epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF DEFENSE

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

DUSDI 01-DoD, Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System

[Docket Nos. DoD-2016-OS-0059 and 0060]

June 20, 2016

By notice published on May 19, 2016,[1] the Office of the Secretary of Defense ("DoD") proposes to establish a new Privacy Act system of records titled "Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System" ("Insider Threat Database" or "DoD Database"). The Database will include detailed, personal data on a large number of individuals. Moreover, the scope of "insider threat" is broad and ambiguous; thus, the extent of data collection is essentially unbounded.

[1] Notice of Privacy Act System of Records, 81 Fed. Reg. 31614 (proposed May 19, 2016) [hereinafter "Insider Threat SORN"].

The DoD proposes to exempt the "Insider Threat" Database from several significant provisions of the Privacy Act of 1974 that safeguard the privacy rights of Americans.[2] Pursuant to DoD's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to (1) underscore the substantial privacy and security issues raised by the database; (2) recommend that DoD withdraw the unlawful and unnecessary proposed routine use disclosures; and (3) urge DoD to significantly narrow the proposed Privacy Act exemptions. The proposed Database creates new risks to the privacy and security of Americans.

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]

---

[2] Notice of Proposed Rulemaking, 81 Fed. Reg. 31561 (proposed May 19, 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), 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), 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.

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."[4] According to DoD, the proposed Database would manage "insider threats" in accordance with E.O. 13587.[5] The Department provides a non-exhaustive list of "insider threats," which include, but are not limited to: "damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."[6]

The agency claims that the proposed Database may therefore include counseling statements; credit reports; user names and aliases; logs of printer, copier and facsimile machine use; information collected through "the technical capability to observe and record the actions and activities of all users, at any time, on a computer network controlled by DoD;" and "information related to investigative or analytical efforts by DoD insider threat program personnel to identify threats to DoD personnel, property, facilities, and information." As discussed below, DoD proposes to disclose sensitive, personal information within the Database to multiple

[4] Exec. Order No. 13,587, 76 Fed. Reg. 63,811 (Oct. 7, 2011). *See also* Insider Threat SORN at 31614.
[5] Insider Threat SORN at 31614.
[6] *Id.* at 31616.

entities that are not subject to the Privacy Act, including state, local, tribal, territorial, foreign, and international government agencies.[7]

2. The Proposed "Insider Threat" Database Would Maintain a Massive Amount of Personal, Sensitive Information

a. Categories of Records in the DoD Database Are Virtually Unlimited

According to the Insider Threat SORN, DoD proposes to 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, biometric data, background reports that include medical and financial data, travel records, association records, and citizenship records for roommates and spouses.[8]

The Database will specifically contain information derived from Standard Form 86, Questionnaire for National Security Positions (SF-86).[9] 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 …."[10] 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 (and degrees earned); passport, driver's license, and license

[7] *Id.* at 31617.
[8] *Id.* at 31615.
[9] Insider Threat SORN at 31615.
[10] *Willner v. Thornburgh*, 928 F.2d 1185, 1191 (D.C. Cir. 1991).

plate numbers; medical reports; biometric data; and records related to drug and alcohol use."[11]

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.[12] The OPM breach exposed sensitive SF-86 forms spanning three decades.[13] The fingerprints of 5.6 million people were also stolen in the data breach.[14] 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.[15] The OPM data breach concerning SF-86 is widely considered the most serious breach in the history of the U.S. government.[16]

---

[11] Insider Threat SORN at 31615.

[12] 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/. *See also* David Larter & Andrew Tilghman, *Military Clearance OPM Data Breach 'Absolute Calamity'*, Navy Times (June 18, 2015), http://www.navytimes.com/story/military/2015/06/17/sf-86-security-clearance-breach-troops-affected-opm/28866125/.

[13] 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.

[14] 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/.

[15] *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/.

[16] *See, e.g.*, Peterson *supra* note 14; Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. Times (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html; Brian Naylor, *One Year After OPM Data Breach, What Has the Government Learned?* NPR (June 6, 2016), http://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned.

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, including health,[17] financial,[18] and education[19] records; Social Security Numbers;[20] and individuals' photographs or images.[21] 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*,[22] 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).[23] 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.[24] EPIC also argued that compelled collection of sensitive data would place at risk personal health

---

[17] *See* Health 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.).
[18] *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.).
[19] *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012).
[20] *See* Driver's Privacy Protection Act, 18 U.S.C. § 2725(4) (defining "highly restricted personal information" to include "social security number").
[21] *Id.* § 2725(4) (defining "highly restricted personal information" to include "individual's photograph or image").
[22] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[23] 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. *See also*, EPIC, *NASA v. Nelson (Concerning Informational Privacy for Federal Contract Employees)*, https://epic.org/amicus/nasavnelson/.
[24] *Id.* at 20-28.

information that is insufficiently protected by the agency.[25] 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.[26]

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, including Robert Nelson, the JPL scientist who sued NASA over its data collection practices.[27] The JPL-NASA breach clearly indicates that DoD 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 DoD 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."[28] This is illustrated by the 2015 data breach at OPM, which compromised the

---

[25] *Id.*
[26] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).
[27] 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.
[28] 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"].

background investigation records of 21.5 million individuals.[29] 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.[30] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[31]

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."[32] According to the report, a majority of federal agencies "have weaknesses with the design and implementation of information security controls …."[33] 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."[34] The GAO report concluded that, due to widespread cybersecurity weaknesses at most federal agencies, "federal systems and information, as well as

[29] GAO Cybersecurity Report at 8.
[30] *Id.* at 7-8.
[31] *Id.* at 8.
[32] 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"].
[33] *Id.* at unpaginated "Highlights" section.
[34] *Id.*

sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats."[35]

DoD is uniquely susceptible to data breaches. For example, in 2011, the Deputy Secretary of Defense announced that a DoD contractor experienced a data breach by foreign intruders, compromising 24,000 files.[36] According to the most recent annual report conducted by the Office of Management and Budget ("OMB"), DoD did not meet the hardware asset management capability threshold as established by the Cybersecurity Cross-Agency Priority ("CAP") goal,[37] scoring lower for automated enterprise visibility capability than any other agency apart from the EPA.[38] DoD lacks sufficient capacity to detect and block unauthorized software.[39] DoD's Strong Authentication Capabilities lag behind civilians agencies.[40] Of seven Anti-Phishing metrics used to measure compliance with the CAP goal target, DoD met three.[41] Of five Anti-Malware metrics, DoD met one.[42] Overall, the number of government data breaches, including for DoD, has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[43]

---

[35] *Id.* at 12.
[36] U.S. Gov't Accountability Office, *Actions Needed to Address Challenge Facing Federal Systems* (Apr. 22, 2015), http://www.gao.gov/assets/670/669810.pdf.
[37] Office of Management and Budget, *Cybersecurity Cross-Agency Priority Goal* https://www.performance.gov/content/cybersecurity?view=public; *see also* Office of Management and Budget, *Cybersecurity CAP Goal Update* (March 19, 2015), https://www.whitehouse.gov/omb/e-gov/docs/#CyberCAP.
[38] Office of Management and Budget, *Federal Information Security Modernization Report to Congress* at 20 (Mar. 18, 2016) [hereinafter "Security Report"], https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf.
[39] *Id.* at 21.
[40] *Id.* at 24.
[41] *Id.* at 26.
[42] *Id.* at 27.
[43] GAO Sensitive Data Protection Report at 4.

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

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. DoD'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, DoD exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

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.[44] 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."[45]

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."[46] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[47] One of these exemptions is "routine use."[48] "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."[49]

The Privacy Act's legislative history and a subsequent report on the Act indicate that a 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

[44] S. Rep. No. 93-1183 at 1 (1974).
[45] Pub. L. No. 93-579 (1974).
[46] 5 U.S.C. § 552a(b).
[47] *Id.* §§ 552a(b)(1) – (12).
[48] *Id.* § 552a(b)(3).
[49] 5 U.S.C. § 552a(a)(7).

> another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[50]

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."[51]

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."[52] 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."[53]

---

[50] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[51] *Id.*
[52] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[53] *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).

The Insider Threat SORN proposes numerous routine uses that are not compatible with the purpose for which the data was collected, as required by law.[54]

One proposed routine use 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 security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DoD 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.[55]

Another proposed routine use would permit DoD to disclose information "[t]o Federal, state, local, territorial, tribal, foreign, or international licensing agencies or associations that require information concerning the suitability or eligibility of an individual for a license."[56]

DoD proposes to disclose "Insider Threat" Database information for purposes unrelated to "insider threat detection and mitigation."[57] Determinations regarding employment, licensing, and other benefit eligibility, as contemplated by the above routine uses are entirely unrelated to the stated purpose of the database. These routine uses directly contradict Congressman William Moorhead's testimony that

---

[54] *Id.*
[55] Insider Threat SORN at 31616-17.
[56] *Id.* at 31617.
[57] *Id.* at 61616.

the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[58] These routine uses unlawfully exceed DoD authority and should be removed from the Insider Threat SORN.

In addition, the proposed routine uses that would permit DoD to disclose records, subject to the Privacy Act, to foreign and international entities should be removed. The Privacy Act only applies to records maintained by federal government agencies and certain government contractors.[59] Releasing information to foreign and international entities would expose individuals covered by this records system to Privacy Act violations.

4. DOD Proposes Broad Privacy Act Exemptions for the "Insider Threat" Database, Contravening Congressional Intent

DoD 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.

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that federal agencies were able to collect.[60] Congress further required agencies to be transparent in their information practices.[61] In *Doe v. Chao*,[62] the Supreme Court underscored the importance of the Privacy Act's

---

[58] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[59] *See* 5 U.S.C. § 552a(a)(1) (incorporating definition of "agency" found in Freedom of Information Act, 5 U.S.C. § 552(f)(1), and Administrative Procedure Act, 5 U.S.C. § 551(1)); § 552a(m)(1). *See also N'Jai v. Pittsburgh Bd. of Pub. Educ.*, 487 F. App'x 735, 737 (3d Cir. 2012) (recognizing that Privacy Act "applies only to federal government agencies") (citing *Pennyfeather v. Tessler,* 431 F.3d 54, 56 & n. 1 (2d Cir.2005)).
[60] S. Rep. No. 93-1183, at 1 (1974).
[61] *Id.*
[62] *Doe v. Chao*, 540 U.S. 614 (2004).

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."[63]

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DoD proposes to exempt the Database from compliance with the following safeguards: 5 U.S.C. 552a(c)(3), (c)(4); (d)(1), (d)(2), (d)(3), (d)(4); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g).[64] 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;[65]
- inform parties to whom records have been disclosed of any subsequent corrections to the disclosed records;[66]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[67]
- 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";[68]
- collect information from the individual to the greatest extent possible, when such information would have an adverse effect on the individual;[69]
- inform individuals from whom they request information the purposes and routine uses of that information, and the effect of not providing the requested information;[70]

[63] *Doe*, 540 U.S. at 618.
[64] 81 Fed. Reg. 31614, 31618.
[65] 5 U.S.C. § 552a(c)(3).
[66] 5 U.S.C. § 552a(c)(4).
[67] *Id.* § 552a(d).
[68] *Id.* § 552a(e)(1).
[69] *Id.* § 552a(e)(2).
[70] *Id.* § 552a(e)(3).

- 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;[71]
- ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[72]
- 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;[73]
- serve notice to an individual whose record is made available under compulsory legal process;[74] and
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act.[75]

Several of DoD's claimed exemptions would further exacerbate the impact of its overbroad categories of records and routine uses in this system of records. DoD 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, DoD claims the authority to collect any information it wants without disclosing where it came from or even

[71] *Id.* § 552a(e)(4)(G), (H), (I).
[72] *Id.* § 552a(e)(5).
[73] *Id.* § 552a(f).
[74] *Id.* § 552a(e)(8).
[75] *Id.* § 552a(g)(1).

acknowledging its existence. The net result of these exemptions, coupled with DoD'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.

DoD 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."[76] In other words, DoD 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."[77] 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.[78] By implication, the agency objects to guaranteeing "fairness" to individuals in the "Insider Threat" Database.[79]

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 concern to the American public – the

[76] 5 U.S.C. § 552a(e)(5).
[77] 81 Fed. Reg. 31561.
[78] *Id.*
[79] *Id.*

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 DoD must reign in the exemptions it claims for its "Insider Threat" Database.

5. Conclusion

For the foregoing reasons, the proposed "Insider Threat" Database is contrary to the core purpose of the federal Privacy Act. Accordingly, DoD 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

Claire Gartland
EPIC Consumer Protection Counsel

Ari Lipsitz
EPIC IPIOP Clerk

Helen Moscardini
EPIC IPIOP Clerk