epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Homeland Security

[Docket No. DHS–2020–0015] *and* [Docket No. DHS–2020–0014],

Privacy Act of 1974; System of Records *and* Privacy Act of 1974: Implementation of Exemptions; U.S. Department of Homeland Security/ALL–046 Counterintelligence Program System of Records

January 13, 2020

By notice published on December 14, 2020,[1] the Department of Homeland Security ("DHS") proposes to establish a Privacy Act system of records titled, "ALL-046 Counterintelligence Program System of Records ("Records System"). The Records System contains sensitive information—including biographical information, identifying documents, social security numbers, biometric information, financial information, medical information, and travel records. The Department also proposes to exempt the Records System from a number of significant provisions of the Privacy Act of 1974.[2]

In response to these notices, the Electronic Privacy Information Center urges DHS to (1) suspend the Records System until the agency narrows the scope of the system and resolves conflicting authorizations and (2) eliminate exemptions to §552a (e)(1), (e)(5), (e)(12), and (g)(1).

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

[1] Notice of Privacy Act system of records, 85 Fed. Reg. 80800, Dec. 14, 2020 [hereinafter "ALL-046 SORN"].
[2] Notice of proposed rulemaking, 85 Fed. Reg. 80667, Dec. 14, 2020 [hereinafter "ALL-046 NPRM"].

privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the Privacy Act safeguards enacted by Congress.[3]

I. The scope of the proposed Records System is broad and mismatched authorities of DHS components with access to the Records System present a risk of mission creep.

The proposed Records System contains the information of DHS employees and contractors, individuals "who are known, reasonably believed to be, or are suspected of being, involved in or linked to" intelligence activities, "officers, employees, or members of an organization reasonably believed to be owned or controlled directly or indirectly by a foreign power", individuals "reasonably believed to be targets, hostages, or victims of international terrorist organizations, transnational criminal organizations, or drug trafficking organizations", and individuals who request assistance from the Counterintelligence Program.[4] The proposed Records System also holds sensitive information of individuals "closely associated" with anyone in the above categories including family members and business partners.[5] DHS has proposed a broad scope of individuals, with a low threshold for inclusion.

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

[3] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, 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), http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. 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 Defense, Personal Vetting Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DoD-2018-OS-0076 and DoD-2018-OS-0075 (Nov. 16, 2018), https://epic.org/apa/comments/EPIC-Comments-DoD-Personnel-Vetting.pdf.

[4] ALL-046 SORN, 85 Fed. Reg. 80802-03.

[5] *Id*.

reports and tax returns), biometric data, and a litany of other sensitive information. The ability to collect nearly any type of information on a broad category of individuals risks serious privacy harms for individuals wrongly included in the Records System.

DHS created this new system of records to accommodate the expansion of the agency's Counterintelligence Program from two DHS components, Office of Information and Analysis and the United States Coast Guard, to nine more agency subcomponents: Cybersecurity and Infrastructure Security Agency (CISA), Countering Weapons of Mass Destruction Office (CWMD), Federal Emergency Management Agency (FEMA), Federal Protective Service (FPS), Transportation Security Administration (TSA), U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service (USSS).[6] DHS acknowledges that under Executive Order 12333 the Coast Guard is the only DHS component authorized to undertake clandestine counterintelligence information gathering.[7] The Coast Guard, and to a lesser extent I&A have authorization to collect information which other components lack. By feeding that information into a common system, a massive number of DHS employees will gain access to information obtained for limited counterintelligence purposes.

The mismatched authorities of components with access to the Records System poses a threat of mission creep in two ways. Mission creep occurs when an agency or component has access to more tools or information than it needs to complete its designed mission and expands into another role outside the designed mission to utilize those tools. First, the Coast Guard may be incentivized to use its clandestine information collection authority for purposes other than counterintelligence if information is requested by other DHS components. Second, allowing components not primarily

[6] 85 Fed. Reg. 80801.
[7] *Id*.

engaged in counterintelligence access to such a sensitive database may tempt those components to engage in counterintelligence operations without the requisite authority, or know-how.

II. The proposed scope of "Routine Uses" is inconsistent with the Privacy Act of 1974.

The definition of "routine use" is precisely tailored and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. However, DHS proposes 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.

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."[8] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[9] One of these exemptions is "routine use."[10]

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.[11]

[8] 5 U.S.C. § 552a(b).
[9] *Id.* § 552a(b)(1) – (12).
[10] *Id.* § 552a(b)(3).
[11] Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy, 1031 (1976).

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted routine use to mean that a "not only compatible with, but related to, the purpose for which the record is maintained."[12]

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."[13] 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."[14]

The routine uses contained in the proposed Records System provide the agency with nearly unlimited authority to disclose individuals' personal information to other federal agencies, state and local law enforcement, and private companies. In particular, routine uses G, H, and J vastly expand DHS's authority to disclose information in conflict with the Privacy Act's language, legislative history, and interpretative case law.

Under proposed routine use G the agency may disclose information:

> To an appropriate Federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory

[12] *Id.*
[13] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[14] *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).

violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.[15]

Under proposed routine use H the agency may disclose information:

To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.[16]

Under proposed routine use J the agency may disclose information:

To any Federal, state, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations, with responsibilities relating to homeland security, including responsibilities to counter, deter, prevent, prepare for, respond to, or recover from a natural or manmade threat, including an act of terrorism, or to assist in or facilitate the coordination of homeland security threat awareness, assessment, analysis, deterrence, prevention, preemption, and response.[17]

The proposed routine uses above authorize DHS to disclose individuals' personally identifying information (PII) to almost anyone for ambiguous purposes. Routine use G provides DHS agents a wide degree of latitude to decide whether a record indicates a potential violation of criminal, civil, or administrative law. Routine use G also permits disclosure to foreign, or international entities that are not bound by Privacy Act protections. The Privacy Act only applies to records maintained by United States government agencies, not to foreign, international, or private authorities.[18] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations.

Routine use H creates substantial risks of data breach by authorizing disclosure of sensitive personally identified information to private contractors and their subcontractors. Routine use H also

[15] 85 Fed. Reg. 80804.
[16] *Id*.
[17] *Id*.
[18] 5 U.S.C. §552a(b).

permits disclosure of personal information to these individuals for reasons inconsistent with the purpose the information was collected for. Routine use J permits disclosure to any entity with "with responsibilities relating to homeland security" including foreign and international entities, and private sector individuals. Routine use J further puts no restrictions on the reason for disclosure to these entities, many of which are not covered by the Privacy Act. In total these routine uses allow the agency to disclose personal information for purposes unrelated to the data's collection, and without the individual's consent.

III. The Records System creates a substantial risk of data breach.

Recent data breaches and hacks within DHS and across the federal government demonstrate that the agency is incapable of safeguarding sensitive personal information. In 2016 the U.S. Government Accountability Office warned that "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[19] The GAO called on DHS to enhance cybersecurity protection in key areas including intrusion detection and prevention. At the time DHS had not even put in place an adequate process for disseminating information on intrusions and potential malicious activity.[20] Since that time DHS and its subcomponents have not shown that they are capable of safeguarding personally identifiable information, particularly biometric data.

DHS and agencies across the federal government were recently exposed in the SolarWinds hack.[21] Hackers gained access to systems across the federal government despite DHS's complex cybersecurity defense systems, and a 2018 warning from the GAO that agencies were vulnerable to

[19] 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) (*hereinafter* 2016 GAO Report), http://www.gao.gov/assets/680/674829.pdf.
[20] *Id*. at 27.
[21] Megan Roos, *Suspected Russian SolarWinds Hack Compromised Homeland Security Department*, Newsweek (Dec. 14, 2020), https://www.newsweek.com/suspected-russian-solarwinds-hack-compromised-homeland-security-department-1554656.

the exact type of "supply chain" attack used by the SolarWinds hackers.[22] The SolarWinds software underlying the hack was first compromised in March, but DHS did not become aware it had been breached until December 2020. While it is not yet clear exactly what data was accessed, hackers were able to breach DHS Microsoft systems and set up false credentials for other systems, giving them "the keys to the kingdom" according to security experts.[23]

In 2019 a data breach at CBP subcontractor Perceptics, LLC exposed approximately 184,000 images of travelers from CBP's Biometric Entry/Exit pilot.[24] Perceptics staff were able to violate several DHS security and privacy protocols to download the images used for facial recognition without CBP's IT security controls preventing the unauthorized action or sounding an alarm.[25] When Perceptics, LLC was subsequently hacked outside agents had access to those 184,000 images and an additional 105,000 license plate images.[26] At least 19 facial recognition images were released on the dark web.[27] DHS's Office of the Inspector General found that, "Perceptics was able to make unauthorized use of CBP's biometric data, in part because CBP did not implement all available IT security controls, including an acknowledged best practice."[28] OIG concluded that CBP "[d]id not adequately fulfill its responsibilities for IT security".[29]

The 2019 breach is far from the only example of DHS and its' subcomponents failing to safeguard sensitive information. The Federal Emergency Management Agency (FEMA)

---

[22] Brian Barrett, *Security News This Week: Russia's SolarWinds Hack Is a Historic Mess*, Wired (Dec. 19, 2020), https://www.wired.com/story/russia-solarwinds-hack-roundup/.
[23] Brian Fung, *SolarWinds hackers gave themselves top administrative privileges to spy on victims undetected, DHS says*, CNN (Jan. 8, 2020), https://www.cnn.com/2021/01/08/politics/solarwinds-russia-hack-cisa-bulletin/index.html.
[24] Joseph Cuffari, Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot, Dep't of Homeland Sec. Off. of Inspector Gen. (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.
[25] *Id*. at 6.
[26] *Id*. at 8.
[27] *Id*. at 13.
[28] *Id*. at 12.
[29] *Id*.

unnecessarily disclosed sensitive information of victims of the 2017 California wildfires, exposing up to 2.3 million people.[30] FEMA shared details of victims financial institutions and personal lives including EFT and bank transit numbers and complete addresses.[31] The unidentified subcontractor then failed to notify FEMA of receiving extra information.[32] A 2017 data breach by an agency employee exposed the personal information, including Social Security numbers, of 247,167 DHS employees.[33] DHS's recent track record demonstrates that the agency has failed to implement adequate safeguards for personal data.

Data breaches are common across the federal government as well, exposing the PII of millions to exploitation and abuse. As an example of the trend across the federal government, a 2015 data breach at the Office of Personnel Management (OPM) exposed social security numbers and other personal data from 21.5 million individuals.[34] Around the same time OPM reported another major data breach exposing records on about 4 million federal employees.[35] Again in 2015, approximately 390,000 tax accounts with the Internal Revenue Service were compromised, revealing SSNs, dates of birth and street addresses among other PII.[36] In September 2014, a breach at the United States Postal Service led to the loss of PII from more than 800,000 employees.[37] In sum, data

[30] Christopher Mele, *Personal Data of 2.3 Million Disaster Victims Was Released by FEMA, Report Says*, N.Y. Times (Mar. 22, 2019), https://www.nytimes.com/2019/03/22/us/fema-data-breach.html, John V. Kelly, Management Alert – FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information, OIG-19-32 Dep't of Homeland Sec. Off. of Inspector Gen. (Mar. 15, 2019), https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-32-Mar19.pdf.
[31] OIG FEMA Memorandum at 4.
[32] *Id*.
[33] Steven Musil, *Homeland Security breach exposes data on 240,000 employees*, CNET (Jan. 3, 2018), https://www.cnet.com/news/homeland-security-breach-exposes-data-on-240000-employees/, Dep't. of Homeland Sec., Privacy Incident Involving DHS Office of Inspector General Case Management System (Update) (Jan. 18, 2018), https://www.dhs.gov/news/2018/01/18/privacy-incident-involving-dhs-oig-case-management-system-update.
[34] 2016 GAO Report, *supra* note 19, at 8.
[35] *Id*.
[36] *Id*. at 7-8.
[37] *Id*. at 8.

breaches at federal agencies have grown exponentially more common in the last decade, from a reported 5,503 breaches in 2006 to 35,277 reported in 2019.[38] Both DHS and the federal government have track records of failing to secure personally identifiable information, resulting in the disclosure of sensitive information on millions of individuals.

DHS should not seek to collect sensitive personally identifiable information on more individuals when the agency cannot even protect the data it currently holds. This Records System creates a particularly serious risk of data breach as the routine uses permit disclosure to a broad array of state, local, and international agencies as well as private parties and DHS contractors. Permitting DHS contractors to handle sensitive information magnifies the risk of data breach because the information is stored away from government systems where it is difficult for DHS to prevent or detect hacks or data theft. Failure to supervise a government contractor was the cause of the 2019 Perceptics data breach. DHS will create similar risks for individuals with information in the proposed Records System by sharing counterintelligence information with private contractors.

IV. DHS's proposed exemptions are unnecessary and allow for unchecked information collection.

DHS proposes to exempt the Records System from fourteen provision of the Privacy Act of 1974, completely eliminating individuals' rights to determine how their information is being used and correct harmful errors.[39] Some exemptions also thwart DHS's public notice obligations and limits on data collection under the Privacy Act.

[38] U.S. Gov't Accountability Office, GAO-20-629 Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy (Aug. 18, 2020), https://www.gao.gov/assets/710/709555.pdf, U.S. Gov't Accountability Office, GAO-19-105 Information Security: Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting against Intrusions (Dec. 18, 2018), https://www.gao.gov/assets/700/696105.pdf, 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.
[39] 85 Fed. Reg. 80668.

When Congress enacted the Privacy Act in 1974, it sought to limit government use and distribution of personal data.[40] In *Doe v. Chao*,[41] 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."[42]

DHS's proposed exemptions make it impossible for individuals to correct harmful errors in ALL-046 System records. DHS proposes to exempt the Records System §552(a) (d) Access and Amendment to Records, (e)(2) Collection of Information from Individuals, (e)(3) Notice to Subjects, (e)(8) Notice on Individuals, and (g)(1) Civil Remedies. Together these provisions function to give individuals the ability to determine whether their information exists in an agency's system and obtain relief when that information is inaccurate. DHS proposes to exempt information in the Records System from these requirements wholesale, instead of asserting narrower provisions for certain records within the system. These exemptions are particularly concerning in light of DHS's routine use G, which permits the agency to disclose information to state, local, and international agencies for the enforcement of laws and regulations.[43] DHS may provide information to a broad array of agencies making determinations about individuals rights and legal liability but need not ensure that that information is accurate or correct information when an individual demonstrates it is wrong. The sweep of the above exemptions not only prevents individuals from knowing when their information is in a system but bars them from correcting that information when it causes harm.

[40] S. Rep. No. 93-1183, at 2-3.
[41] *Doe v. Chao*, 540 U.S. 614 (2004).
[42] *Id*.
[43] 85 Fed. Reg. 80804.

Exemption from §552a(e)(1), Relevancy and Necessity of Information, permits unlimited data collection. DHS has claimed an exemption to §552a(e)(1) on the grounds that "[i]n the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity."[44] This provision requires DHS to:

> "maintain in its records only such information 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;"

DHS's claimed exemption thwarts the basic purpose of the Privacy Act, that agencies limit information collection to the what the agency actually needs. Under the claimed exemption DHS components may collect and store information without any justification. DHS has not placed any limits on the exemption, so the proposed Records System is exempt from one of the core protections of the Privacy Act.

Similarly, DHS proposes to exempt the Records System from §552a(e)(12), the requirement that agencies disclose to the public when the agency establishes a computer matching program to share information with a non-Federal agency. DHS claims that disclosing the existence of a computer matching system would "would impair DHS operations by indicating which data elements and information are valuable to DHS's analytical functions". Such an exemption is unnecessary as computer matching disclosure does not require DHS to publish minute details of the information the agency will receive. DHS's computer matching notices only disclose the participating parties, authority for the matching program, the purpose of the program, categories of individuals, and the categories of records. All of this information is disclosed in the underlying SORN. While the computer matching disclosure requirement is a useful tool for public oversight it does not require DHS to disclose substantially more information than in the ALL-046 SORN.

[44] 85 Fed. Reg. 80668.

The scope of exemptions DHS proposes, especially when read with the scope of routine uses, would permit DHS to collect a nearly unlimited amount of information and distribute that information without notice or consent of individuals. Such broad authority flies in the face of the Privacy Act which sought to limit the information federal agencies could collect and provide individuals with meaningful remedies when agencies overstepped and caused harm. 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.

Conclusion

EPIC urges DHS to suspend the Records System until the agency narrows the scope of the system, resolves mismatched authorities to reduce the risk of mission creep, and takes further steps to mitigate the risk of data breach. Furthermore, DHS should substantially narrow the claimed exemptions to subsets of sensitive records in the system and specifically remove exemptions (e)(1) and (e)(12).

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

Jake Wiener
Jake Wiener
EPIC Law Fellow