



## DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2015-0050]

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

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** The Department of Homeland Security (DHS) is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the “Department of Homeland Security/ALL-038 Insider Threat Program System of Records” and this proposed rulemaking. In this proposed rulemaking, the Department proposes 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.

**DATES:** Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit comments, identified by docket number DHS-2015-0050 or by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: Karen L. Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

**Instructions:** All submissions received must include the agency name and docket number for this document. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.

**Docket:** For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For questions please contact: Karen L. Neuman, (202-343-1717), Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

**SUPPLEMENTARY INFORMATION:**

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department proposes to establish a new DHS system of records titled “DHS/ALL-038 Insider Threat Program System of Records.”

DHS has created a Department-wide system, known as the Insider Threat Program system of records to manage insider threat matters within DHS. The Insider Threat Program was mandated by E.O. 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” issued October 7, 2011, which requires 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 with appropriate protections for privacy and civil liberties. Insider threats

include: attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Department and its personnel, facilities, resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information or technology; and indicators of potential insider threats. The Insider Threat Program system may include information from any DHS Component, office, program, record, or source, and includes records from information security, personnel security, and systems security for both internal and external security threats.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-038 Insider Threat Program system of records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS may share information with appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in the DHS ALL-038 system of records notice.

DHS is issuing this Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act. The system of records notice is published elsewhere in this Federal Register. This newly established system will be included in DHS's inventory of record systems.

## II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is

maintained in a “system of records.” A “system of records” is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/ALL-038 Insider Threat Program System of Records. Some information in DHS/ALL-038 Insider Threat Program System of Records relates to official DHS national security, law enforcement, and intelligence activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to: preclude subjects of these activities from frustrating these processes; avoid disclosure of insider threat techniques; protect the identities and physical safety of confidential informants and law enforcement personnel; ensure DHS’ ability to obtain information from third parties and other sources; protect the privacy of third parties; and safeguard classified information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, where compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

A notice of system of records DHS/ALL-038 Insider Threat Program System of Records is also published in this issue of the Federal Register.

**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:** Pub. L. 107-296, 116 Stat. 2135; (6 U.S.C. 101 et seq.); 5 U.S.C. 301.

Subpart A also issued under 5 U.S.C. 552. Subpart B also issued under 5 U.S.C. 552a.

2. In appendix C to part 5, add paragraph 74 to read as follows:

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

\* \* \* \* \*

74. The 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 System of Records is a repository of information held by DHS in connection with various missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; and national security and intelligence activities. 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. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 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), (g)(1), and (h). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 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. 552a(j)(2), 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 and 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 and 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 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.

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

Dated: February 18, 2016.

Karen L. Neuman,  
Chief Privacy Officer,  
Department of Homeland Security.

[FR Doc. 2016-03923 Filed: 2/25/2016 8:45 am; Publication Date: 2/26/2016]