

Request for Records Disposition Authority

Records Schedule Number **DAA-0446-2016-0001**
Schedule Status **Approved**

Agency or Establishment **Defense Security Service**
Record Group / Scheduling Group **Records of the Defense Security Service**
Records Schedule applies to **Agency-wide**
Schedule Subject **Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) Records System**

Internal agency concurrences will be provided **No**

Background Information **In accordance with the E.O 13467 the Department of Defense has established the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) to support implementation of a Department-wide insider threat detection and prevention program. The purpose of this information system is to: (1) analyze, monitor, and audit insider threat information for insider threat detection and mitigation within the DoD on threats that insiders may pose to DoD/U.S. government installations, facilities, personnel, missions or resources; (2) support DoD component insider threat programs; (3) 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 (4) assist in identifying best practices among other Federal Government Insider Threat Programs. In addition, the purpose of this information system is to: (1) perform research, development, and analyses. These analyses are conducted to: (a) evaluate and improve DoD and federal insider threat, and other information, personnel, and mission security procedures, programs, and policies; (b) assist in providing training, instruction, advice on insider threats, and assess continuing reliability of subjects for DoD Components and other elements of the federal government; (c) encourage cooperative research within and among DoD Components, the Intelligence Community, and the Executive branch on initiatives having DoD or Federal Government-wide implications in order to maximize integration and avoid duplication; (d) address items of special interest to information, personnel, and mission security officials within DoD Components, the Intelligence Community, and the Executive branch; (f) conduct insider threat advanced analytic tool and data pilot test projects.**

System Interfaces / Data Sources: Government data sources include, but are not limited to, Case Adjudication Tracking System (CATS), Joint Personnel Adjudication System (JPAS), FBI National Crime Information Center files, Defense Enrollment Eligibility Reporting System (DEERS); and non-governmental and commercial data sources such as National Law Enforcement Telecommunications System, TRSS, Equifax, and iMapData.

System Inputs: All information contained in the system interfaces and data sources above (e.g., name; DaB; PoB; SSN; physical attributes; gender; race; ethnicity; contact information; passport information; citizenship; current and previous addresses; reference information; education information; employment information (up to 10 years, includes performance information such as warnings, misconduct, and termination information); military history information; current and former spouse and cohabitant information; family information (immediate, in-laws, living or deceased); foreign contact information; foreign activities (including those of spouse, cohabitant or dependents), to include financial interests, business, professional activities, foreign government activities, travel; psychological and emotional health; police record information such as arrests, convictions, probation, criminal charges, imprisonment, and domestic violence; illegal use of drugs or controlled substances; alcohol consumption; financial information; inappropriate use of information technology systems; associations with terrorists; investigation packages: type of DoD affiliation; employing activity; current employment status; position sensitivity; personnel security investigative basis; status of current adjudicative action; security clearance eligibility and access status; whether eligibility determination was based on a condition, deviation from prescribed investigative standards or waiver of adjudication guidelines; reports of security-related incidents, to include issue files; suspension of eligibility and/or access; denial or revocation of eligibility and/or access; eligibility recommendations or decisions made by an appellate authority; non-disclosure execution dates; indoctrination date(s); level(s) of access granted; debriefing date(s); and reasons for debriefing; Wants and Warrants alerts and information; extradition limitations; incarceration information; court records; etc.,

Item Count

Number of Total Disposition Items	Number of Permanent Disposition Items	Number of Temporary Disposition Items	Number of Withdrawn Disposition Items
1	0	1	0

GAO Approval

Outline of Records Schedule Items for DAA-0446-2016-0001

Sequence Number	
1	Department of Defense (DoD) Insider Threat Management and Analysis Center (DI TMAC) system Disposition Authority Number: DAA-0446-2016-0001-0001

Records Schedule Items

Sequence Number	
1	<p>Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) system</p> <p>Disposition Authority Number DAA-0446-2016-0001-0001</p> <p>DITMAC records consist of information aggregated on current DoD-affiliated personnel in support of DoD Component insider threat programs. The master files include, but are not limited to: name; DoB; PoB; SSN; physical attributes; gender; race; ethnicity; contact information; passport information; citizenship; current and previous addresses; reference information; education information; employment information (up to 10 years, includes performance information such as warnings, misconduct, and termination information); military history information; publicly available electronic information.</p> <p>Final Disposition Temporary</p> <p>Item Status Active</p> <p>Is this item media neutral? Yes</p> <p>Do any of the records covered by this item currently exist in electronic format(s) other than e-mail and word processing? Yes</p> <p>Do any of the records covered by this item exist as structured electronic data? Yes</p> <p>Disposition Instruction</p> <p>Cutoff Instruction Cutoff is after investigative closing or date of the most recent investigative or operational activity.</p> <p>Retention Period Destroy after 25 years from the date of closing or the date of the most recent investigative or operational activity, whichever is later.</p> <p>Additional Information</p> <p>GAO Approval Not Required</p>

Agency Certification

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal in this schedule are not now needed for the business of the agency or will not be needed after the retention periods specified.

Signatory Information

Date	Action	By	Title	Organization
03/05/2018	Certify	Ron White	Records Manager	DOD - OSD
06/05/2018	Submit for Concurrency	Steven Rhodes	Senior Appraisal Archivist	National Archives and Records Administration - Records Management Services
06/06/2018	Concur	Sebastian Welch	Supervisory Archives Specialist	National Archives and Records Administration - ACR4
06/14/2018	Concur	Margaret Hawkins	Director of Records Management Services	National Records Management Program - ACNR Records Management Services
06/15/2018	Approve	David Ferriero	Archivist of the United States	Office of the Archivist - Office of the Archivist