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

[Docket Nos. DoD-2018-OS-0076 and DoD-2018-OS-0075]

Notice of Privacy Act System of Records; Notice Proposed Rulemaking

November 16, 2018

By notice published on October 17, 2018,[1] the Department of Defense ("DoD") proposes to establish a Privacy Act system of records titled, "Personnel Vetting Records System" DUSDI 02-DoD ("Records System"). The Records System contains extensive sensitive information on federal agency personnel, civilian personnel, contractors, and consultants, Red Cross volunteers, foreign nationals, and private sector employees, spouses, relatives, friends and colleagues. The DoD also proposes to exempt the Records System from several significant provisions of the Privacy Act of 1974.[2] Under these notices, the Electronic Privacy Information Center ("EPIC") submits these comments to urge DoD to (1) suspend the implementation of the Records System until the agency solicits and considers public comments; (2) curtail the scope of information collected; (3) withdraw

[1] Notice of Privacy Act system of records, 83 Fed. Reg. 52420, Oct. 17, 2018 [hereafter "Personnel Vetting SORN"].
[2] Notice of proposed rulemaking, 83 Fed. Reg. 52317, Oct. 17, 2018.

unlawful and unnecessary proposed routine use disclosures; and (4) narrow the proposed Privacy Act exemptions for the Records System.

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 agency recordkeeping activities that would diminish the privacy rights and agency obligations set out in the federal Privacy Act.[4]

I. Purpose and Scope of the Matching Program

Executive Order 13467, as amended by Executive Order 13764, requires DoD to "design, develop, deploy, operate, secure, defend, and continuously update and modernize… vetting information technology systems."[5] According to DoD, the proposed Records System will support

[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;Comments of the Electronic Privacy Information Center to the Selective Service System and Department of Education, Dec. 31, 2004, https://epic.org/privacy/student/sssdatamatch.html.

[5] Executive Order 13764 of Jan. 17, 2017, *Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*, https://www.gpo.gov/fdsys/pkg/FR-2017-01-23/pdf/2017-01623.pdf; Executive Order 13467 of Jul. 2, 2008, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,* https://www.gpo.gov/fdsys/pkg/FR-2008-07-02/pdf/08-1409.pdf.

personnel security background investigations, adjudications, and continuous vetting activities in compliance with this Order. The Records System will contain background information on "all personnel for whom DoD conducts or adjudicates background investigations for security, suitability, fitness, and credentialing."[6] These categories include federal agency personnel, civilian personnel, contractors, and consultants, Red Cross volunteers, foreign nationals, and private sector employees who require security clearances, among other categories.[7] Data collection also applies to spouses and relatives of the data subject.[8] The scope of information collection is virtually limitless, including SSN, date and place of birth, hair and eye color, residential history, maternal maiden name, immigration and passport information, drug/alcohol consumption records, mental health history, financial records (e.g. credit reports and tax returns), biometric data, and a litany of other sensitive information.

II. DoD's Proposed Information Collection and Routine Uses Would Have a Substantial Effect on Members of the Public and Thus the Administrative Procedure Act Requires Public Notice and Comment Prior to Implementation

The Privacy Act requires agencies "at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, [to] publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency."[9] Paragraph (4)(B) and 4(C) of the subsection refer to "categories of individuals on whom records are maintained in the system" and "categories of records maintained in the system," respectively. Paragraph (4)(D) of the subsection refers to "each routine use of the records contained in the system, including the categories of users and the purposes of such use."[10]

---

[6] 83 Fed. Reg. 52420.
[7] *Id.*
[8] *Id.*
[9] 5 U.S.C. § 552a(e)(11).
[10] *Id.* at (e)(4)(D).

In addition to the Privacy Act's Federal Register public notice requirement, DoD is also obligated under the Administrative Procedure Act ("APA") to provide notice and comment on the proposed updates to the system of records because the system of records' "substantive effect is sufficiently grave so that notice and comment are needed to safeguard the policies underlying the APA."[11] The substantive effect of the proposed routine uses within DoD's system of records is "sufficiently grave" because they "impose directly and significantly upon so many members of the public."[12] DoD's system of records applies to a broad category of individuals, including any "[p]ersonnel for whom DoD conducts or adjudicates background investigations for security, suitability, fitness, and credentialing." Among others, these personnel categories include DoD and civilian contractor personnel, consultants, and applicants for these positions, "other government personnel who have authorized access to the system," Red Cross volunteers and staff, "other individuals requiring a DoD determination for fitness," and officials or employees of private sector entities sponsored for access to classified information by a federal agency. The proposed routine uses and lack of specific data security measures require notice and comment because they create "sufficiently grave" privacy risks to these individuals.

A. *DoD Must Consider Public Comments Before It May Implement the Proposed Revisions*

The APA notice and comment requirement does not exist in a vacuum. Following the required notice and comment period, § 553(c) of the APA states that "[a]fter consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose."[13] Indeed, the "essential purpose of those [notice and comment]

[11] *EPIC v. U.S. Dep't. of Homeland Sec.,* 653 F.3d 1, 5-6 (D.C. Cir. 2011) (rehearing *en banc* denied) (quoting *Lamoille Valley R.R.Co. v. ICC*, 711 F.2d 295, 328 (D.C. Cir. 1983)); The Administrative Procedure Act, 5 U.S.C.§ 553 (b)-(c)(2011).
[12] *EPIC v. U.S. Dep't. of Homeland Sec.,* 653 F.3d at 6.
[13] 5 U.S.C. §553(c).

provisions is the generation of comments that will permit the agency to improve its tentative rule"[14] and to give the agency "the opportunity 'to educate itself on the full range of interests the rule affects.'" [15] Additionally, it is well established that agencies must provide rationale for their decision-making processes by "responding to those comments that are relevant and significant."[16]

The SORN invites public comments on the proposed routine uses, but there is no opportunity for the agency to consider them because the proposed routine uses go into effect on November 16, 2018, the same day that the comments are due. The SORN indicates that the remainder of SORN "is effective on October 17, 2018,"[17] the same day the agency proposed to establish the Records System. By not considering the public comments it receives in response to the substantial privacy risks the proposed routine uses present, DoD violates § 553(c).

B. *Without Public Comment Review, DoD's Proposed Revisions Will Fail on Procedural Grounds*

Courts have consistently held that "[i]f the agency fails to provide this notice and opportunity to comment or the notice and comment period are inadequate, the 'regulation must fall on procedural grounds, and the substantive validity of the change accordingly need not be analyzed.'"[18]

DoD's notice and comment concerning the proposed Records System is inadequate because the agency does not afford itself opportunity to review the public comments it receives. The proposed routine uses will become effective on the day that comments are due, and the remainder of

[14] *Am. Fed'n of Labor & Cong. of Indus. Organizations v. Donovan*, 757 F.2d 330, 337 (D.C. Cir. 1985) (quoting *Am. Fed'n of Labor & Cong. of Indus. Organizations v. Donovan*, 582 F. Supp. 1015, 1024 (D.D.C. 1984)).
[15] *Louis v. U.S. Dept. of Labor*, 419 F.3d 970, 976-77 (9th Cir. 2005) (quoting *Alcaraz v. Block*, 746 F.2d 593, 611 (9th Cir. 1984)).
[16] *Grand Canyon* Air *Tour Coal v. FAA*, 154 F.3d 455, 468 (D.C. Cir. 1998); *Cement Kiln Recycling Coalition v. E.P.A.*, 493 F.3d 207, 225 (D.C. Cir. 2007); *Interstate Natural Gas Ass'n of America v. F.E.R.C.*, 494 F.3d 1092, 1096 (D.C. Cir. 2007); *Int'l Fabricare Inst. V. U.S. EPA*, 972 F.2d 384, 389 (D.C. Cir. 1992).
[17] 83 Fed. Reg. 52420.
[18] *Public Citizen, Inc. v. Mineta*, 427 F.Supp.2d 7, 12 (D.D.C. 2006) (quoting *AFL-CIO v. Donovan*, 757 F.2d 330, 338 (D.C. Cir. 1985)). *See also Stainback v. Mabus*, 671 F. Supp.2d 126, 135 (D.D.C. 2009); *Steinhorst Associates v. Preston*, 572 F.Supp.2d 112, 124 n. 13 (D.D.C. 2008); *National Ass'n of Home Builders v. U.S. Army Corps of Engineers*, 453 F. Supp. 2d 116, 123 (D.D.C. 2006).

the SORN entered into force on the day the Record System was proposed. Therefore, the proposed routine uses must fall on procedural grounds and should not be implemented without the agency reviewing and considering public comment. Because DoD intends to establish information collection and routine uses for its Record System, it is required to provide a meaningful opportunity for public comment by reviewing public comments.

III. The Proposed Scope of Information Collection Contravenes the Intent of the Privacy Act

The Personnel Vetting SORN indicates that DoD may collect an unbounded amount of information from an expansive array of individuals. The Records System could include highly sensitive information including but not limited to an individual's SSN, biometric data, mental health records, drug and alcohol use records, credit reports and other financial information, foreign contacts and activities, polygraph examination reports, and "other biographical information as required…"[19] DoD indicates that it may also collect sensitive information from a data subject's spouse and relatives, including date and place of birth, countries of citizenship, physical addresses, email addresses, and phone numbers.[20]

The Personnel Vetting SORN notes that records will be derived from a variety of sources, including Standard Form 86 (SF-86), Questionnaire for National Security positions. 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…"[21] 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

[19] 83 Fed. Reg. 52420.
[20] *Id.*
[21] *Willner v. Thornburgh*, 928 F.2d 1185, 1191 (D.C. Cir. 1991).

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.

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.[22] The OPM breach exposed sensitive SF-86 forms spanning three decades.[23] The fingerprints of 5.6 million people were also stolen in the data breach.[24] 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.[25]

The categories of records contained in the Records System represent a wealth of sensitive information typically afforded the highest privacy and security protections, such as health,[26] financial,[27] and education[28] records; Social Security Numbers;[29] and individuals' photographs or images.[30] 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.

---

[22] 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/.
[23] 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.
[24] 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/.
[25] *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/.
[26] *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.).
[27] *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.).
[28] *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012).
[29] *See* Driver's Privacy Protection Act, 18 U.S.C. § 2725(4) (defining "highly restricted personal information" to include "social security number").
[30] *Id.* § 2725(4) (defining "highly restricted personal information" to include "individual's photograph or image").

In *NASA v. Nelson*,[31] 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).[32] 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.[33] EPIC also argued that compelled collection of sensitive data would place at risk personal health information insufficiently protected by the agency.[34] 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.[35]

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.[36] The JPL-NASA breach is a clear warning about why DoD 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 surge in government data breaches, the vast quantity of sensitive information in the proposed Records System 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

[31] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[32] 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.
[33] *Id*. at 20-28.
[34] *Id.*
[35] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[36] 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.

systems have become not only more numerous and diverse but also more damaging and disruptive."[37] Government data breaches increased twelve-fold from 2006-2014 alone (surging from 5,503 to 67,168),[38] 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.[39] 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.[40] 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 Jeh Johnson and Central Intelligence Agency (CIA) director John Brennan.[41] In May 2018, the Office of Management and Budget indicated that most federal agencies' data security 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.'"[42] These weaknesses in agency databases increase the risk that unauthorized individuals could compromise the sensitive information contained in the Records System and put many individuals' privacy at risk. DoD should only maintain records that are relevant and necessary to performing its functions.

[37] 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"].
[38] U.S. Gov't Accountability Office, *Federal Agencies Need to Better Protect Sensitive Data* 4 (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf [hereinafter "GAO Sensitive Data Protection Report"].
[39] GAO Cybersecurity Report at 8.
[40] *Id.* at 7-8.
[41] 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.
[42] 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.

IV. The Proposed Scope of "Routine Uses" Is Inconsistent with the Privacy Act

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, DoD proposes to significantly increase its authority to disclose records for purposes that are inconsistent with the reasons for which the information was originally gathered and without the consent of the individual concerned.

When it enacted the Privacy Act in 1974, Congress required agencies to be transparent in their information practices.[43] 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."[44]

Accordingly, 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."[45] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[46] One of these exemptions is "routine use."[47] The SORN states that "the records contained herein may specifically be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3)."[48] 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."[49]

[43] S. Rep. No. 93-1183 at 1 (1974).
[44] Pub. L. No. 93-579 (1974).
[45] 5 U.S.C. § 552a(b).
[46] *Id*. § 552a(b)(1) – (12).
[47] *Id*. § 552a(b)(3).
[48] 83 Fed. Reg. 52420.
[49] 5 U.S.C. § 552a(b)(3) referencing § 552a(a)(7).

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

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[50]

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."[51]

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."[52] 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."[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 wide range of routine uses contained in DoD's proposed Records System provide the agency with broad authority to disclose individuals' personal information to other federal agencies. In particular, proposed routine uses L, Q, Z, BB, and CC vastly expand DoD's authority to disclose information in conflict with the Privacy Act's language, legislative history, and interpretative case law.

Under proposed routine use L, the agency may disclose information:

> To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual under investigation, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.[54]

Under proposed routine use BB, the agency may disclose information:

> To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law…[55]

The proposed routine uses above authorize DoD to disclose individuals' personally identifying information (PII) to almost anyone for ambiguous purposes. Routine use L does not define "source," suggesting that information can be disclosed to public, private, and potentially foreign or international entities that are not bound by the Privacy Act protections. The Privacy Act only applies to records maintained by United States government agencies, not to foreign, international, or private authorities.[56] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations. The same problem arises under routine use BB, which authorizes disclosure to foreign and international law enforcement authorities that are not subject to the Privacy Act. What's more, this routine use

[54] 83 Fed. Reg. 52420 (emphasis added).
[55] 83 Fed. Reg. 52420.
[56] 5 U.S.C. §552a(b).

authorizes disclosure without reasonable certainty that the information is actually necessary, such as where a record or combination thereof indicates merely a *potential* violation of law.

> Under proposed routine use Q, the agency may disclose information:
>
> To the U.S. Citizenship and Immigration Services for use in alien admission and naturalization inquiries.[57]
>
> Under proposed routine use Z, the agency may disclose information:
>
> To the Office of Personnel Management (OPM) for the purpose of addressing civilian pay and leave, benefits, retirement deduction, and any other information necessary for the OPM to carry out its legally authorized government-wide personnel management functions and studies.[58]

The proposed routine uses above, along with aforementioned routine uses L and BB, allow the agency to disclose personal information for purposes unrelated to the data's collection. The Records System is designed to help DoD help track and manage background investigations, and to support insider threat detection, prevention, and mitigation activities,[59] not to assist other agencies with immigration services, law enforcement, or addressing employee payroll and leave. 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."[60]

Because these routine uses significantly threaten the privacy of many individuals whose data is supplied for employment-related background investigation purposes only, DoD should withdraw these routine uses.

---

[57] 83 Fed. Reg. 52420.
[58] 83 Fed. Reg. 52420.
[59] *Id.*
[60] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

Under proposed routine use CC, the agency may disclose information:

> To any component of the Department of Justice for the purpose of representing DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.[61]

Similar to proposed routine use BB, this proposed routine use establishes a low standard for authorized disclosure because it is unclear that the records are truly necessary to effectuate a certain purpose. Under this proposed routine use, disclosure to assist in *potential* litigation is sufficient, allowing DoD to collect, store, and release potentially limitless amounts of an individual's sensitive information on the grounds that it might eventually be useful in a lawsuit that hasn't arisen yet. Moreover, this proposed routine use is discordant with the Privacy Act because it gratuitously puts the face of the agency above an individual's right to privacy. DoD should withdraw this proposed routine use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by DoD.

V. DoD Proposes Broad Exemptions for the Records System Against the Intent of the Privacy Act.

DoD proposes to exempt the Records System from several key Privacy Act obligations, such as the requirement that individuals be allowed to access and amend their personal records.

When Congress enacted the Privacy Act in 1974, it sought to limit government use and distribution of personal data.[62] In *Doe v. Chao*,[63] 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."[64]

---

[61] 83 Fed. Reg. 52420.
[62] S. Rep. No. 93-1183, at 2-3.
[63] *Doe v. Chao*, 540 U.S. 614 (2004).
[64] *Id*. at 618.

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DoD proposes to exempt the Records System from compliance with the following safeguards: 5 U.S.C. 552a(c)(1), (c)(3), (d), (e)(1)-(3), (e)(4)(G)-(I), (e)(5), (e)(8) and (g), among others. These provisions of the Privacy Act require agencies to:

- keep an accurate accounting of the data, nature, and purpose of records, as well as the name and address of the entity to whom disclosure is made;[65]
- grant individuals access to an accounting of when, why, and to whom their records have been disclosed;[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] and to inform individuals whom it asks to supply information about the extent of routine uses that authorize disclosure;[69]
- 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;[70]
- maintain all records with accuracy, relevance, timeliness, and completeness to ensure fairness when making determinations about an individual;[71]
- serve notice to an individual whose record is made available under compulsory legal process;[72]
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act;[73]

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

[65] 5 U.S.C. 552a(c)(1).
[66] *Id.* § 552a(c)(3).
[67] *Id.* §552a(d).
[68] *Id.* §552a(e)(1).
[69] *Id.* §552a(e)(3).
[70] *Id.* §552a(e)(4)(G), (H), (I).
[71] *Id.* §552a(e)(5).
[72] *Id.* §552a(e)(8).
[73] *Id.* §552a(g)(1).

categories of sources of records in the system. And the agency exempts itself from its Privacy Act duties under § 552a(e)(4)(G) and (H) to allow individuals to access and correct information in its records system. Put another way, 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 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.

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 DoD must narrow the exemptions it claims for the Records System.

VI. Conclusion

For the foregoing reasons, the proposed Records System is contrary to the Privacy Act, conflicts with the law, and exceeds agency authority. The Department of Defense must curtail the breadth of records contained in the Records System; withdraw proposed routine uses L, BB, Q, Z, and CC 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