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 DEFENSE

Privacy Act of 1974; System of Records

[Docket ID: DOD-2019-OS-0033]

April 22, 2019

By notice published March 22, 2019, the Department of Defense (DoD) published a notice to modify a system of records, titled "DoD Insider Threat Management and Analysis Center and DoD Component Insider Threat Records System."[1] The Database includes 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.

EPIC submits these comments to the DoD to: (1) draw attention to the substantial privacy and security concerns associated with this Database; (2) urge the withdrawal of the unlawful and unnecessary routine use disclosures; (3) insist that the DoD significantly narrow the Privacy Act exemptions; and (4) recommend the adoption of the Universal Guidelines for Artificial Intelligence with respect to the 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

[1] *Privacy Act of 1974; System of Records*, 84 Fed. Reg. 10803-10808 (Mar. 22, 2019), https://www.federalregister.gov/documents/2019/03/22/2019-05540/privacy-act-of-1974-system-of-records.

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.[2]

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 sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties."[3] According to DoD, the Database manages "insider threats" in accordance with E.O. 13587.[4] The Department provides a non-exhaustive list of "insider threats," which include, but are not limited to: "espionage, terrorism, the unauthorized disclosure of national security information (including protected and sensitive information), and the loss or degradation of departmental resources or capabilities can damage the United States."[5]

The Database may 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

---

[2] *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.

[3] Exec. Order No. 13,587, 76 Fed. Reg. 63,811 (Oct. 7, 2011). *See also* 84 Fed. Reg. 10803.

[4] 84 Fed. Reg. 10804.

[5] *Id.* at 10804-05.

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."[6] As discussed below, DoD claims the right to disclose sensitive, personal information within the Database to multiple entities that are not subject to the Privacy Act, including state, local, tribal, territorial, foreign, and international government agencies.[7]

II. The "Insider Threat" Database maintains vast amounts of personal, sensitive information.

According to the Insider Threat SORN, DoD gathers an inordinate amount of personal information about federal employees, their friends, and family members.[8] 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.[9]

The Database specifically contains information derived from Standard Form 86, Questionnaire for National Security Positions (SF-86).[10] 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 …."[11] 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 plate numbers;

[6] *84 Fed. Reg.* 10805-06.
[7] *Id.* at 10806.
[8] *Id.* at 10805.
[9] *Id.* at 10805-06.
[10] *Id.* at 10805.
[11] *Willner v. Thornburgh*, 928 F.2d 1185, 1191 (D.C. Cir. 1991).

medical reports; mental health history; biometric data; and records related to drug and alcohol use."[12]

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.[13] The OPM breach exposed sensitive SF-86 forms spanning three decades.[14] The fingerprints of 5.6 million people were also stolen in the data breach.[15] 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.[16] The OPM data breach concerning SF-86 is widely considered the most serious breach in the history of the U.S. government.[17]

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

[12] 84 Fed. Reg. 10805.
[13] 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/.
[14] 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.
[15] 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/.
[16] *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/.
[17] *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 highest degree of privacy and security protections, including 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 previously argued to the U.S. Supreme Court that much of this information simply should not be collected by the federal government.

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 that is 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]

---

[18] *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.).
[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. *See also*, EPIC, *NASA v. Nelson (Concerning Informational Privacy for Federal Contract Employees)*, https://epic.org/amicus/nasavnelson/.
[25] *Id*. at 20-28.
[26] *Id*.
[27] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).

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.[28] 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]ybersecurity incidents continue to impact entities across various critical infrastructure sectors."[29] The report further noted, "IT systems are often riddled with security vulnerabilities—both known and unknown. These vulnerabilities can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety."

This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[30] "[M]ore recently, in 2017, a security breach reported by Equifax—one of the nation's largest credit bureaus— that resulted in the loss of PII for an estimated 148 million U.S. consumers."[31] In March 2018, the Department of Justice reported a "massive cybersecurity theft campaign on behalf of the Islamic Revolutionary Guard

[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, *HIGH-RISK SERIES: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, 4 (July 25, 2018), available at https://www.gao.gov/assets/700/693405.pdf, [hereinafter GAO Cybersecurity Report].
[30] GAO Cybersecurity Report at 2.
[31] *Id.*

Corps[,]" where "nine Iranians allegedly stole more than 31 terabytes of documents and data from more than 140 American universities, 30 U.S. companies, and *five federal government agencies*, among other entities."[32] That same month, the Department of Homeland Security and the Federal Bureau of investigation stated that "since at least March 2016, Russian government actors had targeted the systems of multiple U.S. government entities and critical infrastructure sectors. Specifically, the alert stated that Russian government actors had affected multiple organizations in the energy, nuclear, water, aviation, construction, and critical manufacturing sectors."[33]

The latest series of high-profile government data breaches indicates that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. "[I]n the last 2 years that federal agencies (1) had not identified and closed cybersecurity skills gaps, (2) had been challenged with recruiting and retaining qualified staff, and (3) had difficulty navigating the federal hiring process."[34]

DoD is uniquely susceptible to data breaches. The GAO reported the "DOD had not addressed cybersecurity workforce management requirements set forth in federal laws."[35] Further:

> DOD's process for monitoring the implementation of cybersecurity guidance had weaknesses and resulted in the closure of certain tasks (such as completing cyber risk assessments) before they were fully implemented[,]… DOD had not identified the National Guard's cyber capabilities (e.g., computer network defense teams) or addressed challenges in its exercises… [and] as of April 2016, DOD had not identified, clarified, or implemented all components of its support of civil authorities during cyber incidents.[36]

[32] GAO Cybersecurity Report, 7 (emphasis added).
[33] *Id.* at 7.
[34] *Id.* at 19.
[35] *Id.* at 19.
[36] *Id.* at 25.

According to a recent DoD Inspector General report, "recently issued cybersecurity reports indicate that the DoD still faces challenges in managing cybersecurity risk to its network. And as of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008."[37]

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.

III. The Routine Uses claimed 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

[37] Office of the Inspector Gen., Dep't of Defense, *Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018*, ii (Jan. 9, 2019), available at https://media.defense.gov/2019/Jan/11/2002078551/-1/-1/1/DODIG-2019-044.PDF.

in their information practices.[38] 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."[39]

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."[40] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[41] One of these exemptions is "routine use."[42] "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."[43]

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 another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[44]

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

[38] S. Rep. No. 93-1183 at 1 (1974).
[39] Pub. L. No. 93-579 (1974).
[40] 5 U.S.C. § 552a(b).
[41] *Id.* §§ 552a(b)(1) – (12).
[42] *Id.* § 552a(b)(3).
[43] 5 U.S.C. § 552a(a)(7).
[44] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

use' must be not only compatible with, but related to, the purpose for which the record is maintained."[45]

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."[46] 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."[47]

The Insider Threat SORN claims numerous routine uses that are not compatible with the purpose for which the data was collected, as required by law.[48]

One routine use permits 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,

[45] *Id*.
[46] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[47] *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).
[48] *Id*.

> or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.[49]

Another routine use permits DoD to disclose information "[t]o the news media or the general public, where the disclosure of factual information would be in the public interest and which would not constitute an unwarranted invasion of personal privacy."[50]

DoD claims the right to disclose "Insider Threat" Database information for purposes unrelated to "insider threat detection and mitigation."[51] Determinations regarding employment, licensing, and other benefit eligibility, or to news media, 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 statement that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[52] These routine uses unlawfully exceed DoD authority and should be removed from the Insider Threat SORN.

In addition, the routine uses that 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.[53] Releasing information to foreign and international entities would expose individuals covered by this records system to Privacy Act violations.

---

[49] 84 Fed. Reg. 10806.
[50] *Id.* at 10807.
[51] *Id.* at 10806-07.
[52] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[53] *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)).

IV. Broad Privacy Act exemptions also contravene legislative intent.

The DoD seeks 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.[54] Congress further required agencies to be transparent in their information practices.[55] In *Doe v. Chao*,[56] 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."[57]

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DoD exempts the Database from compliance with the following safeguards: 5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f); and (g).[58] 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;[59]
- inform parties to whom records have been disclosed of any subsequent corrections to the disclosed records;[60]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[61]

[54] S. Rep. No. 93-1183, at 1 (1974).
[55] *Id*.
[56] *Doe v. Chao*, 540 U.S. 614 (2004).
[57] *Doe*, 540 U.S. at 618.
[58] 81 Fed. Reg. 31614, 31618.
[59] 5 U.S.C. § 552a(c)(3).
[60] 5 U.S.C. § 552a(c)(4).
[61] *Id*. § 552a(d).

- 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";[62]
- collect information from the individual to the greatest extent possible, when such information would have an adverse effect on the individual;[63]
- inform individuals from whom they request information the purposes and routine uses of that information, and the effect of not providing the requested information;[64]
- notify the public when it establishes or revises a database, and provide information on the procedures whereby individuals can determine whether they have records in the database and how to access and amend records contained in the database;[65]
- ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[66]
- 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;[67]
- serve notice to an individual whose record is made available under compulsory legal process;[68] and
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act.[69]

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 seeks to exempt itself from § 552a(e)(1), which requires agencies to maintain only those records relevant to the agency's statutory mission. 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 acknowledging its existence. The net result of these

[62] *Id*. § 552a(e)(1).
[63] *Id*. § 552a(e)(2).
[64] *Id*. § 552a(e)(3).
[65] *Id*. § 552a(e)(4)(G), (H).
[66] *Id*. § 552a(e)(5).
[67] *Id*. § 552a(f).
[68] *Id.* § 552a(e)(8).
[69] *Id.* § 552a(g)(1).

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 claims exemption from maintaining records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[70] In other words, DoD admits that it contemplates collecting information that will not be relevant or necessary to a specific investigation. 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.[71] By implication, the agency objects to guaranteeing "fairness" to individuals in the "Insider Threat" Database.[72]

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 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.

[70] 5 U.S.C. § 552a(e)(5).
[71] *Id.*
[72] *Id.*

V. DoD should adopt the Universal Guidelines for Artificial Intelligence.

The Database also implicates the fairness, accountability, and transparency of decisions that concern federal employees. As more personal data is processed by federal agencies with advanced analytic capabilities, the need to ensure baseline protections increases.

The Universal Guidelines for Artificial Intelligence have been endorsed by over 300 organizations and experts.[73] Given the DoD uses the "Insider Threat" Database to "to analyze, monitor, and audit insider threat information for insider threat detection and mitigation within the DoD on persons eligible to access classified information and or hold a sensitive position[,]"[74] the agency should commit to the principles, rights, and obligations contained in the Universal Guidelines for Artificial Intelligence. DoD's database, which uses machine learning and algorithms to make decisions that impact individuals, should be governed by clear policy rules set out in agency regulations. There are several guidelines in the UGAI that are particularly applicable to the DoD's "Insider Threat" Database.

a. Right to Transparency and the Assessment and Accountability Obligation

The rights and freedoms of individuals predicted to be "insider threats" are directly at stake. Therefore, the Universal Guidelines for Artificial Intelligence apply to the Database and its use of analytical and machine learning algorithms.

The principle of transparency is found in various modern privacy laws including US Privacy Act, the EU Data Protection Directive, the GDPR, and the Council of Europe Convention 108. The aim of transparency is to "enable independent accountability for automated

[73] The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018) available at https://thepublicvoice.org/ai-universal-guidelines/ [hereinafter UGAI].
[74] 84 Fed. Reg. 10805.

decisions."[75] This principle translates into an affirmative right of individuals, "to know the basis of an AI decision that concerns them[,]" including "access to the factors, the logic, and techniques that produced the outcome."[76] Individuals should not be left in the dark about analytical systems making decisions that affect them.

Further, DoD should implement an assessment and accountability mechanism. The UGAI states that "An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system."[77] There is no indication that a full assessment and proper accountability mechanisms are in place for the "Insider Threat" Database.

EPIC urges DoD to create and publish "Algorithmic Assessments" similar to the Privacy Impact Assessments conducted by federal agencies pursuant to Section 208 of the E-Government Act of 2002. These assessments would force the agency to determine the risks and rewards of an AI system prior to and during deployment. The assessments would also allow individuals to understand the methods and factors used in decisions that have an impact on their lives.

b. Fairness Obligation and Right to Human Determination

As the Universal Guidelines state, "Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions." This fairness obligation is particularly important to ensure that the systems of the Insider Threat database are not used to make decisions that will adversely affect particular groups for illegitimate reasons. It is important

[75] The Public Voice, *Universal Guidelines for Artificial Intelligence Explanatory Memorandum and References* (Oct. 2018), available at https://thepublicvoice.org/ai-universal-guidelines/memo/ [hereinafter UGAI Explanatory Memo].
[76] UGAI, 1.
[77] *Id.* at 5.

to remember that seemingly neutral factors and rules could lead to impermissible discriminatory results.[78]

This is particularly true for DoD's "Insider Threat" Database because it uses information such as ethnicity and race, biometric data, education history, names of associates, citizenship information, mental health history, information on equal opportunity complaints, and citizenship information for spouse or cohabitants.[79] It is unclear how this data relates to detecting "insider threats", and even if it did, the potential for abuse and unfair results is strong. The utility of big data is alluring, but it is important to avoid perpetuating unfair bias or discrimination by way of automation.

The right to meaningful human intervention is helpful to ensure algorithmic discrimination does not take place. Human decisionmaking "reaffirms that individuals and not machines are responsible for automated decision-making."[80] With better accountability for the results of such systems, there is less of a chance of unfair results.

c. Accuracy, Reliability, and Validity Obligations and Data Quality Obligation

The obligations of accuracy, reliability, validity, and data quality are important principles in any system, especially with the potential to put vast amounts of individuals under unwarranted scrutiny. These obligations are all the more important for DoD to commit to since the agency has exempted the "Insider Threat" Database from Privacy Act obligations that require the information in these system to be relevant and necessary.[81] Therefore, DoD must verify the information used in the Database and should frequently audit such systems.

---

[78] Joi Ito, *Supposedly 'Fair' Algorithms Can Perpetuate Discrimination*, Wired (Feb. 5, 2019), https://www.wired.com/story/ideas-joi-ito-insurance-algorithms/.
[79] 84 Fed. Reg. 10805.
[80] UGAI Memo.
[81] 84 Fed. Reg. 10808; 5 U.S.C. § 552a(e)(5).

Conclusion

The "Insider Threat" database contains extensive and detailed personal information on federal employees, their friends, and family members..[82] While the stated purpose of the system is to "deter[] insider activity endangering DoD and U.S. Government installations, facilities, personnel, missions, or resources[,]"[83] the creation of this system of records -- despite a documented inability to protect personal data[84] -- invites the very threats the program seeks to prevent.

Further, the DoD's claimed routine uses and broad Privacy Act exemptions contravene legislative intent and compromise fairness to the individuals who are included in this database. The DoD should narrow the routine uses and exemptions from the Privacy Act and adopt the Universal Guidelines for Artificial Intelligence to ensure fairness and accountability in the operation of the agency's Insider Threat database.

Respectfully submitted,

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

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC Senior Counsel

/s/ Ellen Coogan
Ellen Coogan
EPIC Domestic Surveillance Fellow

[82] *Id.* at 10805-06.
[83] 84 Fed. Reg. 10804
[84] GAO Cybersecurity Report, 19.