BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 310

[Docket ID: DOD-2016-OS-0059]

Privacy Act of 1974; Implementation

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Final rule.

SUMMARY: The Office of the Secretary of Defense is exempting records maintained in DUSDI 01-DoD, "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); and (g) of the Privacy Act.

In addition, in the course of carrying out collections and analysis of information in connection with the operations of the DITMAC and DoD Component insider threat programs, exempt records received from other systems of records may become part of this system. To the extent that copies of exempt records from those other systems of records are maintained in this system, the Department also claims the same exemptions for the records from those other

systems that are maintained in this system, as claimed for the original primary system of which they are a part.

DATES: Effective Date: This rule is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTGER].

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

SUPPLEMENTARY INFORMATION:

BACKGROUND

The DITMAC was established by the Under Secretary 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. For purposes of this system of records, the term "insider threat" is defined in the Minimum Standards for Executive Branch Insider Threat Task Force based on direction provided in Section 6.3(b) of Executive Order 13587. 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 of records 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 sensitive positions may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. The system of records will support the DITMAC and 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.

PUBLIC COMMENTS

The Department of Defense published a proposed Privacy Act exemption rule for its Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records Systems (hereafter Insider Threat) on May 19, 2016 (81 FR 31561). The Department of Defense received comments from seven submitters related to a proposed Federal Rulemaking (docket: DOD-2016-OS-0059, published May 19, 2016) relating to a Privacy Act exemption rule for the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System (hereafter Insider Threat). In addressing comments submitted to this proposed Privacy Act exemption rule, the Department notes that such rules do not mandate exemptions in every instance, and are not intended to apply to all records, but must be reviewed in each specific case. Two commenters were opposed to the proposed exemption rule but did not provide specific concerns; an additional commenter provided a number of proposals for the Insider Threat program at large, as well as one addressing an access concern which is addressed in the access discussion.

The largest number of comments related to the proposed exemption from the access provisions of the Privacy Act (5 U.S.C. § 552a(d)(1), (2), (3), and (4)). The Department notes that the specific exemptions upon which the access limitation is based are generally predicated on "the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence" found in 5 U.S.C. § 552a(k)(2), (5), and (7). One of these commenters raised concerns that the "largest and most common sources providing information to the DITMAC provide such information under a general promise of confidentiality." It is not clear to the Department which sources the commenter believes are providing information under a general promise of confidentiality, but the language used in exemptions (k)(2), (5), and (7) requires an "express promise" (if promised after the Act took effect). This is normally done on a case-by-case basis. One commenter noted that "it is important to allow people as much access as possible to the data being collected about them, so that they can make informed decisions about what to do in the event of a data loss." In response, the Department anticipates providing access rights, except in those specific cases where an exemption rule would appropriately

apply. In view of the earlier discussion in this paragraph, DoD anticipates exercising access exemption rules as the exception rather than the norm.

Another commenter was also particularly concerned that "it would become entirely possible that qualified Soldiers might unknowingly become flagged as non-promotable for being a possible insider threat." We note first that when exercising the (k)(7) exemption, the Department uses reasonable segregability to provide the maximum amount of the record to the subject while honoring the express promise of confidentiality to the source. Moreover, the Department notes that the Insider Threat system of records is not a source of information for the promotion selection process.

Several comments also addressed the proposed exemption from the amendment provisions of the Privacy Act. The Insider Threat Hubs will aggregate information from a number of sources, the first of which is the subject of the record. Since the subjects of Insider Threat records are cleared personnel, the most appropriate place for them to address a factual error is with the appropriate DoD source (e.g., human resources offices for human resources records or the security officer for personnel security concerns). Insider Threat records are updated at scheduled intervals or upon a

specified query for current information and validated prior to any investigative or administrative action taken by a DoD Component.

One commenter noted that the collections and proposed exemptions asserted by the Department of Defense were overly extensive and would diminish accountability:

> DoD claims the authority to collect any information it wants without disclosing where it came from or even acknowledging its existence. The net result of these exemptions, coupled with DoD's proposal to collect and retain virtually unlimited information unrelated to any purpose Congress delegated to the agency, would be to diminish the legal accountability of the agency's information collection activities.

In response, disclosure could interfere with or reveal information relating to actual or potential criminal, civil, or administrative investigations or actions. DoD further notes that it identified the varied sources of Insider Threat information in the System of Records Notice and has asserted exemptions to protect from disclosure sources expressly promised confidentiality (pursuant to 5 U.S.C. § 552a(k)(2), (5), and (7) as discussed above). Such promises apply to a relatively narrow scope of DoD

records. If DoD were not able to provide such promises on a case-by-case basis, they would find it difficult, if not impossible, to gather candid information that is not generally known, precisely the type of information needed to make well-informed assessments of behavior (and potential behavior) to identify and address insider threats. As previously mentioned, exemption rules do not mandate the application of exemptions in every instance, are not intended to apply to all records, and will be applied on a case-by-case basis.

The commenter claims that DoD "contemplates collecting information that will not be relevant or necessary to a specific investigation" and that "the inability to determine, in advance, whether information is accurate, relevant, timely, and complete precludes its agents from complying with the obligation to ensure that the information meets these criteria after it is stored." In response, the Department notes that it is implementing an insider threat program required by Executive Order as well as by Public Law (e.g., Public Law 112-81, Title IX, Section 922, (10 U.S.C. § 2224 note), Insider Threat Detection). The statutory note requires the use of anomaly detection techniques, which logically require ingestion of non-anomalous information in order to identify anomalous

information. Further, the purpose of the Insider Threat program is to identify potential insider threat behavior; cases of concern are referred to the appropriate DoD or Federal investigative entity. DoD takes seriously its requirement under the Privacy Act to "balance the Government's need to maintain information about individuals with the rights of those individuals to be protected from unwarranted invasions of their privacy."

There were no comments related to the exemption of the access provisions through (k)(1), pertaining to classified information; (k)(4), applicable to records required by statute to be maintained and used solely as statistical records; or (k)(6), testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process. The Department also asserted an access exemption under (j)(2), which addresses law enforcement activities, which did not receive comment.

DoD made no changes to the regulatory text of the rule based on public comments received.

REGULATORY PROCEDURES

Executive Order 12866, "Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review"

It has been determined that this rule is not a significant rule. This rule does not (1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive orders.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C Chapter 6)

It has been certified that this rule does not have a significant economic impact on a substantial number of small entities because it is concerned only with the

administration of Privacy Act systems of records within DoD. A Regulatory Flexibility Analysis is not required.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

It has been determined that this rule does not impose additional information collection requirements on the public under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

Section 202, Public Law 104-4, "Unfunded Mandates Reform Act"

It has been determined that this rule does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million or more and that it will not significantly or uniquely affect small governments.

Executive Order 13132, "Federalism"

It has been determined that this rule does not have federalism implications. This rule does not have substantial direct effects on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

List of Subjects in 32 CFR Part 310

Privacy.

Accordingly, 32 CFR part 310 is amended as follows:

PART 310 [Amended]

1. The authority citation for 32 CFR part 310 continues to read as follows:

Authority: 5 U.S.C. 552a.

§§310.30 through 310.53 [Redesignated as §§310.31 through 310.54]

2. Redesignate §310.30 through §310.53 as §310.31 through §310.54.

3. In Subpart F, add a new §310.30 to read as follows:

§310.30 DoD-wide exemptions.

(a) Use of *DoD-wide exemptions*. DoD-wide exemptions for DOD-wide systems of records are established pursuant to 5 U.S.C. 552a(j) and (k) of the Privacy Act.

(b) *Promises of confidentiality.* (1) Only the identity of sources that have been given an express promise of confidentiality may be protected from disclosure under paragraphs (d)(3)(i), (ii), and (iii) and (d)(4) of this section. However, the identity of sources who were given implied promises of confidentiality in inquiries conducted before September 27, 1975, also may be protected from disclosure.

(2) Ensure promises of confidentiality are not automatically given but are used sparingly. Establish appropriate procedures and identify fully categories of individuals who may make such promises. Promises of confidentiality shall be made only when they are essential to obtain the information sought (see 5 CFR part 736).

(c) *Access to records for which DOD-wide exemptions are claimed.* Deny the individual access only to those portions of the records for which the claimed exemption applies.

(d) *DoD-wide exemptions*. The following exemptions are applicable to all components of the Department of Defense for the following system(s) of records:

(1) *System identifier and name:* DUSDI 01-DoD "Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System." Exemption: This system of records is exempted from subsections (c)(3) and (4); (d)(1), (2), (3) and (4); (e)(1),(2),(3),(4)(G)(H) and (I),(5) and (8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j) (2) and (k)(1), (2), (4), (5), (6), and (7).

(2) Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent that such provisions have been identified and an exemption claimed for the record and the

purposes underlying the exemption for the record pertain to the record.

(3) Exemption from the particular subsections is justified for the following reasons:

(i) *Subsection (c)(3).* To provide the subject with an accounting of disclosures of records in this system could inform that individual of the existence, nature, or scope of an actual or potential law enforcement or counterintelligence investigation, and thereby seriously impede law enforcement or counterintelligence efforts by permitting the record subject and other persons to whom he might disclose the records to avoid criminal penalties, civil remedies, or counterintelligence measures. Access to the accounting of disclosures could also interfere with a civil or administrative action or investigation which may impede those actions or investigations. Access also could reveal the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations.

(ii) *Subsection (c)(4).* This subsection is inapplicable to the extent that an exemption is being claimed for subsection (d).

(iii) *Subsection (d)(1).* Disclosure of records in the system could reveal the identity of confidential sources

and result in an unwarranted invasion of the privacy of others. Disclosure may also reveal information relating to actual or potential criminal investigations. Disclosure of classified national security information would cause damage to the national security of the United States. Disclosure could also interfere with a civil or administrative action or investigation; reveal the identity of confidential sources incident to Federal employment, military service, contract, and security clearance determinations; and reveal the confidentiality and integrity of Federal testing materials and evaluation materials used for military promotions when furnished by a confidential source.

(iv) *Subsection (d)(2).* Amendment of the records could interfere with ongoing criminal or civil law enforcement proceedings and impose an impossible administrative burden by requiring investigations to be continuously reinvestigated.

(v) *Subsections (d)(3) and (4).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(vi) *Subsection (e)(1).* It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement and

counterintelligence, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(vii) *Subsection (e)(2).* To collect information from the subject individual could serve notice that he or she is the subject of a criminal investigation and thereby present a serious impediment to such investigations.

(viii) *Subsection (e)(3).* To inform individuals as required by this subsection could reveal the existence of a criminal investigation and compromise investigative efforts.

(ix) *Subsection (e)(4)(G), (H), and (I).* These subsections are inapplicable to the extent exemption is claimed from (d)(1) and (2).

(x) *Subsection (e)(5).* It is often impossible to determine in advance if investigatory records contained in this system are accurate, relevant, timely and complete, but, in the interests of effective law enforcement, it is necessary to retain this information to aid in establishing patterns of activity and provide investigative leads.

(xi) *Subsection (e)(8).* To serve notice could give persons sufficient warning to evade investigative efforts.

(xii) *Subsection (g).* This subsection is inapplicable to the extent that the system is exempt from other specific subsections of the Privacy Act.

(4) In addition, in the course of carrying out analysis for insider threats, exempt records from other systems of records may in turn become part of the case records maintained in this system. To the extent that copies of exempt records from those other systems of records are maintained into this system, the DoD claims the same exemptions for the records from those other systems that are entered into this system, as claimed for the original primary system of which they are a part.

Dated: October 5, 2016.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

[FR Doc. 2016-24536 Filed: 10/14/2016 8:45 am; Publication Date: 10/17/2016]