Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2016-OS-0060]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to add a New System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to establish a new system of records, DUSDI 01-DoD, entitled the "Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System." This system has been established to enable DoD to implement the requirements of Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (October 7, 2011), and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (November 21, 2012). For purposes of this system of records, the term "insider threat" is defined in the Minimum Standards for Executive Branch Insider Threat Programs which were issued by the National Insider Threat Task Force based on directions provided in Section 6.3(b) of Executive Order 13587. The system will be used to analyze, monitor, and audit insider threat information for insider threat detection

and mitigation within DoD on threats that insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. The system will support the DITMAC and DoD Component insider threat programs, enable the identification of systemic insider threat issues and challenges, provide a basis for the development and recommendation of solutions to mitigate potential insider threats, and assist in identifying best practices amongst other Federal Government insider threat programs.

DATES: Comments will be accepted on or before [**INSERT 30-DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective the day following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: The public, OMB, and Congress are invited to submit any comments, identified by docket number and title, by any of the following methods:

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

* Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, 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 http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Cindy Allard, Director of the Defense Privacy, Civil Liberties, and Transparency Division, 703-571-0070.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. § 552a), as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at http://dpcld.defense.gov/. The proposed system report, as required by 5 U.S.C. § 552a(r) of the Privacy Act of 1974, as amended, was submitted on April 29, 2016, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: May 13, 2016.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of

Defense.

DUSDI 01-DoD

System name:

Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System

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.

Categories of individuals covered by the system:

Individuals covered by the system are those who had or have been granted eligibility for access to classified information or eligibility to hold a sensitive position, and who have exhibited

actual, probable, or possible indications of insider threat behaviors or activities. These individuals include active and reserve component (including National Guard) military personnel, civilian employees (including non-appropriated fund employees), and DoD contractor personnel; this includes officials or employees from Federal, state, Local, Tribal and Private Sector entities affiliated with or working with DoD who have been granted access to classified information by DoD based on an eligibility determination made by DoD or by another Federal agency authorized to do so.

Individuals or persons embedded with DoD units operating abroad who had or have been granted eligibility for access to classified information or eligibility to hold a sensitive positions, and who have exhibited actual, probable, or possible indications of insider threat behaviors or activities.

Current members of the U.S. Coast Guard and mobilized retired military personnel, when activated, who had or have been granted eligibility for access to classified information or eligibility to hold a sensitive positions by DoD and when operating with the military services or DoD Components, and Limited Access Authorization grantees, who have exhibited actual, probable, or possible indications of insider threat behaviors or activities.

Categories of records in the system:

Records containing information can be derived from:

Responses to information requested by official questionnaires (e.g., SF 86 Questionnaire for National Security Positions) that include: 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; current and former home and work addresses, phone numbers, and email addresses; employment history; military record information; selective service registration record; residential history; education history and degrees earned; names of associates and references with their contact information; citizenship information; passport information; driver's license information; identifying numbers from access control passes or identification cards; 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 or cohabitant; the name and marriage

information for current and former spouse(s); the citizenship, name, date and place of birth, and 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:

a. payroll information, travel vouchers, benefits information, credit reports, equal employment opportunity complaints, performance evaluations, disciplinary files, 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.

b. 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 who is responsible for managing and overseeing the program.

c. 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;

DoD Component information, summaries of reports, and full reports, about potential insider threats regarding: 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 usage of government telephone systems, including the telephone number initiating the call, the telephone number receiving the call, and the date and time of the call.

DoD Component information, summaries of reports, and full reports, about potential insider threats 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 related to the management and operation of DoD Component insider threat programs, including but not limited to: Information related to investigative or analytical efforts by DoD insider threat program personnel to identify threats to DoD personnel, property, facilities, and information; information obtained from Intelligence Community members, the Federal Bureau of Investigation, or from other agencies or organizations about individuals known or suspected of being engaged 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; and from social media.

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; Pub. L. 112-81, Section 922, National Defense Authorization Act for Fiscal Year 2012 (NDAA for FY12), Insider Threat Detection (10 USC § 2224 note); Pub. L 113-66, Section 907(c)(4)(H), (NDAA for FY14), Personnel security (10 U.S.C. § 1564 note); Pub. L. 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); 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, June 30, 2008; 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; National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs; and DoD Directive (DoDD) 5205.16, The DoD Insider Threat Program.

Purpose(s):

The Department of Defense proposes to establish a new system of records to assist in the management of the DITMAC Program and DoD Component insider threat programs. The DITMAC was established by the Undersecretary of Defense for Intelligence in order to consolidate and analyze insider threat information reported by the DoD Component insider threat programs mandated by Presidential Executive Order 13587, issued October 7, 2011, which required 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. The DITMAC helps prevent, deter, detect, and/or mitigate the potential threat that personnel, including DoD military personnel, civilian employees, and contractor personnel, who have or had been granted eligibility for access to classified information or eligibility to hold a sensitive position may harm the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. The system will be used to analyze, monitor, and audit insider

threat information for insider threat detection and mitigation within DoD on threats that persons who have or had been granted eligibility for access to classified information or eligibility to hold a sensitive position may pose 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, 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.

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:

Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether Federal, state, local, tribal, territorial, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

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 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.

To the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

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.

To any person, organization, or governmental entity in order to notify them of a serious terrorist threat for the purpose of guarding against or responding to such a threat.

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.

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 the DoD DITMAC system of records.

To Federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations that require information concerning the suitability or eligibility of an individual for a license.

To a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.

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.

To appropriate agencies, entities, and persons when (1) the Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Component's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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.

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

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

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.

To a Federal agency or entity that may have 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.

To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or(b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or(d) the United States Government is a party to litigation or has interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

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

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 CIA act of 1949 as emended, Executive Order 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.

Storage:

Paper and electronic storage media.

Retrievability:

Information in this system may be retrieved by name, SSN, and/or DoD identification number.

Safeguards:

IT systems are protected by military personnel, civilian employee, or contract security personnel guards. Physical access to rooms is controlled by combination lock and by identification badges that are issued only to authorized individuals. Electronic authorization and authentication of users is required at all points before any system information can be accessed. All data transfers and information retrievals that use remote communication facilities are required to be encrypted. Paper records are contained and stored in safes and filing cabinets that are located in a secure area with access only by authorized personnel.

Retention and disposal:

Disposition pending (until the National Archives and Records Administration (NARA) disposition schedule is approved, treat as permanent).

System manager(s) and address:

Department of Defense Insider Threat Management and Analysis Center, Assistant Director, Enterprise Tools and Architecture, Defense Security Service, 27130 Telegraph Road, Quantico, VA 22134-2253.

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.

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 PA, 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/PrivacyContacts.aspx

Signed, written requests must contain the full name (and any alias and/or alternate names used), SSN, and date and place of birth.

Record Access Procedures:
Individuals seeking information about themselves contained in the DITMAC system of record should address written inquires to the Defense Security Service, Office of FOIA and PA, 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/PrivacyContacts.aspx

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 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.

Record source categories:
Information in the system is received from DoD Components and program offices throughout DoD and DoD contractor databases, 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.

Exemptions claimed for the system:
The Department of Defense is exempting 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.

[FR Doc. 2016-11703 Filed: 5/18/2016 8:45 am; Publication Date: 5/19/2016]