Army, Air Force, and Navy and staffs, field operating agencies, major commands, installations, and activities. Official mailing addresses are published with each Component's compilation of systems of records notices.

SYSTEM MANAGER(S): Program Manager, Department of Defense Insider Threat Management and Analysis Center, Defense Security Service, 27130 Telegraph Road, Quantico, VA 22134–2253; email: dss.ncr.dss-ci.mbx.ditmac@mail.mil; phone: (571) 357–6850. DoD Components including the Departments of the Army, Air Force, and Navy and staffs, field operating agencies, major commands, installations, and activities. Official mailing addresses are published as an appendix to each Service's compilation of systems of records notices.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 137, Under Secretary of Defense for Intelligence; 44 U.S.C. 3554, Federal agency responsibilities; 44 U.S.C. 3557, National security systems; Public Law 112–81, Section 922, National Defense Authorization Act for Fiscal Year 2012 (NDAA for FY12), Insider Threat Detection (10 U.S.C. 2224 note); Public Law 113–66, Section 907(c)(4)(H) (NDAA for FY14), Personnel security (10 U.S.C. 1564 note); Public Law 114–92, Section 1086 (NDAA for FY16), 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 FY17), Enhanced security programs for Department of Defense personnel and innovation initiatives (10 U.S.C. 1564 note); E.O. 12829, as amended, National Industrial Security Program; E.O. 12968, as amended, Access to Classified Information; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information; E.O. 9397, as amended, Numbering System for Federal Accounts Relating to Individual Persons; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; Presidential Memorandum dated November 21, 2012, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; and DoD Directive 5205.16, The DoD Insider Threat Program; DoD Instruction 5205.83, DoD Insider Threat Management and Analysis Center (DITMAC), Directive-type Memorandum 09–012, Interim Policy Guidance for DoD Physical Access Control, as amended.

PURPOSE(S) OF THE SYSTEM: The DITMAC was established by the Under Secretary of Defense for Intelligence to consolidate and analyze insider threat information reported by DoD Component insider threat programs. The DoD maintains this system of records to assist with managing DoD Component insider threat programs and the DITMAC in accordance with Executive Order (E.O.) 13587 and Section 951 of the National Defense Authorization Act for Fiscal Year 2017 (NDAA for FY17). E.O. 13587 requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified networks and

the responsible sharing and safeguarding of classified information consistent with appropriate protections for privacy and civil liberties. Section 951 of the NDAA for FY17 requires DoD insider threat programs collect, store, and retain information from various data sources, including personnel security, physical security, information security, law enforcement, counterintelligence, user activity monitoring, information assurance, and other appropriate data sources to detect and mitigate potential insider threats.

Insider threats including espionage, terrorism, the unauthorized disclosure of national security information (including protected and sensitive information), and the loss or degradation of departmental resources or capabilities can damage the United States. The system will be used to analyze, monitor, and audit insider threat information for insider threat detection and mitigation within the DoD on persons eligible to access classified information and or hold a sensitive position. In addition, the system will monitor the insider threats from individuals with physical or logical access to a DoD installation or controlled information system via a Common Access Card (CAC) to DoD and U.S. Government installations, facilities, personnel, missions, or resources.

The system will support DoD Component insider threat programs, enable the identification of systemic insider threat issues and challenges and provide a basis for the development and recommendation of solutions to deter, detect, and/or mitigate potential insider threats. It will assist in identifying best practices among other Federal Government insider threat programs, through the use of existing DoD resources and functions and by leveraging existing authorities, policies, programs, systems, and architectures.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The following categories of individuals are covered: Individuals with or previously granted access to classified information or those currently or previously holding a sensitive position. These individuals include active and reserve component (including National Guard) military personnel; civilian employees (including non-appropriated fund employees); DoD contractor personnel, and officials or employees from Federal, state, local, tribal and private sector entities affiliated with or working with DoD and granted access to classified information by DoD or another authorized Federal agency based on an eligibility determination; individuals embedded with DoD units operating abroad eligible or previously eligible to access classified information or hold sensitive positions; active duty U.S. Coast Guard and mobilized retired military personnel, eligible or previously eligible for access to classified information or to hold sensitive positions (DoD and when operating with the military services or DoD Components) and limited access authorization grantees; individuals with an active DoD CAC for authenticating physical access to DoD installations or logical access to DoD controlled information systems; military family members and military retirees with active Uniformed Services ID cards; individuals with active DoD Civilian Retiree cards; individuals with an active identification card, pass or credential from a DoD organization used as proof of identification to gain physical or logical access to a DoD facility, network, system or program.

CATEGORIES OF RECORDS IN THE SYSTEM: Records from DoD Components and the DITMAC, including: Responses to information requested by official questionnaires and applications (e.g., SF 86 Questionnaire for National Security Positions, DD 1173, DD 1173–1, DD 2765, DD 1172–2 Application for Identification Card/DEERS Enrollment) including:

Individual's full name, former names and aliases; date and place of birth; Social Security Number (SSN); height and weight; hair and eye color; gender; ethnicity and race; biometric data; mother's maiden name; DoD identification number (DoD ID Number); current and former home and work addresses, phone numbers, and email addresses; employment history; military record information; branch of service; selective service registration record; education history and completed degrees; names of associates and references and their contact information; citizenship information; passport information; driver's license information; identifying numbers from access control passes or identification cards; alien registration number; criminal history; civil court actions; prior personnel security eligibility, investigative, and adjudicative information, including information collected through continuous evaluation; mental health history; records related to drug and/or alcohol use; financial record information; credit reports; the name, date and place of birth, social security number, and citizenship information for spouse and/ or cohabitant; the name and marriage information for current and former spouse(s); the citizenship, name, date and place of birth, and current address for relatives. Information on foreign contacts and activities; association records; information on loyalty to the United States; and other agency reports furnished to DoD or collected by DoD in connection with personnel security investigations, continuous evaluation for eligibility for access to classified information, and insider threat detection programs operated by DoD Components pursuant to Federal laws and Executive Orders and DoD regulations. These records can include, but are not limited to: Reports of personnel security investigations completed by investigative service providers (such as the Office of Personnel Management). Polygraph examination reports; nondisclosure agreements; document control registries; courier authorization requests; derivative classification unique identifiers; requests for access to sensitive compartmented information (SCI); facility access records; security violation files; travel records; foreign contact reports; briefing and debriefing statements for special programs, positions designated as sensitive, other information and documents required in connection with personnel security adjudications; and financial disclosure filings. DoD component information, summaries or reports, and full reports, about potential insider threats from: Payroll information, travel vouchers, benefits information, equal employment opportunity complaints, performance evaluations, disciplinary files (including information related to reports of misconduct or disciplinary actions and or considerations), information related to discharges, resignations, and retirements in lieu of court-martial for military members and information related to discharges, resignations, and retirements in lieu of disciplinary action for civilians, information related to disciplinary and administrative negotiations and settlements, training records, substance abuse and mental health records of individuals undergoing law enforcement action or presenting an identifiable imminent threat, counseling statements, outside work and activities requests, and personal contact records.

Particularly sensitive or protected information, including information held by special access programs, law enforcement, inspector general, or other investigative sources or programs. Access to such information may require additional approval by the senior DoD official responsible for managing and overseeing the program. Reports of investigation regarding security violations, including but not limited to: Statements, declarations, affidavits and correspondence; incident reports; investigative records of a criminal, civil or administrative nature; letters, emails, memoranda, and reports; exhibits and evidence; and, recommended remedial or corrective actions for security violations. Information, data (transiting or stored) and activity, in part or in combination collected through network monitoring, cyber defense, information security or any related activity conducted for network protection on DoD owned or

operated systems, networks, endpoints, cloud infrastructure, or devices. Information containing personnel user names and aliases, levels of network access, audit data, information regarding misuse of a DoD device, information regarding unauthorized use of removable media, and logs of printer, copier, and facsimile machine use; information collected through user activity monitoring, which is the technical capability to observe and record the actions and activities of all users, at any time, on a computer network controlled by DoD or a component thereof in order to deter, detect, and/or mitigate insider threats as well as to support authorized investigations. Such information may include key strokes, screen captures, and content transmitted via email, chat, or data import or export. DoD component summaries of reports, and full reports, about potential insider threats from records of government telephone system usage, including the telephone number initiating and receiving the call, and the date and time of the call; Information obtained from other Federal Government sources, such as information regarding U.S. border crossings and financial information obtained from the Financial Crimes Enforcement Network; Information specific to the management and operation of each DoD Component insider threat program, including information related to investigative or analytical efforts by DoD insider threat program personnel to identify threats to DoD personnel, property, facilities, and information, and information obtained from Intelligence Community members, the Federal Bureau of Investigation, or from other agencies or organizations about individuals known or suspected of engaging in conduct constituting, preparing for, aiding, or relating to an insider threat including, but not limited to espionage or unauthorized disclosure of classified national security information. Publicly available information, such as information regarding: Arrests and detentions; real property; bankruptcy; liens or holds on property; vehicles; licensure (including professional and pilot's licenses, firearms and explosive permits); business licenses and filings; Publicly available social media information, including electronic social media information published or broadcast for public consumption, available on request to the public, accessible online to the public, available to the public by subscription or purchase, or is otherwise lawfully accessible to the public. It includes social media information generally available to persons in a military community even though the military community is not open to the civilian general public. Publicly available social media information does not include information only accessible by logging into a private account of the individual about whom the record pertains or by requiring the individual to provide a password to social media information that is not publicly available. Workplace performance information, including performance management and appraisal reviews and other performance based measures. Information collected from the DoD Defense Performance Management and Appraisal Program, and information related to reports regarding harassment, discrimination, and drug testing violations or results, including but not limited to: Statements, declarations, affidavits and correspondence; incident reports; investigative records of a criminal, civil or administrative nature; letters, emails, memoranda, and reports; exhibits and evidence; and, recommended remedial or corrective actions. Information generated from Prevention, Assistance, and Response elements operating at DoD Installations: Information held by DoD operated education institutions, such as dean of students records, housing records, financial information, and other information maintained by an DoD educational institution. Information contained in, or developed from, the Department of Defense Identity Matching Engine for Security and Analysis. Information contained in physical access logs, to include visitor logs, at all DoD Facilities, information contained in a installations Carrier Appointment System, and information contained in, or developed from DoD Electronic Physical Access Control System.

RECORD SOURCE CATEGORIES: Individuals; DoD Component program offices including DoD contractor databases, internal and external sources including counterintelligence and security databases and files, personnel security databases and files, DoD component human resources databases and files, Office of the Chief Information Officer and information assurance databases and files, information collected through user activity monitoring, DoD telephone usage records, Federal, state, tribal, territorial, and local law enforcement and investigatory records, Inspector General records, available U.S. Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats, other Federal agencies, and publicly available information, including commercially available subscription databases containing public records.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to disclosures permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may be disclosed outside DoD as a routine use pursuant to 5 U.S.C. 552(b)(3) as follows:

a. To an appropriate federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or the issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DoD decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

b. To appropriate contractors, grantees, experts, consultants, companies, corporations and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, if the information is relevant and necessary to the entities' decision concerning the suitability, the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DoD decision concerning the suitability, the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person or entity making the request, determination, decision or judgment.

c. A record consisting of, or relating to, terrorism information, homeland security information, counterintelligence, or law enforcement information may be disclosed to a Federal, state, local, tribal, territorial, foreign government, multinational agency, and to a private sector agent either in response to its request, or upon the initiative of the DoD Component, for purposes of sharing such information as is necessary and relevant to the agency's investigations and inquiries related to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America as contemplated by the Intelligence Reform and Terrorism Protection Act of 2004.

d. To any person, organization or governmental entity (e.g., local governments, first responders, American Red Cross, etc.), in order to notify them of or respond to a serious and imminent terrorist or homeland security threat or natural or manmade disaster as is necessary and relevant for the purpose of guarding against or responding to such threat or disaster.

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

f. To officials and agencies of the Executive Branch of government, federal contractors and grantees, for purposes of conducting studies, research and analyses of insider threat programs or issues.

g. 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.

h. To designated officers and employees of Federal, State, local, territorial, tribal, international, or foreign agencies maintaining civil, criminal, enforcement, or other pertinent information, such as current licenses, if necessary to obtain information relevant and necessary to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

i. To foreign law enforcement, security, investigatory, or administrative 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.

j. To any agency, organization, or individual for the purposes of performing audit or oversight of the DoD Insider Threat Program as authorized by law and as necessary and relevant to such audit or oversight functions.

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

l. To third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the individual making the disclosure.

m. To a Federal agency or entity with possible information relevant to an allegation or investigation or was consulted regarding an insider threat for purposes of obtaining guidance, additional information, or advice from such Federal agency or entity regarding the handling of an insider threat matter.

n. To the news media or the general public, where the disclosure of factual information would be in the public interest and which would not constitute an unwarranted invasion of personal privacy.

o. To a Federal, state, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the Central Intelligence Act of 1949, as amended, E.O. 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.

p. 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.

q. To the Department of Justice for the purpose of representing the Department of Defense, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

r. 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.

s. 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.

t. 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.

u. 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.

v. 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 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained in paper and electronic storage media, in accordance with the safeguards mentioned below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Information in this system may be retrieved by name, SSN, and/or DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: System records are retained and disposed of according to DoD records maintenance and disposition schedules and the requirements of the National Archives and Records Administration (General Records Schedule 5.6: Security Records Transmittal No. 28 July 2017, item 210–240).

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: Military personnel, civilian employees, or contract security personnel guards protect information technology systems. Physical access to rooms maintaining information technology systems is controlled by combination lock and by identification badges only issued to authorized individuals. Electronic authorization and authentication of users is provided on a need-to-know basis and is required at all points prior to accessing system information. All data transfers and information retrievals using remote communication facilities require encryption. Paper records are maintained in safes and filing cabinets located in a secure area and only accessible by authorized personnel.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in the DITMAC system of record should address written inquires to the Defense Security Service, Office of FOIA and Privacy, 27130 Telegraph Road, Quantico, VA 22134–2253. Individuals seeking information about themselves contained in any specific DoD Component's insider threat program system of records should address written inquiries to the official mailing address for that Component, which is published with each Component's compilation of systems of records notices. DoD Component addresses are also listed at: http://dpcld.defense.gov/ Privacy/Privacy-Contacts/. Individuals seeking information about themselves contained in the DITMAC system of records originating in another DoD Component may be directed to the originating DoD Component maintaining the records. Individuals should provide their full name (and any alias and/or alternate name), SSN, and date and place of birth, and the address where the records are to be returned. 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 following format:

If executed outside of 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).''

Attorneys or other persons acting on behalf of an individual must provide written authorization from that individual for the representative to act on their behalf.

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records and for contesting or appealing agency determinations are published in DoD Regulation 5400.11; 32 CFR 310; or may be obtained from the Defense Privacy, Civil Liberties, and Transparency

Division, 4800 Mark Center Drive; ATTN: DPCLTD, Mailbox #24; Alexandria, VA 22350–1700.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in the DITMAC system of records should address written inquires to the Defense Security Service, Office of FOIA and Privacy, 27130 Telegraph Road, Quantico, VA 22134–2253. Individuals seeking to determine whether information about themselves is contained in any specific DoD Component's insider threat program system of records should address written inquiries to the official mailing address for that Component, which is published with each Component's compilation of systems of records notices. DoD Component addresses are also listed at: http://dpcld.defense.gov/ Privacy/Privacy-Contacts/. Signed, written requests must contain the full name (and any alias and/or alternate names used), SSN, and date and place of birth. 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 following format:

If executed outside of 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 has exempted records maintained in DUSDI 01-DoD, the ''Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System,'' from subsections (c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(1), (2), (4), (5), (6), (7). In addition, exempt records received from other systems of records in the course of DITMAC or Component record checks may, in turn, become part of the case records in this system. When records are exempt from disclosure in systems of records for record sources accessed by this system, DoD also claims the same exemptions for any copies of such records received by and stored in this system.

An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 310. For additional information contact the system manager.

HISTORY: March 21, 2018, 83 FR 12345; September 23, 2016, 81 FR 65631; May 19, 2016, 81 FR 31614.