epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974; Department of Homeland Security/ALL—038 Insider Threat Program System of Records

Notice of Privacy Act System of Records and Notice of Proposed Rulemaking

[Docket Nos. DHS-2015-0049 and 0050]

March 28, 2016

---

By notice published on February 26, 2016,[1] the Department of Homeland Security ("DHS") proposes to establish a new Privacy Act system of records titled "Department of Homeland Security/ALL—038 Insider Threat Program System of Records" ("Insider Threat Database" or "DHS Database"). The Database will include detailed, personal data on an unusually large number of individuals, including current and former DHS employees; all individuals who have access to DHS facilities, including visitors; family members, relatives, and associates of a person who may be subject to an investigation; witnesses and others who assist

[1] Notice of Privacy Act System of Records, 81 Fed. Reg. 9871 (proposed Feb. 26, 2016) [hereinafter "Insider Threat SORN"].

the agency with investigations; and visitors to DHS facilities. The scope of "insider threat" is broad and ambiguous; the extent of data collection is essentially unbounded.

By notice published on February 26, 2016,[2] DHS proposes to exempt the "Insider Threat" Database from several significant provisions of the Privacy Act of 1974. Pursuant to DHS's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) address the substantial privacy and security issues raised by the database; (2) narrow the scope of individuals included in the database; (3) recommend that DHS withdraw unlawful and unnecessary proposed routine use disclosures; and (4) urge DHS to significantly narrow the Privacy Act exemptions for its Database.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards, established by Congress, in the development of new information systems operated by the federal government.[3] EPIC also routinely interacts with DHS through

[2] Notice of Proposed Rulemaking, 81 Fed. Reg. 9789 (proposed Feb. 26, 2016) [hereinafter "Insider Threat NPRM"].

[3] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket No. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), *available at* https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf; Comments of EPIC to the Department of Homeland Security, Notice of Privacy Act System of Records, Docket No. DHS-2011-0094 (Dec. 23, 2011), *available at* http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), *available at* http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the United States Customs and Border Protection; Department of Homeland Security on the Establishment of Global Entry Program, Docket No. USCBP-2008-0097 (Jan. 19, 2010), *available at* http://epic.org/privacy/global_entry/EPIC-Comments-Global-Entry-2010.pdf.

formal meetings with the Privacy Office.[4] Thus, EPIC staff would be subject to the proposed database as currently envisioned.

### 1. Purpose and Scope of the "Insider Threat" Database

Executive Order 13587, titled "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," ordered federal agencies to create "insider threat detection and prevention program[s]" and "to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties."[5] According to DHS, the proposed "Insider Threat" Database would manage "insider threats within DHS" in accordance with E.O. 13587.[6] DHS provides a non-exhaustive list of "insider threats," which include, but are not limited to:

> Attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against DHS 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.[7]

The proposed database "may include information from any DHS Component, office, program, record, or source, and [may] include[] records from information security, personnel security, and systems security for both internal and external security threats."[8] DHS proposes to disclose information within the Database to "other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence,

[4] Most recently, an EPIC staff member attended a March 14, 2016 DHS meeting with public interest groups at a DHS facility in Virginia for a briefing on the Interim Privacy and Civil Liberties Guidelines for the Cybersecurity Information Sharing Act of 2015.
[5] Exec. Order No. 13,587, 76 Fed. Reg. 63,811 (Oct. 7, 2011). *See also* Insider Threat SORN at 9871-72.
[6] Insider Threat SORN at 9872.
[7] *Id*.
[8] *Id.*

or other homeland security functions."[9] And as discussed below in detail, DHS proposes to disclose sensitive, personal data within the database to multiple entities that are not subject to the Privacy Act: state, local, tribal, territorial, foreign, and international government agencies.[10]

According to the agency, the purpose(s) of the DHS Database is to:

> manage insider threat matters; facilitate insider threat investigations and activities associated with counterintelligence and counterespionage complaints, inquiries, and investigations; identify threats to DHS resources and information assets; track referrals of potential insider threats to internal and external partners; and provide statistical reports and meet other insider threat reporting requirements.[11]

### 2. The Proposed "Insider Threat" Database Would Maintain a Massive Amount of Personal, Sensitive Information About a Wide Variety of Individuals

#### *a. Categories of Records in the DHS Database Are Virtually Unlimited*

According to the Insider Threat SORN, the DHS Database will include an exorbitant amount of personal information about an expansive array of individuals. The Database would include: name, date of birth, social media account information, ethnicity and race, gender, medical reports, background reports that include medical and financial data, travel records, and information "provided by record subjects and individual members of the public."[12]

The DHS Database will specifically contain information derived from Standard Form 86, Questionnaire for National Security Positions (SF-86).[13] SF-86 is a 127-page form used to conduct background checks for federal employment in sensitive positions, a process the D.C. Circuit has described as "an extraordinarily intrusive process designed to uncover a vast array of information …."[14] SF-86 includes such personal and sensitive information as an individual's

---

[9] *Id.*
[10] *Id.*
[11] Insider Threat SORN at 9873.
[12] *Id*. at 9872-73.
[13] *Id*. at 9872.
[14] *Willner v. Thornburgh*, 928 F.2d 1185, 1191 (D.C. Cir. 1991).

name; date of birth; Social Security Number (SSN); address; social media activity; personal and official email addresses and phone numbers; citizenship, ethnicity and race; employment and educational history; passport, driver's license, and license plate numbers; medical reports; biometric data; photographic images, videotapes, and voice recordings; and "[i]nformation on family members, dependents, relatives, and other personal associations."[15]

The detailed sensitive information included in SF-86 was a focal point of the 2015 Office of Personnel Management (OPM) data breaches, which compromised the personal information of 21.5 million people, including 1.8 million people who did not apply for a background check.[16] The OPM breach exposed sensitive SF-86 forms spanning three decades.[17] The fingerprints of 5.6 million people were also stolen in the data breach.[18] This information could be used to blackmail government employees, expose the identities of foreign contacts, and cause serious damage to counterintelligence and national security efforts.[19]

The categories of records contained in the "Insider Threat" Database, including the data contained in SF-86 forms, represent a wealth of sensitive information that is typically afforded the highest degree of privacy and security protections, such as health,[20] financial,[21] and

[15] Insider Threat SORN at 9872.
[16] Dan Goodin, *Call it a "Data Rupture": Hack Hitting OPM Affects 21.5 Million*, ARSTECHNICA (July 9, 2015), http://arstechnica.com/security/2015/07/call-it-a-data-rupture-hack-hitting-opm-affects-21-5-million/.
[17] Andrea Shalal & Matt Spetalnick, *Data Hacked from U.S. Government Dates Back to 1985: U.S. Official*, REUTERS (June 5, 2015), http://www.reuters.com/article/us-cybersecurity-usa-idUSKBN0OL1V320150606.
[18] Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sep. 23 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.
[19] *See* Kim Zetter & Andy Greenberg, *Why the OPM Breach is Such a Security and Privacy Debacle*, WIRED (June 11, 2015), http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.
[20] *See* Heath Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C.).
[21] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered section of 12 and 15 U.S.C.).

education[22] records; Social Security Numbers;[23] and individuals' photographs or images.[24] Federal contractors, security experts, and EPIC have previously argued to the U.S. Supreme Court that much of this information simply should not be collected by the federal governments.

In *NASA v. Nelson*,[25] the Supreme Court considered whether federal contract employees have a Constitutional right to withhold personal information sought by the government in a background check. EPIC filed an amicus brief, signed by 27 technical experts and legal scholars, siding with the contractors employed by the Jet Propulsion Laboratory (JPL).[26] EPIC's brief highlighted problems with the Privacy Act, including the "routine use" exception, security breaches, and the agency's authority to carve out its own exceptions to the Act.[27] EPIC also argued that compelled collection of sensitive data would place at risk personal health information that is insufficiently protected by the agency.[28] The Supreme Court acknowledged that the background checks implicate "a privacy interest of Constitutional significance" but stopped short of limiting data collection by the agency, reasoning that the personal information would be protected under the Privacy Act.[29]

That turned out not to be true. Shortly after the Court's decision, NASA experienced a significant data breach that compromised the personal information of about 10,000 employees,

[22] *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012).
[23] *See* Driver's Privacy Protection Act, 18 U.S.C. § 2725(4) (defining "highly restricted personal information" to include "social security number").
[24] *Id*. § 2725(4) (defining "highly restricted personal information" to include "individual's photograph or image").
[25] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[26] Amicus Curiae Brief of EPIC, *Nat'l Aeronautics & Space Admin. v. Nelson*, No. 09-530 (S.Ct. Aug. 9, 2010), https://epic.org/amicus/nasavnelson/EPIC_amicus_NASA_final.pdf.
[27] *Id*. at 20-28
[28] *Id*.
[29] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).

including Robert Nelson, the JPL scientist who sued NASA over its data collection practices.[30] The JPL-NASA breach is a clear warning about why DHS should narrow the amount of sensitive data collected. Simply put, the government should not collect so much data; to do so unquestionably places people at risk.

Given the recent surge in government data breaches, the vast amount of sensitive information contained in the DHS Database faces significant risk of compromise. According to a recent report by the U.S. Government Accountability Office (GAO), "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[31] This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[32] Also in 2015, the Internal Revenue Service (IRS) reported that approximately 390,000 tax accounts were compromised, exposing Social Security Numbers, dates of birth, street addresses, and other sensitive information.[33] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[34]

Data breaches have directly impacted DHS information systems in recent years. For example, in 2014, a DHS contractor conducting background investigations for the agency experienced a data breach that compromised the records of at least 25,000 employees, including

[30] Natasha Singer, *Losing in Court, and to Laptop Thieves, in a Battle With NASA Over Private Data*, N.Y. TIMES (Nov. 28, 2012), http://www.nytimes.com/2012/11/29/technology/ex-nasa-scientists-data-fears-come-true.html.
[31] U.S. Gov't Accountability Office, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System* (Jan. 2016) http://www.gao.gov/assets/680/674829.pdf [hereinafter "GAO Cybersecurity Report"].
[32] GAO Cybersecurity Report at 8.
[33] *Id*. at 7-8.
[34] *Id*. at 8.

undercover investigators.[35] Last year, another DHS contractor suffered a data breach that affected as many as 390,000 people associated with DHS, including current and former employees as well as contractors and job applicants.[36] More recently, a 16-year-old teenage boy was arrested in connection with hacks that exposed the information of more than 20,000 Federal Bureau of Investigation (FBI) employees and 9,000 DHS employees, as well as the personal email accounts of DHS Secretary Jeh Johnson and Central Intelligence Agency (CIA) director John Brennan.[37] Overall, the number of government data breaches, including for DHS, has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[38]

The latest series of high-profile government data breaches indicates that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. Indeed, GAO recently released a report on widespread cybersecurity weaknesses throughout the executive branch, aptly titled "Federal Agencies Need to Better Protect Sensitive Data."[39] According to the report, a majority of federal agencies, "including the Department of Homeland Security, have weaknesses with the design and implementation of information security controls …."[40] In addition, most agencies "have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware."[41] The GAO report concluded that, due to widespread

[35] Jim Finkle & Mark Hosenball, *U.S. Undercover Investigators Among Those Exposed in Data Breach*, REUTERS (Aug. 22, 2014), http://www.reuters.com/article/us-usa-security-contractor-cyberattack-idUSKBN0GM1TZ20140822.
[36] Alicia A. Caldwell, *390,000 Homeland Employees May Have Had Data Breached*, ASSOCIATED PRESS (June 15, 2015), http://www.pbs.org/newshour/rundown/390000-homeland-employees-may-have-had-data-breached/.
[37] Alexandra Burlacu, *Teen Arrested Over DHS and FBI Data Hack*, TECH TIMES (Feb. 13, 2016), http://www.techtimes.com/articles/133501/20160213/teen-arrested-over-dhs-and-fbi-data-hack.htm.
[38] U.S. Gov't Accountability Office, *Federal Agencies Need to Better Protect Sensitive Data* 4 (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf [hereinafter "GAO Sensitive Data Protection Report"].
[39] GAO Sensitive Data Protection Report.
[40] *Id*. at unpaginated "Highlights" section.
[41] *Id*.

cybersecurity weaknesses at DHS and most other federal agencies, "federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats."[42]

These weaknesses in DHS databases increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including medical, financial, education, and biometric information contained in the "Insider Threat" Database on a wide variety of individuals. Accordingly, DHS should maintain only records that are relevant and necessary to detecting and preventing insider threats. To the extent that DHS continues to collect this vast array of sensitive personal information, DHS should limit disclosure to only those agencies and government actors that require the information as a necessity. Further, DHS should strictly limit the use of this information to the purpose for which it was originally collected.

*b. DHS Database Covers Broad Categories of Individuals and Implicates Individuals Who Are Not Under Investigation*

DHS proposes to collect the aforementioned personal, sensitive information on a large group of individuals, including individuals that are not themselves under DHS investigation. The DHS Database would contain records on:

1. DHS current or former employees, contractors, or detailees who have access or had access to national security information, including classified information.

2. Other individuals, including Federal, State, local, tribal, and territorial government personnel and private-sector individuals, who are authorized by DHS to access Departmental facilities, communications security equipment, and/or information technology systems that process sensitive or classified national security information.

3. Any other individual with access to national security information including classified information, who accesses or attempts to access DHS IT systems, DHS national security information, or DHS facilities.

[42] *Id*. at 12.

4. Family members, dependents, relatives, and individuals with a personal association to an individual who is the subject of an insider threat investigation; and

5. Witnesses and other individuals who provide statements or information to DHS related to an insider threat inquiry.[43]

By collecting, maintaining, and disclosing the records of family members and acquaintances of individuals who may be subject to investigation, DHS proposes to create detailed profiles on individuals who are not themselves the target of any investigation. DHS should remove "family members, dependents, relatives, and individuals with a personal association to an individual who is the subject of an insider threat investigation" from the proposed categories of records. Moreover, DHS routinely hosts non-governmental organizations (NGOs) and civil liberties groups at DHS facilities to solicit feedback on programs that implicate privacy and civil liberties.[44] Accordingly, DHS should clarify that records kept on "private-sector individuals who are authorized by DHS to access Departmental facilities" will not include NGOs or any other visitors.

### 3. Proposed Routine Uses Would Circumvent Privacy Act Safeguards and Contravene Legislative Intent

The Privacy Act's definition of "routine use" is precisely tailored, and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. DHS's Insider Threat Database contains a broad category of personally identifiable information. By disclosing information in a manner inconsistent with the purpose for which the information was originally gathered, DHS exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

[43] Insider Threat SORN at 9872.

[44] For example, DHS has held meetings with NGOs and civil liberties groups regarding the Cybersecurity Information Sharing Act (CISA) Privacy and Civil Liberties Guidelines (Mar. 14, 2016); the DHS National Cybersecurity and Communications Integration Center (NCCIC) (Jan. 29, 2015); and DHS's use of license plate data (Nov. 10, 2014).

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[45] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[46]

The Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the written request or consent of the "individual to whom the record pertains."[47] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[48] One of these exemptions is "routine use."[49] "Routine use" means "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[50]

The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[51]

---

[45] S. Rep. No. 93-1183 at 1 (1974).
[46] Pub. L. No. 93-579 (1974).
[47] 5 U.S.C. § 552a(b).
[48] *Id*. §§ 552a(b)(1) – (12).
[49] *Id*. § 552a(b)(3).
[50] 5 U.S.C. § 552a(a)(7).
[51] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[52]

Subsequent Privacy Act case law interprets the Act's legislative history to limit routine use disclosure based upon a precisely defined system of records purpose. In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit relied on the Privacy Act's legislative history to determine that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[53] The Court of Appeals went on to quote the Third Circuit as it agreed, "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[54]

The Insider Threat SORN proposes numerous routine uses that are incompatible with the purpose for which the data was collected, as required by law.[55]

Proposed Routine Use H would permit the agency to disclose information contained in the "Insider Threat" Database:

> To an appropriate Federal, State, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a

[52] *Id*.
[53] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[54] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv.*, 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).
[55] *Id*.

> security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.[56]

Proposed Routine Use I would permit DHS to disclose information contained in the Database:

> To an individual's prospective or current employer to the extent necessary to determine employment eligibility.[57]

Proposed Routine Use K would permit DHS to disclose information:

> To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.[58]

DHS proposes to disclose "Insider Threat" Database information for purposes that do not relate to detecting and preventing insider threats. Determinations regarding employment, licensing, and other benefit eligibility, as contemplated by Routine Uses H, I, and K are entirely unrelated to this purpose. These Routine Uses directly contradict Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[59] Routine Uses H, I, and K unlawfully exceed DHS authority and should be removed from the Insider Threat SORN.

DHS also proposes to create a "Public Relations" exemption to the Privacy Act that would permit the agency to release personal information if – incredibly – such disclosure would

[56] 81 Fed. Reg. 9871, 9874.
[57] *Id*.
[58] *Id*.
[59] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

"preserve confidence" in the agency or "demonstrate accountability." Proposed Routine Use T would permit the agency to disclose information:

> To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS' officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.[60]

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS"[61] in Routine Use T is discordant with the Privacy Act because it gratuitously puts the face of the agency above an individual's right to privacy. The term "necessary" is ambiguous; DHS could take advantage of this criterion to unduly influence its image. DHS should remove this proposed Routine Use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by DHS.

In addition, the proposed routine uses that would permit DHS to disclose records, subject to the Privacy Act, to foreign, international, and private entities should be removed. The Privacy Act only applies to records maintained by United States government agencies.[62] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations.

#### 4. DHS Proposes Broad Exemptions for the "Insider Threat" Database, Contravening the Intent of the Privacy Act of 1974

DHS proposes to exempt the Database from key Privacy Act obligations, such as the requirement that records be accurate and relevant, or that individuals be allowed to access and amend their personal records.

[60] Insider Threat SORN at 9875.
[61] *Id*.
[62] 5 U.S.C. § 552a(b).

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that federal agencies were able to collect.[63] Congress further required agencies to be transparent in their information practices.[64] In *Doe v. Chao*,[65] the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that "in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies."[66]

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DHS proposes to exempt the Database from compliance with the following safeguards: 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).[67] These provisions of the Privacy Act require agencies to:

- grant individuals access to an accounting of when, why, and to whom their records have been disclosed;[68]
- inform parties to whom records have been disclosed of any subsequent corrections to the disclosed records;[69]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[70]
- collect and retain only such records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";[71]
- collect information from the individual to the greatest extent possible, when such information would have an adverse effect on the individual;[72]

[63] S. Rep. No. 93-1183, at 1 (1974).
[64] *Id*.
[65] *Doe v. Chao*, 540 U.S. 614 (2004).
[66] *Doe*, 540 U.S. at 618.
[67] 81 Fed. Reg. 9789, 9790.
[68] 5 U.S.C. § 552a(c)(3).
[69] 5 U.S.C. § 552a(c)(4).
[70] *Id*. § 552a(d).
[71] *Id*. § 552a(e)(1).
[72] *Id*. § 552a(e)(2).

- inform individuals from whom they request information the purposes and routine uses of that information, and the effect of not providing the requested information;[73]
- notify the public when it establishes or revises a database, and provide information on the categories of information sources and procedures to access and amend records contained in the database;[74]
- ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[75]
- promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record;[76]
- serve notice to an individual who's record is made available under compulsory legal process;[77]
- provide public notice prior to the establishment or revision of a computerized comparison of the system of records with non-Federal records;[78]
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act;[79] and
- provide rights to parents of minors and legal guardians to act on behalf of the individual.[80]

Several of DHS's claimed exemptions would further exacerbate the impact of its overbroad categories of records and routine uses in this system of records. DHS exempts itself from § 552a(e)(1), which requires agencies to maintain only those records relevant to the agency's statutory mission. The agency exempts itself from § 552a(e)(4)(I), which requires agencies to disclose the categories of sources of records in the system. And the agency exempts itself from its Privacy Act duties under to § 552a(e)(4)(G) and (H) to allow individuals to access and correct information in its records system. In other words, DHS claims the authority to collect any information it wants without disclosing where it came from or even acknowledging its

[73] *Id*. § 552a(e)(3).
[74] *Id*. § 552a(e)(4)(G), (H), (I).
[75] *Id*. § 552a(e)(5).
[76] *Id*. § 552a(f).
[77] *Id.* § 552a(e)(8).
[78] *Id.* § 552a(e)(12).
[79] *Id.* § 552a(g)(1).
[80] *Id.* § 552a(h).

existence. The net result of these exemptions, coupled with DHS'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.

DHS also proposes exemption from maintaining records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[81] In other words, DHS admits that it contemplates collecting information that will not be relevant or necessary to a specific investigation. The agency's alleged purpose in consciously flouting this requirement is to establish "patterns of unlawful activity."[82] The agency also claims 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.[83] By implication, the agency objects to guaranteeing "fairness" to individuals in the "Insider Threat" Database.[84]

It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to maintain a database on U.S. citizens containing so much personal information and simultaneously be granted broad exemptions from Privacy Act obligations. It is as if the agency has placed itself beyond the reach of the American legal system on the issue of greatest concerns to the American public – the protection of personal privacy. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of database records, and DHS must reign in the exemptions it claims for its "Insider Threat" Database.

[81] 5 U.S.C. § 552a(e)(5).
[82] Insider Threat NPRM at 9790.
[83] *Id*.
[84] *Id*.

## 5. Conclusion

For the foregoing reasons, the proposed "Insider Threat" Database is contrary to the core purpose of the federal Privacy Act. Accordingly, DHS must limit the records contained in the Database and the individuals to whom the records pertain, narrow the scope of its proposed Privacy Act exemptions, and remove the proposed unlawful routine use disclosures from the Insider Threat SORN.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director and Administrative Law Counsel

Claire Gartland
EPIC Consumer Protection Counsel

Jeramie Scott
EPIC National Security Counsel