epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DEPARTMENT OF TRANSPORTATION

[Docket Nos. OST-2018-0128 and OST-2016-0028]

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

November 2, 2018

By notice published on October 3, 2018,[1] the Department of Transportation ("DOT") proposed to establish a Privacy Act system of records titled "DOT/ALL-26 Insider Threat Program" ("Insider Threat Database"). This database will be administered by the Office of the Secretary and the Federal Aviation Administration, and will apply to all DOT Operation Administrations and Secretarial Offices. The Database will include detailed, sensitive information on many individuals who have had access to DOT information systems (classified and unclassified), including current and former DOT employees, contractors, consultants, licensees, and interns, as well as individuals who have never worked for the agency, communicated with the agency, or have any relationship with the agency. "Insider threat" is broad and ambiguous, the extent of data collection is limitless, and proposed disclosures contravene legal authority.

By notice published on Oct. 4, 2018,[2] DOT proposes to exempt the Insider Threat Database from several significant provisions of the Privacy Act of 1974. Under these notices, the Electronic

[1] Notice of Privacy Act system of records, 83 Fed. Reg. 49981, Oct. 3, 2018 [hereafter "Insider Threat SORN"].
[2] Notice of proposed rulemaking, 83 Fed. Reg. 50053, Oct. 4, 2018.

Privacy Information Center ("EPIC") submits these comments to: (1) underscore the substantial privacy and security issues raised by the Database; (2) recommend that DOT curtail the scope of information collected and narrow the categories of individuals to whom the records pertain; (3) urge DOT to withdraw unlawful and unnecessary proposed routine use disclosures; and (4) encourage DOT to narrow the proposed Privacy Act exemptions for the Database.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.[3] EPIC has a particular interest in preserving privacy safeguards established by Congress, including the Privacy Act of 1974, and routinely comments on new agency systems of records and public rulemakings that would diminish the privacy rights and agency obligations set out in the federal Privacy Act.[4]

I. 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

[3] *About EPIC*, EPIC (2018), https://epic.org/epic/about.html.

[4] *See, e.g.,* Comments of the Electronic Privacy Information Center to the Office of Management and Budget, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (Oct. 28, 2016), *available at* https://epic.org/apa/comments/EPIC-OMB-Cir-A-108-Comments-10-28-2016.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Automated Targeting System, Notice of Privacy Act System of Records and Proposed Rule, DHS-2012-0019 and 2012-0020 (June 21, 2012), *available at*: https://epic.org/apa/comments/EPIC-ATS-Comments-2012.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records, DHS-2011-0082 (Nov. 28, 2011), *available at* http://epic.org/privacy/1974act/EPIC-DHS-2011-0082.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records, DHS-2011-0030 (June 8, 2011), *available at* http://epic.org/privacy/EPIC%20E-Verify%20Comments%20Final%2006.08.11.pdf; Comments of the Electronic Privacy Information Center to the Office of the Director of National Intelligence, Notice of Privacy Act System of Records (May 12, 2010), *available at* http://epic.org/privacy/ODNI_Comments_2010-05-12.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System, System of Records and Notice of Proposed Rulemaking: Implementation of Exemptions; Automated Targeting System(Sept. 5, 2007), *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security United States Customs and Border Protection, Docket No. DHS-2005-0053, Notice of Revision to and Expansion of Privacy Act System of Records (May 22, 2006), *available at* http://epic.org/privacy/airtravel/ges052206.pdf.

sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties."[5] According to DOT, the "Insider Threat" Database would help detect, deter, and mitigate risks associated with insider threats under E.O. 13587.[6] DOT's non-exhaustive definition for "insider threats" includes but is not limited to, "espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of Government resources or capabilities."[7] DOT indicates that the proposed database may include information from DOT Operating Administrations, other Federal agencies, or publicly available sources.[8] DOT proposes to disclose information to multiple entities not subject to the Privacy Act, including state, local, and foreign law enforcement, experts, consultants, and contractors.[9]

II. The Agency's Proposed "Insider Threat" Database Would Maintain a Massive Amount of Personal, Sensitive Information About a Wide Variety of Individuals

a. Categories of records are virtually limitless

The Insider Threat SORN indicates that DOT may collect an unbounded amount of personal information from an expansive array of individuals. The Database could include highly sensitive information including but not limited to an individual's SSN, biometric data, credit reports and other financial information, foreign contacts and activities, and polygraph examination reports.[10] DOT suggests that it may also collect sensitive information from a data subject's cohabitants, spouse, or relatives, including SSN, birthplace, and citizenship information.[11]

Because DOT indicates that the Database may include personnel records, the Database will likely contain information derived from Standard Form 86, Questionnaire for National Security

[5] Exec. Order No. 13,587, 76 Fed. Reg. 63,811 (Oct. 7, 2011). *See also* Insider Threat SORN at 49981.
[6] Insider Threat SORN at 49981.
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*

Positions (SF-86). SF-86 is 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…"[12] SF- 86 includes such personal and sensitive information as an individual's 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 information on family members, dependents, relatives, and other personal associations.[13]

The detailed sensitive information 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.[14] The OPM breach exposed sensitive SF-86 forms spanning three decades.[15] The fingerprints of 5.6 million people were also stolen in the data breach.[16] 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.[17]

---

[12] *Willner v. Thornburgh*, 928 F.2d 1185, 1191 (D.C. Cir. 1991).
[13] Questionnaire for National Security Positions (SF-86), U.S. Office of Personnel Management, https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf
[14] 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/.
[15] 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.
[16] 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/.

[17] *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/.

The categories of records contained in the "Insider Threat" Database represent a wealth of sensitive information typically afforded the highest privacy and security protections, such as health,[18] financial,[19] and education[20] records; Social Security Numbers;[21] and individuals' photographs or images.[22] Federal contractors, security experts, and EPIC have 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*,[23] 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).[24] 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.[25] EPIC also argued that compelled collection of sensitive data would place at risk personal health information insufficiently protected by the agency.[26] 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.[27]

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,

---

[18] *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.).
[19] *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.).
[20] *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012).
[21] *See* Driver's Privacy Protection Act, 18 U.S.C. § 2725(4) (defining "highly restricted personal information" to include "social security number").
[22] *Id.* § 2725(4) (defining "highly restricted personal information" to include "individual's photograph or image").
[23] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[24] 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.
[25] *Id*. at 20-28.
[26] *Id.*
[27] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).

including Robert Nelson, the JPL scientist who sued NASA over its data collection practices.[28] The JPL-NASA breach is a clear warning about why DOT should narrow the amount of sensitive data collected. 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 quantity of sensitive information in the proposed DOT 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."[29] Government data breaches increased twelve-fold from 2006 to 2014 alone (surging from 5,503 to 67,168), [30]and the severity of attacks have only gotten worse. This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[31] 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.[32] More recently, a 16-year-old teenage boy was arrested in connection with hacks that exposed the information of over 20,000 FBI employees and 9,000 Department of Homeland Security ("DHS") employees, and the personal email accounts of DHS Secretary Jeh Johnson and Central Intelligence Agency (CIA) director John Brennan.[33] In May 2018, the Office of Management and Budget indicated that most federal agencies' data security

[28] 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.
[29] 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"].
[30] 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"].
[31] GAO Cybersecurity Report at 8.
[32] *Id.* at 7-8.
[33] 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.

procedures are inadequate to protect sensitive data, finding that 71 out of 96 federal agencies have been "relying on cybersecurity programs deemed 'at risk or high risk.'"[34] These weaknesses in agency databases increase the risk that unauthorized individuals could compromise the sensitive information contained in the "Insider Threat" Database and put a wide variety of individuals' privacy at risk. DOT should maintain only records that are relevant and necessary to detecting and preventing insider threats.

b. DOT database implicates individuals who are not affiliated with the agency

DOT proposes to collect the personal, sensitive information on a large group of individuals, including individuals that are not themselves affiliated with the agency. The Database would contain records on "[c]urrent and former DOT employees, including contractors, subcontractors, experts, consultants, licensees, certificate holders, grantees, interns, students, and anyone who has authorized access to classified or controlled unclassified information…"[35] The DOT also proposes to collect sensitive information from data subjects' cohabitants and families. These proposed collection practices will create detailed profiles on individuals who are not affiliated with the agency. DOT should limit the scope of sensitive information collected from individuals with prior access to agency information systems, and DOT should remove "spouse, cohabitant, or relative" from the proposed categories of records.

c. The Proposed Scope of "Routine Uses" Is Inconsistent With the Privacy Act and Contravenes Legislative Intent

The 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. However, DHS proposes

[34] Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, 3 (May 2018), https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.
[35] Insider Threat SORN at 49981.

to increase its authority to disclose records for purposes inconsistent with the reasons for which the information was originally gathered and without the consent of the data subject.

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.[36] 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."[37]

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."[38] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[39] One exemption is "routine use."[40] The SORN states that "all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3)."[41] The Privacy Act defines "routine use" to mean "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."[42]

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

[36] S. Rep. No. 93-1183 at 1 (1974).
[37] Pub. L. No. 93-579 (1974).
[38] 5 U.S.C. § 552a(b).
[39] *Id*. § 552a(b)(1) – (12).
[40] *Id*. § 552a(b)(3).
[41] 83 Fed. Reg. 49981.
[42] 5 U.S.C. § 552a(b)(3) referencing § 552a(a)(7).

> 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.[43]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted routine use to mean that a "not only compatible with, but related to, the purpose for which the record is maintained."[44]

Courts interpret the Act to require a precisely defined system of records purpose for a "routine use." In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit cited 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."[45] The Court of Appeals said "[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."[46]

DOT's proposed routine uses provide the agency with broad authority to disclose individuals' personal information to other federal agencies. Proposed routine uses (3), (5), and (12) expand DHS's authority to disclose information in contravention to the Privacy Act's language, legislative history, and interpretative case law.

Under proposed routine use (3), the agency may disclose information:

> To the appropriate agency, whether Federal, State, local, international, or foreign charged with the responsibility of implementing, investigating, prosecuting, or

---

[43] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[44] *Id*.
[45] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[46] *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).

> enforcing a statute, regulation, rule or order, when a record in this system indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, including any records from this system relevant to the implementation, investigation, prosecution, or enforcement of the statute, regulation, rule or order that was or may have been violated.
>
> Under proposed routine use (5), DOT may disclose information:
>
> To a Federal agency, upon its request, in connection with the requesting Federal agency's hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation or an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information requested is relevant and necessary to the requesting agency's decision on the matter.

The Insider Threat database is purportedly intended to help DOT manage and track insider threat reports and inquiries, not to assist law enforcement agencies in potential investigations or provide information for the hiring of an employee, the letting of a contract, or other proposed uses. 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."[47] Moreover, proposed routine use (3) would expose individuals' information to uses that are not protected by the Privacy Act. The Privacy Act only applies to records maintained by United States government agencies, not to foreign, international, or private authorities.[48] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations. Because these routine uses threaten the privacy of many individuals who communicate or who are a subject of communications with the agency, DOT should withdraw these routine uses.

Under proposed routine use (12), DOT may disclose information:

[47] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[48] 5 U.S.C. §552a(b).

> To appropriate agencies, entities, and persons, when (1) DOT suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DOT has determined that as a result of the suspected… compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DOT or not) that rely on the compromised information; and (3) the disclosure… is reasonably necessary to assist in connection with DOT's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

This proposed routine use gives the agency significant discretion to disclose personal information, following a suspected or confirmed breach. It is unclear how the agency would make a determination that a potential breach occurred, the extent of systems or programs that could "rely on compromised information," if there is a risk of harm, if and how much data is necessary to mitigate that risk, or how frequently proactive disclosure may occur in absence of a genuine breach. Until these concerns are addressed through a comprehensive Privacy Impact Assessment, the agency should remove routine use (12).

III. DOT Proposes Broad Exemptions for the "Insider Threat" Database Against the Intent of the Privacy Act.

DOT proposes to exempt the Database from several key Privacy Act obligations, such as the requirement that individuals be allowed to access and amend their personal records.[49]

When Congress enacted the Privacy Act in 1974, it sought to limit government use and distribution of personal data.[50] In *Doe v. Chao*,[51] 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

[49] 83 Fed. Reg. 50053.
[50] S. Rep. No. 93-1183 at 2-3.
[51] *Doe v. Chao*, 540 U.S. 614 (2004).

Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies."[52]

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DOT proposes to exempt the Database from compliance with the following safeguards: 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G)-(I), and (f). 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;[53]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[54]
- 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;"[55]
- 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;[56]
- 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," institute disclosure procedures for medical and psychological records, create procedures, review amendment requests, determine 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;[57]

Several of DOT's claimed exemptions would further exacerbate the impact of its overbroad categories of records and routine uses in this system of records. DOT 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

[52] *Id*. at 618.
[53] 5 U.S.C. 552a(c)(3).
[54] *Id.* §552a(d).
[55] *Id.* §552a(e)(1).
[56] Id. §552a(e)(4)(G), (H), (I).
[57] Id. §552a(f).

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. Put another way, DOT claims the authority to collect any information it wants without disclosing where it came from or even acknowledging its existence. The net result of these exemptions, coupled with DOT'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.

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 vast reserves of personal information and simultaneously claim 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 narrow the exemptions it claims for the "Insider Threat" Database.

Conclusion

For the foregoing reasons, the proposed "Insider Threat" database undercuts the purpose of the Privacy Act, conflicts with the law, and exceeds agency authority. The Department of Transportation must limit the breadth of records contained in the database and the individuals to whom the records pertain; withdraw proposed routine uses (3), (5), and (12) to safeguard individual privacy; and narrow proposed Privacy Act exemptions.

Respectfully submitted,

/s/ *Marc Rotenberg*
EPIC President and Executive Director

/s/ Jeramie D. Scott
EPIC National Security Counsel

/s/ *Spencer K. Beall*
EPIC Administrative Law Fellow