epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974; Implementation of Exemptions; Department of Homeland Security/ALL—038 Insider Threat Program System of Records

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

[Docket Nos. DHS-2019-0033 and 0034]

April 9, 2020

By notice published on March 10, 2020,[1] the Department of Homeland Security ("DHS") proposes to modify an existing Privacy Act system of records titled "Department of Homeland Security/ALL—038 Insider Threat Program System of Records" ("Insider Threat Database" or "DHS Database"). The Insider Threat Database will include detailed, personal data on an unusually large number of individuals, including "present and former DHS employees, contractors, detailees, assignees, interns, visitors, and guests."[2] The Insider Threat Database will also include information on "persons who report concerns, witnesses, relatives, and individuals

[1] Notice of modified Privacy Act System of Records, 85 Fed. Reg. 13914 (proposed Mar. 10, 2020) [hereinafter "Modified Insider Threat SORN"].
[2] *Id.* at 13915.

with other relevant personal associations with a DHS insider."[3] The DHS database will include social security numbers, personal emails, license plate numbers, medical information, biometric data, and social media posts. The scope of individuals covered by the "insider threat" database is broad and ambiguous; the extent of the data collection is essentially unbounded.

The DHS proposes to exempt the modified "Insider Threat" Database from several significant provisions of the Privacy Act of 1974.[4] Pursuant to DHS's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) address the substantial privacy and security issues raised by the database; (2) recommend that the DHS narrow the scope of individuals included in the database; (3) recommend that DHS withdraw unlawful and unnecessary proposed routine use disclosures; and (4) urge DHS to significantly narrow the Privacy Act exemptions for the system.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the Privacy Act safeguards enacted by Congress.[5] EPIC also routinely interacts with

[3] *Id.*
[4] Notice of Proposed Rulemaking, 85 Fed. Reg. 13831 (proposed Mar. 10, 2020) [hereinafter "Insider Threat NPRM"].
[5] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, Docket No. DHS-2018-0029 (Oct. 26, 2018), *available at* https://epic.org/apa/comments/EPIC-Comments-DHS-Correspondence-Records.pdf; 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), *available at* 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), *available at* 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

DHS and subcomponents of DHS through formal meetings held by the agency. Thus, EPIC staff, in exercising First Amendment rights including the right to "petition the government for a redress of grievances," would be subject to the Insider Threat database, which is also contrary to the Privacy Act[6]

1. Purpose and Scope of the "Insider Threat" Database

Executive Order 13587, titled "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," ordered federal agencies to create "insider threat detection and prevention program[s]" and "to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties."[7]

According to the modified SORN for the Insider Threat database, "pursuant to a memorandum, *Expanding the Scope of the Department of Homeland Security Insider Threat Program*, the scope of the program will now include all individuals 'with past or current access to DHS facilities, information, equipment, networks, or systems."[8] The memorandum also authorized additional information to be included in the database.[9]

Entry Program, Docket No. USCBP-2008-0097 (Jan. 19, 2010), *available at* http://epic.org/privacy/global_entry/EPIC-Comments-Global-Entry-2010.pdf.

[6] 5 U.S.C. 552a(e)(7)("Agency Requirements.—Each agency that maintains a system of records shall— . . . maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.").

[7] Exec. Order No. 13,587, 76 Fed. Reg. 63,811 (Oct. 7, 2011).

[8] Modified Insider Threat SORN at 13914.

[9] *Id.*

2. The Modified "Insider Threat" DHS Database Would Maintain a Massive Amount of Personal, Sensitive Information About a Wide Variety of Individuals

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

According to the modified Insider Threat SORN, the DHS Database will include an exorbitant amount of personal information about an expansive array of individuals. The Database would include: name, date of birth, social media information, ethnicity and race, gender, medical reports, background reports that include medical and financial data, travel records, and "information on family members, dependents, relatives and other personal associations."[10] 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 Insider Threat database faces significant risk of compromise. According to a report by the U.S. Government Accountability Office (GAO), "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[11] This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[12] 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

[10] Modified Insider Threat SORN at 13915-16.
[11] 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.
[12] *Id.* at 8.

sensitive information.[13] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[14]

Data breaches have directly impacted DHS information systems in recent years. For example, in 2018, DHS had a data breach that exposed the information of more than 240,000 current and former DHS employees.[15] Last year, Customs and Border Protection, a subcomponent of DHS, suffered the loss "tens of thousands of images of travelers and license plates."[16] In 2014, a DHS contractor conducting background investigations for the agency experienced a data breach that compromised the records of at least 25,000 employees, including undercover investigators.[17] Another DHS contractor suffered a data breach that affected as many as 390,000 people associated with DHS, including current and former employees as well as contractors and job applicants.[18] Overall, the number of government data breaches, including for DHS, has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[19]

The latest series of high-profile government data breaches indicates that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. Indeed, GAO released a report on widespread cybersecurity weaknesses throughout the executive branch, aptly titled "Federal Agencies Need to Better Protect Sensitive Data."[20] According to the

---

[13] *Id*. at 7-8.
[14] *Id*. at 8.
[15] Greg Otto, *DHS Confirms Data Breach Affecting More Than 240,000 Current and Former Employees*, CYBERSCOOP (Jan. 3, 2018), https://www.cyberscoop.com/dhs-data-breach-oig-office-january-2018/.
[16] Zolan Kanno-Youngs and David E. Sanger, *Border Agency's Images of Travelers Stolen in Hack*, N.Y. TIMES (June 10, 2019), https://www.nytimes.com/2019/06/10/us/politics/customs-data-breach.html.
[17] Jim Finkle & Mark Hosenball, *U.S. Undercover Investigators Among Those Exposed in Data Breach*, REUTERS (Aug. 22, 2014), http://www.reuters.com/article/us-usa-security-contractor-cyberattack-idUSKBN0GM1TZ20140822.
[18] Alicia A. Caldwell, *390,000 Homeland Employees May Have Had Data Breached*, ASSOCIATED PRESS (June 15, 2015), http://www.pbs.org/newshour/rundown/390000-homeland-employees-may-have-had-data-breached/.
[19] 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.
[20] *Id*.

report, a majority of federal agencies, "including the Department of Homeland Security, have weaknesses with the design and implementation of information security controls …."[21] In addition, most agencies "have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware."[22] The GAO report concluded that, due to widespread cybersecurity weaknesses at DHS and most other federal agencies, "federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats."[23]

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

b. DHS Insider Threat Database Covers Broad Categories of Individuals and Implicates Individuals Who Are Not Under Investigation

The DHS proposes to collect personal, sensitive information on a large group of individuals, including individuals that are not themselves under DHS investigation. The DHS Insider Threat database would contain records on:

[21] *Id*. at unpaginated "Highlights" section.
[22] *Id*.
[23] *Id*. at 12.

> …present and former DHS employees, contractors, detailees, assignees, interns, visitors, and guests. In addition, persons who report concerns, witnesses, relatives, and individuals with other relevant personal associations with a DHS insider . . . .[24]

By collecting, maintaining, and disclosing the records of family members and acquaintances of individuals who may be subject to investigation, DHS proposes to create detailed profiles on individuals who are not themselves the target of any investigation.

The DHS should remove "relatives, and individuals with other relevant personal associations" from the proposed categories of records. Moreover, DHS routinely hosts non-governmental organizations (NGOs) and civil liberties groups at DHS facilities to solicit feedback on programs that implicate privacy and civil liberties. *Accordingly, DHS should clarify that records kept on "visitors, and guests" will not include NGOs.*

3. Proposed Routine Uses Would Circumvent Privacy Act Safeguards and Contravene Legislative Intent

The Privacy Act's definition of "routine use" is precisely tailored, and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. DHS's modified 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, DHS exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[25] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by

[24] Modified Insider Threat SORN at 13915.
[25] S. Rep. No. 93-1183 at 1 (1974).

Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[26]

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."[27] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[28] One of these exemptions is "routine use."[29] "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."[30]

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.[31]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[32]

---

[26] Pub. L. No. 93-579 (1974).
[27] 5 U.S.C. § 552a(b).
[28] *Id*. §§ 552a(b)(1) – (12).
[29] *Id*. § 552a(b)(3).
[30] 5 U.S.C. § 552a(a)(7).
[31] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[32] *Id*.

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."[33] 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."[34]

The modified Insider Threat SORN proposes numerous routine uses that are incompatible with the purpose for which the data was collected, as required by law.[35]

Proposed Routine Use I would permit the agency to disclose information contained in the "Insider Threat" Database:

> To an appropriate Federal, State, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.[36]

---

[33] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[34] *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).
[35] *Id*.
[36] Modified Insider Threat SORN at 13917.

Proposed Routine Use J would permit DHS to disclose information contained in the Database:

> To a prospective or current employer . . . to the extent necessary to determine employment eligibility.[37]

Proposed Routine Use L would permit DHS to disclose information:

> To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.[38]

DHS proposes to disclose "Insider Threat" information for purposes that do not relate to detecting and preventing insider threats. Determinations regarding employment, licensing, and other benefit eligibility, as contemplated by Routine Uses I, J, and L are entirely unrelated to this purpose. 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."[39] Routine Uses I, J, and L unlawfully exceed DHS authority and should be removed from the Insider Threat SORN.

DHS also proposes to create an exemption to the Privacy Act that would permit the agency to release personal information if – incredibly – such disclosure would "preserve confidence" in the agency or "demonstrate accountability." Proposed Routine Use T would permit the agency to disclose information:

> To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS' officers, employees, or individuals covered by the system,

[37] *Id*.
[38] *Id*.
[39] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.[40]

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS"[41] in Routine Use T is discordant with the Privacy Act because it gratuitously puts the face of the agency above an individual's right to privacy. The term "necessary" is ambiguous; DHS could take advantage of this criterion to unduly influence its image. DHS should remove 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 DHS.

In addition, the proposed routine uses that would permit DHS to disclose records, subject to the Privacy Act, to foreign, international, and private entities should be removed. The Privacy Act only applies to records maintained by United States government agencies.[42] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations.

EPIC urges the DHS to withdraw these proposed routine uses. They would circumvent Privacy Act safeguards and contravene legislative intent.

4. DHS Proposes Broad Exemptions for the modified "Insider Threat" Database, Contravening the Intent of the Privacy Act of 1974

DHS proposes to exempt the Database from key Privacy Act obligations, such as the requirement that records be accurate and relevant, or that individuals be allowed to access and amend their personal records.

[40] Modified Insider Threat SORN at 13917.
[41] *Id*.
[42] 5 U.S.C. § 552a(b).

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that federal agencies were able to collect.[43] Congress further required agencies to be transparent in their information practices.[44] In *Doe v. Chao*,[45] 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."[46]

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DHS proposes to exempt the Database from compliance with the following safeguards: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12); (f); and (g)(1).[47] 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;[48]
- inform parties to whom records have been disclosed of any subsequent corrections to the disclosed records;[49]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[50]
- 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";[51]
- collect information from the individual to the greatest extent possible, when such information would have an adverse effect on the individual;[52]

[43] S. Rep. No. 93-1183, at 1 (1974).
[44] *Id*.
[45] *Doe v. Chao*, 540 U.S. 614 (2004).
[46] *Doe*, 540 U.S. at 618.
[47] 81 Fed. Reg. 9789, 9790.
[48] 5 U.S.C. § 552a(c)(3).
[49] *Id.* § 552a(c)(4).
[50] *Id*. § 552a(d).
[51] *Id*. § 552a(e)(1).
[52] *Id*. § 552a(e)(2).

- inform individuals from whom they request information the purposes and routine uses of that information, and the effect of not providing the requested information;[53]
- 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;[54]
- ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[55]
- 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;[56]
- serve notice to an individual whose record is made available under compulsory legal process;[57]
- provide public notice prior to the establishment or revision of a computerized comparison of the system of records with non-Federal records;[58]
  and
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act.[59]

Several of DHS's claimed exemptions would further exacerbate the impact of its overbroad categories of records and routine uses in this system of records. DHS exempts itself from § 552a(e)(1), which requires agencies to maintain only those records relevant to the agency's statutory mission. The agency exempts itself from § 552a(e)(4)(I), which requires agencies to disclose the categories of sources of records in the system. And the agency exempts itself from its Privacy Act duties under to § 552a(e)(4)(G) and (H) to allow individuals to access and correct information in its records system. In other words, DHS 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 DHS's proposal to collect and retain

[53] *Id*. § 552a(e)(3).
[54] *Id*. § 552a(e)(4)(G), (H), (I).
[55] *Id*. § 552a(e)(5).
[56] *Id*. § 552a(f).
[57] *Id.* § 552a(e)(8).
[58] *Id.* § 552a(e)(12).
[59] *Id.* § 552a(g)(1).

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.

DHS also proposes exemption from maintaining records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[60] In other words, DHS admits that it contemplates collecting information that will not be relevant or necessary to a specific investigation. The agency's alleged purpose in consciously flouting this requirement is to establish "patterns of unlawful activity."[61] 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.[62] By implication, the agency objects to guaranteeing "fairness" to individuals in the "Insider Threat" Database.[63]

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 concerns to the American public – the protection of personal privacy. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of database records, and DHS must reign in the exemptions it claims for its "Insider Threat" Database.

EPIC urges the DHS to withdraw these proposed exemptions. They would circumvent Privacy Act safeguards and contravene legislative intent.

[60] 5 U.S.C. § 552a(e)(5).
[61] Insider Threat NPRM at 13832.
[62] *Id*.
[63] *Id*.

5. Conclusion

For the foregoing reasons, the modified "Insider Threat" Database is contrary to the core purpose of the federal Privacy Act. Accordingly, DHS must limit the records contained in the Database and the individuals to whom the records pertain, narrow the scope of its proposed Privacy Act exemptions, and remove the proposed unlawful routine use disclosures from the Insider Threat SORN.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Jeramie Scott
EPIC Senior Counsel