PUBLIC SUBMISSION

Docket: PBGC-2019-0004
Privacy Act Regulation; Exemption for Insider Threat Program Records

Comment On: PBGC-2019-0004-0001
Privacy Act Regulation; Exemption for Insider Threat Program Records

Document: PBGC-2019-0004-DRAFT-0001
Comment on FR Doc # 2019-14604

Submitter Information

Name: Kermit Kubitz

General Comment

The exemption for insider threat program records should have the following limitations:

1. Any data which is subject to breach or hacking should be made available to affected individuals and other interested persons, including the journalism community.

2. The use of such data must be strictly limited to necessary purposes. Broad collection of personal data, for the reasons described in the attachment, without access for review or correction of improper or unnecessary data should not be permitted.

3. An objective third party should be an option for review of data if requested by an affected individual or group, subject to reasonable confidentiality protections necessary to protect any legitimate law enforcement or investigatory purposes.

Changes should be made to the regulations to consider these issues.

Attachments

EPIC-DOJ-Insider-Threat-Database

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 JUSTICE

Privacy Act of 1974; Implementation

Privacy Act of 1974; System of Records

[CPCLO Order Nos. 001–2017 and 002–2017]

June 30, 2017

By notice published on June 5, 2017,[1] the United States Department of Justice ("DOJ") proposed to establish a new Privacy Act system of records JUSTICE/DOJ-018, "DOJ Insider Threat Program Records ("Insider Threat Database"). This database will replace the previously proposed and rescinded "FBI Insider Threat Program Records." The Database will include detailed, personal data on a large number of individuals who have authorized access to DOJ facilities, information systems, or classified information including present and former DOJ employees, contractors, detailees, assignees, interns, visitors, and guests. The scope of "insider threat" is broad and ambiguous; the extent of data collection is essentially unbounded.

By notice published on June 5, 2017,[2] the DOJ proposes to exempt the Insider Threat Database from several significant provisions of the Privacy Act of 1974. Pursuant to the DOJ's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) underscore the substantial privacy and security issues raised by the database; (2) recommend the

[1] *Privacy Act of 1974; System of Records*, 82 Fed. Reg. 25,812, Jun. 5, 2017 [hereafter "Insider Threat SORN"].
[2] *Privacy Act of 1974; Implementation*, 82 Fed. Reg. 25,751 [hereafter "Insider Threat NPRM"].

DOJ withdraw unlawful and unnecessary proposed routine use disclosures and; (3) urge the FBI to significantly narrow the Privacy Act exemptions for its Database.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards, established by Congress, in the development of new information systems operated by the federal government.[3]

Purpose and Scope of the "Insider Threat" Database

Executive Order 13587, titled "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," ordered federal agencies to create "insider threat detection and prevention program[s]" and "to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties."[4] According to the DOJ, the proposed "Insider Threat" Database would manage insider threats within the DOJ in

[3] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, *Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records*, Jun. 5, 2017, https://epic.org/apa/comments/EPIC-DHS-FALCON-Database-Comments.pdf; Comments of EPIC to the Department of Defense, *DUSDI 01-DoD, Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) and DoD Component Insider Threat Records System*, Jun. 20, 2016, https://epic.org/apa/comments/EPIC-Comments-DoD-Insider-Threat-Database.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, https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf; Comments of EPIC to the Department of Homeland Security, *Notice of Privacy Act System of Records, Docket No. DHS-2011-0094*, Dec. 23, 2011, http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, *001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085,* Dec. 15, 2010, http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the United States Customs and Border Protection; *Department of Homeland Security on the Establishment of Global Entry Program, Docket No. USCBP-2008-0097,* Jan. 19, 2010, http://epic.org/privacy/global_entry/EPIC-Comments-Global-Entry-2010.pdf.

[4] Exec. Order No. 13,587, 76 Fed. Reg. 63,811 (Oct. 7, 2011). *See also* Insider Threat SORN at 25813.

accordance with E.O. 13587.[5] The FBI provides a non-exhaustive list of "insider threats," which include, but are not limited to:

> Accessing, gathering, integrating, assessing, and sharing information and data derived from offices across the organization for a centralized analysis, reporting, and response; monitoring user activity on classified computer networks controlled by the Federal Government; evaluating personnel security information; and establishing procedures for insider threat response actions, such as inquiries, to clarify or resolve insider threat matters.[6]

The DOJ states that the proposed database may include information from (1) all relevant counterintelligence and security database files; (2) all relevant Unclassified and Classified network information and; (3) all relevant Human Resources databases and files.[7] As discussed below, the FBI proposes to disclose information within the Database to multiple entities not subject to the Privacy Act, including state, local, tribal, or foreign law enforcement, private organizations, contractors, grantees, consultants, and the news media."[8]

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

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

According to the Insider Threat SORN, the FBI Database will likely include an exorbitant amount of personal information about an expansive array of individuals. The Database could potentially include personnel files, payroll and voucher files, personal contact records, polygraph examination reports, facility access files, travel records, foreign contact reports, and financial disclosure filings. [9]

---

[5] *Id*.
[6] *Id*. at 25813.
[7] *Id.*at 25814.
[8] *Id.*at 25814-5.
[9] *Id*. at 25814.

Given the FBI's statements that personnel records will be included in the database it is likely that the Database will contain information derived from Standard Form 86, Questionnaire for National Security Positions (SF-86). SF-86 is a 127-page form used to conduct background checks for federal employment in sensitive positions, a process the D.C. Circuit has described as "an extraordinarily intrusive process designed to uncover a vast array of information …."[10] SF-86 includes such personal and sensitive information as an individual's name; date of birth; Social Security Number (SSN); address; social media activity; personal and official email addresses and phone numbers; citizenship, ethnicity and race; employment and educational history; 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 included in SF-86 was a focal point of the 2015 Office of Personnel Management (OPM) data breaches, which compromised the personal information of 21.5 million people, including 1.8 million people who did not apply for a background check.[11] The OPM breach exposed sensitive SF-86 forms spanning three decades.[12] The fingerprints of 5.6 million people were also stolen in the data breach.[13] 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.[14]

---

[10] *Willner v. Thornburgh*, 928 F.2d 1185, 1191 (D.C. Cir. 1991).
[11] 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/.
[12] 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.
[13] 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/.
[14] *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/.

The categories of records contained in the "Insider Threat" Database represent a wealth of sensitive information that is typically afforded the highest degree of privacy and security protections, such as health,[15] financial,[16] and education[17] records; Social Security Numbers;[18] and individuals' photographs or images.[19] Federal contractors, security experts, and EPIC have previously argued to the U.S. Supreme Court that much of this information simply should not be collected by the federal governments.

In *NASA v. Nelson*,[20] 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).[21] 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.[22] EPIC also argued that compelled collection of sensitive data would place at risk personal health information that is insufficiently protected by the agency.[23] 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.[24]

---

[15] *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.).
[16] *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.).
[17] *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012).
[18] *See* Driver's Privacy Protection Act, 18 U.S.C. § 2725(4) (defining "highly restricted personal information" to include "social security number").
[19] *Id*. § 2725(4) (defining "highly restricted personal information" to include "individual's photograph or image").
[20] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[21] 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.
[22] *Id*. at 20-28
[23] *Id*.
[24] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).

That turned out not to be true. Shortly after the Court's decision, NASA experienced a significant data breach that compromised the personal information of about 10,000 employees, including Robert Nelson, the JPL scientist who sued NASA over its data collection practices.[25] The JPL-NASA breach is a clear warning about why the FBI should narrow the amount of sensitive data collected. Simply put, the government should not collect so much data; to do so unquestionably places people at risk.

Given the recent surge in government data breaches, the vast amount of sensitive information contained in the FBI Database faces significant risk of compromise. According to a recent report by the U.S. Government Accountability Office (GAO), "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[26] This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[27] 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.[28] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[29]

The latest series of high-profile government data breaches indicates that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. Indeed, GAO recently released a report on widespread cybersecurity weaknesses throughout the

[25] 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.
[26] 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"].
[27] GAO Cybersecurity Report at 8.
[28] *Id*. at 7-8.
[29] *Id*. at 8.

executive branch, aptly titled "Federal Agencies Need to Better Protect Sensitive Data."[30] According to the report, a majority of federal agencies, "have weaknesses with the design and implementation of information security controls …."[31] 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."[32] The GAO report concluded that, due to widespread cybersecurity weaknesses at most 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."[33]

The DOJ is not insulated from the increase in government database breaches. Recently, a 16-year-old teenage boy was arrested in connection with hacks that exposed the information of more than 20,000 FBI employees and 9,000 Department of Homeland Security ("DHS") employees, as well as the personal email accounts of DHS Secretary Jeh Johnson and Central Intelligence Agency (CIA) director John Brennan.[34] Overall, the number of government data breaches has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[35]These weaknesses in FBI 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, the DOJ should maintain only records that are relevant and necessary to detecting and preventing insider threats. To the extent that the DOJ continues to collect this vast array of sensitive personal information, DOJ should limit disclosure to only those agencies

[30] GAO Sensitive Data Protection Report.
[31] *Id*. at unpaginated "Highlights" section.
[32] *Id*.
[33] *Id*. at 12.
[34] 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.
[35] 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"].

and government actors that require the information as a necessity. Further, DOJ should strictly limit the use of this information to the purpose for which it was originally collected.

b. DOJ Database Covers Broad Categories of Individuals and Implicates Individuals Who Are Not Under Investigation

The DOJ proposes to collect the aforementioned personal, sensitive information on a large group of individuals, including individuals that are not themselves under DOJ investigation. The DOJ Database would contain records on "former DOJ employees, members of joint task forces under the purview of DOJ, contractors, detailees, asssigness, interns, visitors, and guests."[36]

By collecting, maintaining, and disclosing the records of anyone with access to DOJ facilities and information systems the DOJ proposes to create detailed profiles on individuals who are not themselves the target of any investigation. The DOJ routinely hosts non-governmental organizations (NGOs) and civil liberties groups at DOJ facilities to solicit feedback on programs that implicate privacy and civil liberties. Accordingly, the DOJ should clarify that the records kept will not include NGOs or any other private individuals who visit DOJ facilities.

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. The DOJ's Insider Threat Database contains a potentially broad category of personally identifiable information. By disclosing information in a manner inconsistent with the purpose for which the information was originally gathered, the DOJ exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

[36] Insider Threat SORN at 25813.

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.[37] 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."[38]

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

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.[43]

---

[37] S. Rep. No. 93-1183 at 1 (1974).
[38] Pub. L. No. 93-579 (1974).
[39] 5 U.S.C. § 552a(b).
[40] *Id*. §§ 552a(b)(1) – (12).
[41] *Id*. § 552a(b)(3).
[42] 5 U.S.C. § 552a(a)(7).
[43] *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 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."[44]

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."[45] 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."[46]

The Insider Threat SORN proposes numerous routine uses that are incompatible with the purpose for which the data was collected, as required by law.[47] Proposed Routine Use I would permit the agency to disclose information contained in the "Insider Threat" Database:

> To the news media or members of the general public in furtherance of a legitimate law enforcement or public safety function as determined by the DOJ…where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy.[48]

---

[44] *Id*.
[45] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[46] *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).
[47] *Id*.
[48] Insider Threat SORN at 25814.

Proposed Routine Use L would permit the FBI to disclose information:

> To appropriate officials and employees of a Federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the assignment, detail, or deployment of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit.[49]

Proposed Routine Use O would permit FBI to disclose information:

> To federal, state, local, tribal, territorial, foreign, or international licensing agencies or associations, when the DOJ determines the information is relevant to the suitability or eligibility of an individual for a license or permit. [50]

The DOJ proposes to disclose "Insider Threat" Database information for purposes that do not relate to detecting and preventing insider threats. Determinations regarding employment or licensing as contemplated by Routine Uses L and O 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."[51] Routine Uses L and O unlawfully exceed DOJ's authority and should be removed from the Insider Threat SORN.

The DOJ also proposes to create a "Public Relations" exemption to the Privacy Act through Routine Use I that would permit the agency to release personal information to the media or members of the general public if it was related to a law enforcement or public safety function unless the DOJ determine that it is an "unwarranted invasion of personal privacy."[52] This routine use is unnecessarily broad especially given the number of people to be included in the proposed database and threatens to mistakenly expose the personal information of individuals. The DOJ

[49] *Id*.
[50] *Id*. at 25815.
[51] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[52] *Id*.

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 the DOJ.

In addition, the proposed routine uses that would permit the DOJ 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.[53] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations.

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

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

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that federal agencies were able to collect.[54] Congress further required agencies to be transparent in their information practices.[55] In *Doe v. Chao*,[56] the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that "in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies."[57]

[53] 5 U.S.C. § 552a(b).
[54] S. Rep. No. 93-1183, at 1 (1974).
[55] *Id*.
[56] *Doe v. Chao*, 540 U.S. 614 (2004).
[57] *Doe*, 540 U.S. at 618.

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DOJ proposes to exempt the Database from compliance with the following safeguards: 5 U.S.C. 552a(c)(3), (c)(4); (d)(1)-(4); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g).[58] These provisions of the Privacy Act require agencies to:

- grant individuals access to an accounting of when, why, and to whom their records have been disclosed;[59]
- inform parties to whom records have been disclosed of any subsequent corrections to the disclosed records;[60]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[61]
- collect and retain only such records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";[62]
- collect information from the individual to the greatest extent possible, when such information would have an adverse effect on the individual;[63]
- inform individuals from whom they request information the purposes and routine uses of that information, and the effect of not providing the requested information;[64]
- notify the public when it establishes or revises a database, and provide information on the categories of information sources and procedures to access and amend records contained in the database;[65]
- ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[66]
- promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record;[67]

[58] 81 Fed. Reg. 9789, 9790.
[59] 5 U.S.C. § 552a(c)(3).
[60] 5 U.S.C. § 552a(c)(4).
[61] *Id*. § 552a(d).
[62] *Id*. § 552a(e)(1).
[63] *Id*. § 552a(e)(2).
[64] *Id*. § 552a(e)(3).
[65] *Id*. § 552a(e)(4)(G), (H), (I).
[66] *Id*. § 552a(e)(5).
[67] *Id*. § 552a(f).

- serve notice to an individual who's record is made available under compulsory legal process; and[68]
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act.[69]

Several of the DOJ's claimed exemptions would further exacerbate the impact of its overbroad categories of records and routine uses in this system of records. The DOJ 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, the DOJ 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 the DOJ'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.

The DOJ 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."[70] In other words, the DOJ 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 "aid in establishing patterns of activity and providing criminal or intelligence leads."[71] 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

[68] *Id.* § 552a(e)(8).
[69] *Id.* § 552a(g)(1).
[70] 5 U.S.C. § 552a(e)(5).
[71] Insider Threat NPRM at 25753.

these criteria after it is stored.[72] By implication, the agency objects to guaranteeing "fairness" to individuals in the "Insider Threat" Database.[73]

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

5. Conclusion

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

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel

/s/ *Kim Miller*
Kim Miller
EPIC Policy Fellow

[72] *Id.*
[73] *Id.*