BILLING CODE: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD-2016-OS-0063]

32 CFR Part 311

Privacy Act of 1974; Implementation

AGENCY: Office of the Secretary, DoD.

ACTION: Direct final rule.

SUMMARY: The Office of the Secretary of Defense is exempting those records contained in DMDC 24 DoD, entitled "Defense Information System for Security (DISS)," when investigatory material is compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that such material would reveal the identity of a confidential source.

This direct final rule establishes a new exemption to the Office of the Secretary Privacy Program. The Defense Information System for Security is the new DoD enterprise-wide information system for personnel security; it provides a common, comprehensive medium to request, record, document, and identify personnel security actions within the Department including: determinations of eligibility and

access to classified information, national security, suitability and/or fitness for employment, and HSPD-12 determination for Personal Identity Verification (PIV) to access government facilities and systems, submitting adverse information, verification of investigation and or adjudicative status, support of continuous evaluation and insider threat detection, prevention, and mitigation activities. DISS consists of two applications, the Case Adjudication Tracking system (CATS) and the Joint Verification System (JVS). CATS is used by the DoD Adjudicative Community for the purpose of recording eligibility determinations. JVS is used by DoD Security Managers and Industry Facility Security Officers for the purpose of verifying eligibility, recording access determinations, submitting incidents for subsequent adjudication, and visit requests from the field (worldwide). The records may also be used as a management tool for statistical analyses, tracking, reporting, evaluating program effectiveness, and conducting research. This direct final rule is consistent with the rule currently published regarding DMDC 11, Investigative Records Repository.

DATES: The rule is effective on [INSERT DATE 90 DAYS AFTER THE DATE OF PUBLICATION IN FEDERAL REGISTER] unless adverse

comments are received by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. If adverse comment is received, the Department of Defense will publish a timely withdrawal of the rule in the Federal Register.

ADDRESSES: You may submit 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 for 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: Mrs. Luz D. Ortiz, 571-372-0478.

SUPPLEMENTARY INFORMATION:

This rule is being published as a direct final rule as the Department of Defense does not expect to receive any adverse comments, and so a proposed rule is unnecessary.

Direct Final Rule and Significant Adverse Comments

DoD has determined this rulemaking meets the criteria for a direct final rule because it involves non-substantive changes dealing with DoD's management of its Privacy Programs. DoD expects no opposition to the changes and no significant adverse comments. However, if DoD receives a significant adverse comment, the Department will withdraw this direct final rule by publishing a notice in the Federal Register. A significant adverse comment is one that explains: (1) Why the direct final rule is inappropriate, including challenges to the rule's underlying premise or approach; or (2) why the direct final rule will be ineffective or unacceptable without a change. In determining whether a comment necessitates withdrawal of this direct final rule, DoD will consider whether it warrants a substantive response in a notice and comment process.

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

It has been determined that Privacy Act rules for the Department of Defense are not significant rules. The rules do 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 determined that this Privacy Act rule for the Department of Defense does not have 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 the Department of Defense. A Regulatory Flexibility Analysis is not required.

Public Law 95-511, "Paperwork Reduction Act" (44 U.S.C.

Chapter 35)

It has been determined that this Privacy Act rule for the Department of Defense imposes no additional information requirements beyond the Department of Defense and that the information collected within the Department of Defense is necessary and consistent with 5 U.S.C. 552a, known as the Privacy Act of 1074.

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

It has been determined that this Privacy Act rule for the Department of Defense 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 this rulemaking will not significantly or uniquely affect small governments.

Executive Order 13132, "Federalism"

It has been determined that this Privacy Act rule for the Department of Defense 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. Therefore, no Federalism assessment is required.

List of Subjects in 32 CFR Part 311

Privacy.

Accordingly, 32 CFR part 311 is amended as follows:

PART 311-OFFICE OF THE SECRETARY OF DEFENSE AND JOINT STAFF PRIVACY PROGRAM

1. The authority citation for 32 CFR part 311 continues to read as follows:

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

2. Section 311.8 is amended by adding paragraph (c)(27) to read as follows:

§311.8 Procedures for exemptions.

* * * * *

(c) * * *

(27) System identifier and name: DMDC 24 DoD, Defense Information System for Security (DISS).

(i) Exemption: Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5), but only to the extent that such material would reveal the identity of a confidential source.

(ii) Authority: 5 U.S.C. 552a(k)(5).

(iii) Reasons: (A) from subsections (c)(3) and (d) when access to accounting disclosure and access to or amendment of records would cause the identity of a confidential source to be revealed. Disclosure of the source's identity not only will result in the Department breaching the promise of confidentiality made to the source but it will impair the Department's future ability to compile investigatory material for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, Federal contracts, or access to classified information. Unless sources can be assured that a promise of confidentiality will be honored, they will be less likely to provide information considered essential to the Department in making the required determinations. (B) From subsection (e)(1) because in the collection of information for investigatory purposes, it is not always possible to determine the relevance and necessity of particular information in the early stages of the investigation. It is only after the information is evaluated in light of other information that its relevance and necessity becomes clear. Such information permits more informed decision-making by the Department when making

required suitability, eligibility, and qualification determinations.

Dated: May 24, 2016.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

[FR Doc. 2016-14183 Filed: 6/14/2016 8:45 am; Publication Date: 6/15/2016]