9110-9B

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 5

Docket No. DHS-2020-0032

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-038 Insider Threat Program System of Records

AGENCY: Department of Homeland Security.

ACTION: Final rule.

SUMMARY: The Department of Homeland Security (DHS) is issuing a final rule to amend its regulations to exempt portions of a newly updated system of records titled, "DHS/ALL-038 Insider Threat Program System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: This final rule is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: For privacy questions, please contact: Constantina Kozanas, (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of Homeland Security (DHS) published a notice of proposed rulemaking in the Federal Register, 85 FR 13831, March 10, 2020, proposing to exempt

portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. In concert with that rulemaking, DHS issued a modified system of records notice, "DHS/ALL-038 Insider Threat Program System of Records" in the Federal Register, 85 FR 13914, March 10, 2020, to the public (1) outlining that DHS is expanding the categories of individuals to *all* individuals who have or had access to the Department's facilities, information, equipment, networks, or systems; (2) to clarify that the categories of records in this SORN will be modified to cover records from any DHS Component, office, program, record, or source, including records from information security, personnel security, and systems security for both internal and external security threats; and (3) to clarify and expand several previously issued routine uses.

DHS invited comments on both the System of Records Notice (SORN) and Notice of Proposed Rulemaking (NPRM).

II. Public Comments

DHS received five comments on the NPRM and one comment on the SORN.

NPRM

DHS received four comments on the published NPRM regarding the collection of information by DHS generally, and not specific to the Insider Threat Program system of records. DHS received one comment on the published NPRM regarding DHS's proposed exemptions covered by the associated Insider Threat Program system of records. In short, the comment argues that DHS's proposed use of these exemptions would circumvent Privacy Act safeguards and contravene legislative intent by permitting DHS to collect records that are not relevant and necessary, failing to disclose its sources of records, and

preventing individuals from accessing and amending their records. DHS believes the explanations and justifications provided in the NPRM and this final rule fully support DHS's uses of these exemptions. In summary, DHS appreciates the public comments and strives to be transparent regarding all Insider Threat collections and uses. After consideration of the public comments, DHS has determined that the exemptions should remain in place and will implement the rulemaking as proposed.

SORN

DHS received one comment on the SORN proposing to (1) minimize the scope of information collected because of the surge of federal government data breaches and general cybersecurity weaknesses that allegedly federal agencies, including DHS, may incur as part of their systems; (2) exclude category of individuals and relevant personal associations, including those not under investigation by DHS; and (3) eliminate the use of routine uses that are incompatible with the purpose for which the data was collected, including those that relate to disclosures for: employment, licensing, and other benefit eligibility decisions; to the news media and public for a legitimate public interest; and to foreign entities. DHS appreciates the public comment and strives to be transparent regarding all Insider Threat collections. After consideration of the public comment, DHS has determined that the SORN should remain in place.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS proposes to amend Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 continues to read as follows:

Authority: 6 U.S.C. sec. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. sec. 301. Subpart A also issued under 5 U.S.C. sec. 552. Subpart B also issued under 5 U.S.C. sec. 552a.

2. In appendix C to part 5, revise paragraph "20" to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

20. The Department of Homeland Security (DHS)/ALL-038 Insider Threat Program System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ALL-038 Insider Threat Program System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities; and protection of the President of the U.S. or other individuals pursuant to Section 3056 and 3056A of Title 18. The DHS/ALL-038 Insider Threat Program System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. secs. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12); (f); and (g)(1). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. secs. 552a(k)(1), (k)(2), and (k)(5), has exempted this system from

the following provisions of the Privacy Act: 5 U.S.C. secs. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). Where a record received from another system has been exempted in that source system under 5 U.S.C. sec. 552a(j)(2), 5 U.S.C. secs. 552a(k)(1), (k)(2), and (k)(5), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. When an investigation has been completed, information on disclosures made may continue to be exempted if the fact that an investigation occurred remains sensitive after completion.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the

existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (e)(12) (Matching Agreements) because requiring DHS to provide notice of a new or revised matching agreement with a non-Federal agency, if one existed, would impair DHS operations by indicating which data elements and information are valuable to DHS's analytical functions, thereby

providing harmful disclosure of information to individuals who would seek to circumvent or interfere with DHS's missions.

(j) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

* * * * *

Constantina Kozanas,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2020-18857 Filed: 10/5/2020 8:45 am; Publication Date: 10/6/2020]