Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2014-OS-0024]

32 CFR Part 311

Privacy Act; Implementation

AGENCY: Office of the Secretary, DoD.

ACTION: Final rule.

SUMMARY: The Office of the Secretary of Defense (OSD) is amending its regulations to exempt portions of a system of records from certain provisions of the Privacy Act. Specifically, the Department proposes to exempt portions of DMDC 16 DoD, entitled "Identity Management Engine for Security and Analysis (IMESA)" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. In 2008, the U.S. Congress passed legislation that obligated the Secretary of Defense to develop access standards for visitors applicable to all military installations in the U.S. The Department of Defense (DoD) developed a visitor system to manage multiple databases that are capable of identifying individuals seeking access to DoD installations who may be criminal and/or security threats. The purpose of the vetting system is to screen individuals wishing to enter a

DoD facility, to include those who have been previously given authority to access DoD installations, against the FBI National Crime Information Center (NCIC) Wanted Person File. The NCIC has a properly documented exemption rule and to the extent that portions of these exempt records may become part of IMESA, OSD hereby claims the same exemptions for the records as claimed at their source (JUSTICE/FBI-001, National Crime Information Center (NCIC)).

DATES: Effective Date: This rule is effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Ms. Cindy Allard, (571) 372-0461.

SUPPLEMENTARY INFORMATION:

The proposed rule was published in the Federal Register on February 27, 2014 (79 FR 11048-11050, Docket ID: DoD-2014-OS-0024). One comment was received. The writer raised a number of personal concerns (issues with neighbor, banking, and family). The issues identified have no relevance to the proposed exemption of the Identity Management Engine for Security and Analysis (IMESA) from portions of the Privacy Act.

Additionally, the title of the system has been changed from Interoperability Layer Service (IoLS) to

Identity Management Engine for Security and Analysis (IMESA). This title change is reflected in the final rule.

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 determined that this rule 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)

This rule does not contain any information collection requirements subject to 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 will not significantly or uniquely affect small governments.

Executive Order 13132, "Federalism"

Executive Order 13132 requires regulations be reviewed for Federalism effects on the institutional interest of states and local governments, and if the effects are sufficiently substantial, preparation of the Federal assessment is required to assist senior policy makers. The amendments will not have any substantial direct effects on state and

local governments within the meaning of the EO. Therefore, no Federalism assessment is required.

List of Subjects in 32 CFR Part 311

Privacy.

Accordingly, 32 CFR part 311 is amended to read as follows:

PART 311—[AMENDED]

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)(26) as follows:

§311.8 Procedures for exemptions.

* * * * *

(c) * * *

(26) System identifier and name: DMDC 16 DoD, Identity Management Engine for Security and Analysis (IMESA).

(i) Exemption: To the extent that copies of exempt records from JUSTICE/FBI-001, National Crime Information Center (NCIC) are entered into the Interoperability Layer Service records, the OSD hereby claims the same exemptions, (j)(2) and (k)(3), for the records as claimed in JUSTICE/FBI-001, National Crime Information Center (NCIC). Pursuant to 5 U.S.C. 552a portions of this system that fall within (j)(2) and (k)(3) are exempt from the following

provisions of 5 U.S.C. 552a, section (c)(3) and (4); (d); (e)(1) through (3); (e)(4)(G) through (I); (e)(5) and (8); (f); and (g) (as applicable) of the Act.

(ii) Authority: 5 U.S.C. 552a(j)(2) and (k)(3).

(iii) Reasons: (A) from subsection (c)(3) because making available to a record subject the accounting of disclosure from records concerning him or her would specifically reveal any investigative interest in the individual. Revealing this information could reasonably be expected to compromise ongoing efforts to investigate a known or suspected terrorist by notifying the record subject that he or she is under investigation. This information could also permit the record subject to take measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(B) From subsection (c)(4) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(C) From subsection (d) because these provisions concern individual access to and amendment of certain records contained in this system, including law enforcement, counterterrorism, investigatory, and intelligence records. Compliance with these provisions could alert the subject of

an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of these records would interfere with ongoing counterterrorism, law enforcement, or intelligence investigations and analysis activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(D) From subsection (e)(1) because it is not always possible to determine what information is relevant and necessary to complete an identity comparison between the individual seeking access and a known or suspected terrorist. Also, because DoD and other agencies may not

always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response.

(E) From subsection (e)(2) because application of this provision could present a serious impediment to counterterrorism, law enforcement, or intelligence efforts in that it would put the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct designed to frustrate or impede that activity. The nature of counterterrorism, law enforcement, or intelligence investigations is such that vital information about an individual frequently can be obtained only from other persons who are familiar with such individual and his/her activities. In such investigations, it is not feasible to rely upon information furnished by the individual concerning his own activities.

(F) From subsection (e)(3) to the extent that this subsection is interpreted to require DoD to provide notice to an individual if DoD or another agency receives or collects information about that individual during an investigation or from a third party. Should this subsection be so interpreted, exemption from this provision

is necessary to avoid impeding counterterrorism, law enforcement, or intelligence efforts by putting the subject of an investigation, study, or analysis on notice of that fact, thereby permitting the subject to engage in conduct intended to frustrate or impede the activity.

(G) From subsection (e)(4)(G),(e)(4)(H), and (e)(4)(I) (Agency Requirements) because portions of this system are exempt from the access and amendment provisions of subsection (d).

(H) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness could unfairly hamper law enforcement processes. It is the nature of law enforcement to uncover the commission of illegal acts at diverse stages. It is often impossible to determine initially what information is accurate, relevant, timely, and least of all complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further details are brought to light.

(I) From subsection (e)(8) because the requirement to serve notice on an individual when a record is disclosed under compulsory legal process could unfairly hamper law enforcement processes. It is the nature of law enforcement that there are instances where compliance with these

provisions could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of intelligence or law enforcement agencies; compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; reveal a sensitive investigative or intelligence technique; or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses.

(J) From subsection (f) because requiring the Agency to grant access to records and establishing agency rules for amendment of records would unfairly impede the agency's law enforcement mission. To require the confirmation or denial of the existence of a record pertaining to a requesting individual may in itself provide an answer to that individual relating to the existence of an on-going investigation. The investigation of possible unlawful activities would be jeopardized by agency rules requiring verification of the record, disclosure of the record to the subject, and record amendment procedures.

(K) From subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Dated: December 2, 2015.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2015-31868 Filed: 12/18/2015 8:45 am; Publication Date: 12/21/2015]