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 HOMELAND SECURITY

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services—018 Immigration Biometric and Background Check (IBBC) System of Records

Notice of Proposed Rulemaking and Notice of a new Privacy Act System of Records

[Docket Nos. DHS-2018-0002 and DHS-2018-0003]

August 30, 2018

---

By notice published July 31, 2018, the Department of Homeland Security ("DHS") published a new Privacy Act system of records notice ("SORN") titled "Department of Homeland Security/U.S. Citizenship and Immigration Services-018 Immigration Biometric Background Check System of Records" ("IBBC"). The new system combines two systems of records, the Department of Homeland Security/U.S. Citizenship and Immigration Services-002 Background Check Service and Department of Homeland Security/U.S. Citizenship and Immigration Services-003 Biometric Storage System.[1] This new database will contain a wide range of sensitive information on individuals, including biometric information like facial images, iris images, and voice samples.[2] The database will also cover a wide range of individuals, including individuals who are merely affiliated/associated with or represent an individual filing for immigration benefits.[3] The scope of the

[1] *Privacy Act of 1974; System of Records*, 83 Fed. Reg. 36950 (July 31, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-07-31/pdf/2018-16138.pdf. (hereinafter "DHS IBBC SORN").
[2] DHS IBBC SORN at 36952.
[3] *Id.*

individuals subject to the database as well as the scope of the information to be collected for the database are both broad and ambiguous.

By notice published July 31, 2018, DHS published a notice of public rulemaking ("NPRM") that proposes to exempt the IBBC 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) underscore the substantial privacy and security issues raised by the database; (2) recommend DHS withdraw unlawful and unnecessary proposed routine use disclosures; (3) recommend that DHS significantly narrow the agency's Privacy Act exemptions; and (4) propose that DHS implement a much shorter retention policy.

## I. EPIC's Interest

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and constitutional values.[5] EPIC has a particular interest in privacy issues related to the collection of biometric identifiers.[6] Biometric data is personally identifiable information that cannot be changed when compromised. Improper collection of this information can contribute to identity theft, inaccurate identifications, and infringement of constitutional rights. Strict limits on the collection and retention of biometric data is the best practice to prevent abuse.

EPIC regularly files Freedom of Information Act ("FOIA") requests and files lawsuits seeking records documenting biometric identification programs.[7] EPIC has filed a FOIA lawsuit to

[4] *Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services–018 Immigration Biometric and Background Check (IBBC) System of Records*, 83 Fed. Reg. 36792 (July 31, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-07-31/pdf/2018-16137.pdf (hereinafter "DHS IBBC NPRM").
[5] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[6] EPIC, *Biometric Identifiers*, https://epic.org/privacy/biometrics/.
[7] *See e.g.*, *EPIC v. CBP (Biometric Entry/Exit Program),* https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC v. FBI (Biometric Data Transfer Agreements), https://epic.org/foia/fbi/biometric-mou/ (EPIC

obtain documents related to CBP's Biometric Entry/Exit program.[8] More recently, EPIC submitted an urgent FOIA request to the Department of Homeland Security seeking the Privacy Impact Assessment for the "Homeland Advanced Recognition Technology," a proposed system that will integrate biometric identifiers across the federal government and serve as the primary biometric database for the Biometric Entry/Exit program.[9] EPIC also regularly submits public comments to federal agencies and to Congress advising on the privacy issues caused by the collection of biometrics.[10] And earlier this month EPIC filed an amicus brief[11] with the Illinois Supreme Court in *Rosenbach v. Six Flags Entertainment Corp.,* about the collection of a child's biometric data in violation of the Illinois Biometric Information Privacy Act.[12]

## II. The IBBC Database Would Maintain a Massive Amount of Personal, Sensitive Information on a Wide Variety of Individuals

### *a. The Database Covers Broad Categories of Individuals, Including Those Only Associated to Individuals Applying for Immigration Benefits*

The DHS proposes to collect the previously described personal data, including data on individuals who are not themselves applying for immigration benefits. This will include both U.S. citizens and noncitizens. The IBBC database would contain records on individuals merely associated

---

has obtained several memorandum of understanding regarding the transfer of biometric identifiers between the FBI and the Department of Defense).

[8] *EPIC v. CBP (Biometric Entry/Exit Program)*, EPIC, https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html.

[9] EPIC FOIA Request (June 18, 2018), https://epic.org/foia/dhs/pia/EPIC-18-06-18-DHS-FOIA-20180618-Request.pdf.

[10] *See, e.g.*, EPIC Statement to U.S. House Committee on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf; EPIC Comments to FBI, Revision of a Currently Approved Collection-CJIS Name Check Form (1-791) (Jan. 8, 2018), https://epic.org/apa/comments/EPIC-Comments-FBI-NGI-Name-Based-Background-Check.pdf (advising the FBI to limit its use of fingerprint-based background checks in favor of name-based background checks for noncriminal purposes).

[11] Brief of Amicus Curiae EPIC, *Rosenbach v. Six Flags Entm't Corp.,* 2018 WL 1382797 (Ill.), https://epic.org/amicus/bipa/rosenbach/EPIC_Amicus_Rosenbach.pdf.

[12] EPIC, *Rosenbach v. Six Flags*, https://epic.org/amicus/bipa/rosenbach/.

with immigration benefits requestors, including "[c]urrent, former, and potential derivative family members," attorneys, household members, and "[a]ffiliated persons who have a clearly articulated rational connection" to the requestor.[13] What is a "potential derivative family member"? What qualifies as a "clearly articulated rational connection"? DHS does not make this clear, meaning that the potential scope of the individuals who may be included in the IBBC database is incredibly broad.

The SORN describes this new system of records as a "consolidated and updated" version of the legacy systems,[14] but in reality it is a massive expansion of the categories of individuals covered by the system. In the Biometric Storage System the only individuals covered were the benefit applicants and those petitioning on their behalf.[15] The only additional category in the Background Check Service was "individuals over the age of 18 residing in a prospective adoptive parent's household whose principal or only residence is the home of the prospective adoptive parents"[16] These two legacy systems narrowly defined the covered individuals, in sharp contrast to the proposed system. DHS is increasingly casting wider nets for information on individuals not suspected of any wrongdoing in order to use that information for intelligence purposes while removing Privacy Act safeguards.

*b. Categories of Records in the Database Are Virtually Unlimited*

According to the IBBC system of record notice, the IBBC database will include an exorbitant amount of personal information about an expansive array of individuals. The categories of records contained in the IBBC database represent a wealth of sensitive information that should be afforded

[13] DHS IBBC SORN at 36952.
[14] DHS IBBC SORN at 36950.
[15] *Privacy Act; Biometric Storage System of Records*, 72 Fed. Reg. 17172 (April 6, 2007), https://www.federalregister.gov/documents/2007/04/06/07-1643/privacy-act-biometric-storage-system-of-records.
[16] *Privacy Act; Background Check Services System of Records*, 72 Fed. Reg. 31082 (June 5, 2007), https://www.federalregister.gov/documents/2007/06/05/07-2782/privacy-act-background-check-services-system-of-records.

the highest degree of privacy and security protections, particularly biometric information (including facial images, fingerprints, iris images, and signatures). The IBBC database will also include travel document information, addresses, phone numbers, immigration benefit data, and information from other government databases. 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 government.

In *NASA v. Nelson*,[17] 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").[18] 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.[19] EPIC also argued that compelled collection of sensitive data would place at risk personal health information that is insufficiently protected by the agency.[20] 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.[21]

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.[22] The

[17] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[18] 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.
[19] *Id*. at 20-28
[20] *Id*.
[21] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).
[22] 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.

JPL-NASA breach is a clear warning about why DHS 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.

The federal government is not equipped to handle the amount and severity of the cyberattacks it faces, risking compromising the IBBC database. The Government Accountability Office has made over 3,000 cybersecurity recommendations to agencies since 2010 but as of July 2018, about 1,000 still needed to be implemented.[23]

Data breaches have directly impacted DHS information systems in recent years. Most recently, DHS breached the personally identifiable information of almost a quarter million employees and individuals associated with the agency's investigations.[24] DHS has suffered several similar breaches in previous years.[25] Furthermore, according to GAO, DHS has not addressed cybersecurity workforce management requirements set forth in federal laws.[26]

These weaknesses in DHS databases increase the risk that unauthorized individuals could read, copy, delete, add, or modify sensitive information contained in the IBBC database. This risk is only magnified by DHS's retention policy. DHS "retains the records 100 years from the date of birth

---

[23] U.S. Gov't Accountability Office, *Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation* (Jul. 2018) https://www.gao.gov/assets/700/693405.pdf (hereafter "GAO Cybersecurity Report").
[24] *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.
[25] *See, e.g.*, 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 (breach exposed information of over 9,000 DHS employees and the personal email account of DHS Secretary Jeh Johnson); 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/ (breach affected 390,000 people associated with DHS); 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 (breach compromised records of at least 25,000 employees, including undercover investigators).
[26] GAO, *Cybersecurity Workforce: Urgent Need for DHS to Take Actions to Identify Its Position and Critical Skill Requirements*, GAO-18-175 (Washington, D.C.: Feb. 6, 2018); and *Defense Civil Support: DOD Needs to Address Cyber Incident Training Requirements*, GAO-18-47 (Washington, D.C.: Nov. 30, 2017).

of the individual" regardless of whether the records are still relevant to the purpose of the database.[27] Accordingly, DHS should implement a much shorter retention policy and only maintain records that are relevant and necessary to an investigation of eligibility for immigration benefits. 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.

There is also reason to be concerned about foreign governments compromising the IBBC database. Foreign governments continue to show a willingness to interfere with and infiltrate government agencies. For example, in March 2018, the Department of Justice reported that it had indicted nine Iranians for stealing more than 31 terabytes data from American entities, including five federal government agencies.[28] That same month DHS and the FBI released an alert stating that Russian government actors had targeted the systems of multiple U.S. government entities.[29] Federal government agencies should be mindful of these risks whenever they decide to implement a new system of records.

## III. Proposed "Routine Uses" Would Circumvent Safeguards and Contravene Legislative Intent of the Privacy Act

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 IBBC 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

[27] DHS IBBC SORN at 36954.
[28] GAO Cybersecurity Report at 7.
[29] *Id.*

originally gathered, the DHS exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

The IBBC SORN proposes 20 routine uses that undermine Privacy Act protections.[30] Routine use J—disclosure "[t]o foreign governments for the purpose of coordinating and conducting the removal of individuals to other nations"[31]—was not included in the legacy systems and could have terrible consequences. The Privacy Act requires agencies to ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness[32] and gives individuals the right to access and review records contained about them in the database and to correct any mistakes.[33] Routine use J would allow DHS to deport an individual based on erroneous information and deny that person an opportunity to correct the mistake. Recent reports have brought to light instances of U.S. citizens being detained or deported because the government had incorrect information about their immigration status.[34] It is completely inappropriate to exempt from Privacy Act protections the use of information in the IBBC database for deportation purposes. This is not the type of "routine use" that was intended by the Privacy Act.

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

---

[30] DHS IBBC SORN at 36953.
[31] *Id.* at 36954.
[32] 5 U.S.C. § 552a(e)(5).
[33] *Id*. § 552a(d).
[34] *See, e.g.*, David Bier, *U.S. Citizens Targeted by ICE: U.S. Citizens Targeted by Immigration and Customs Enforcement in Texas*, Cato Institute (Aug. 29, 2018), https://www.cato.org/publications/immigration-research-policy-brief/us-citizens-targeted-ice-us-citizens-targeted; Hamed Aleaziz, *This Man Beat ICE in an Argument Over Who His Father Was*, BuzzFeed News (Aug. 20, 2018), https://www.buzzfeednews.com/article/hamedaleaziz/immigration-ice-citizen-detained-paternity-appeals-court; Kevin Sieff, *U.S. is denying passports to Americans along the border, throwing their citizenship into question,* Washington Post (Aug. 29, 2018), https://www.washingtonpost.com/world/the_americas/us-is-denying-passports-to-americans-along-the-border-throwing-their-citizenship-into-question/2018/08/29/1d630e84-a0da-11e8-a3dd-2a1991f075d5_story.html.

information practices.[35] 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."[36]

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."[37] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[38] One of these exemptions is "routine use."[39] "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."[40]

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.[41]

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

Subsequent Privacy Act case law limits routine use disclosures to 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 determined that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[43] The Court of Appeals went on to quote the Third Circuit and made clear, "[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."[44]

The expansion of routine uses directly contradicts Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[45] Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of database records, and the DHS must reign in the exemptions it claims for its IBBC database.

---

[42] *Id*.
[43] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[44] *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).
[45] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).

## IV. The Collection, Retention, and Dissemination of Data by the IBBC Treats Innocent People Like Criminals and Terrorists for the Rest of Their Lives

As described above, the IBBC consolidates two previous databases while increasing the breadth of individuals that data is collected on and expanding the entities the data is disseminated to.[46] And, this information is kept by default until the individual turns 100 year old. As indicated in the NPRM, the information collected for this database used in the processing of immigration benefits is also used for "national security and intelligence activities."[47] Indeed, the database in its entirety can be disseminated to the Office of Director of National Intelligence National Counterterrorism Center.[48] The IBBC data is also disseminated to the FBI for background checks.[49] Per the FBI's policies, the Bureau retains this information until the individual reaches 110 years of age or for 7 years after the individual is confirmed deceased.[50]

Once collected, an individual's information will be a part of criminal, national security, and intelligence databases for the rest of his or her life—subject to every search or analysis run on the data in the database. The lengthy retention and broad dissemination policies will increasingly fill important criminal, national security, and intelligence databases with irrelevant information and increase the likelihood that an individual is wrongly targeted by the law enforcement or national security apparatus of the federal government.

DHS proposal to exempt the IBBC database from any meaningful safeguards provided by the Privacy Act compounds the issue by, for example, not subjecting the agency to requirements to make sure the information in the database is accurate. The IBBC represents a wide, unaccountable net cast by DHS for information on U.S. and non-U.S. individuals to be used for law enforcement

[46] *See generally*, DHS IBBC SORN.
[47] DHS IBBC NPRM at 36793.
[48] DHS IBBC SORN at 36954.
[49] DHS IBBC SORN at 36950.
[50] *Privacy Act of 1974; Systems of Records*, 81 Fed. Reg. 27284, 27287, https://www.gpo.gov/fdsys/pkg/FR-2016-05-05/pdf/2016-10120.pdf.

and intelligence purposes. The IBBC database essentially creates a criminal/intelligence database posing as an immigration benefit system.

## V. The Use of Facial Recognition Will Disproportionally Impact Marginalized Groups and Lead to Mission Creep

The collecting of facial images, and other biometric information, in the IBBC for the purpose of facial recognition poses significant risks to privacy and civil liberties. The technology can be used on unsuspecting people from a distance in a covert manner and on a mass scale. Similarly, facial recognition can easily be applied to large amounts of pictures and videos posted online. In short, facial recognition—which lacks any meaningful federal protections—gives the government the power to identify individuals whenever and wherever it wants without the consent or the knowledge of the individual.

The use of facial recognition will disproportionately impact minorities. Studies have shown that facial recognition has significantly higher error rates for darker-skinned individuals. One study found that while the maximum error rate for lighter-skinned males is 0.8%, it is 34.7% for darker-skinned females.[51] This is unacceptable in any context, but is especially problematic in this context because the color of an individual's skin may impact immigration benefit determinations.

The mass collection of facial images for use in facial recognition runs a serious risk of mission creep. The probability of mission creep is heightened by the fact that there are few laws that regulation the collection, use, dissemination, and retention of biometric data.[52] Indeed, DHS's new biometric database can freely pull biometric information from numerous other biometric databases like the FBI's Next Generation Identification, the State Department's Passport Records, and the

[51] Joy Buolamwini (MIT Media Lab) and Timnit Gebru (Microsoft Research), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[52] Jeramie D. Scott, *Facial recognition is here – but privacy protections are not*, The Hill (July 13, 2017), http://thehill.com/blogs/pundits-blog/technology/341906-opinion-facial-recognition-surveillance-is-here-but-privacy.

Department of Defense's Defense Biometric Identification Records System.[53] Similarly, DHS can provide any of the biometric data within the IBBC to numerous other state, federal, and foreign entities.[54]

Ubiquitous identification eliminates an individual's ability to control their identities and poses specific risk to the First Amendment rights of free association and free expression. The use of facial recognition by DHS for this database will have real consequences for U.S. citizens as well as non-U.S. citizens and will disproportionately impact marginalized groups.

## VI. Conclusion

For the foregoing reasons, the IBBC database is contrary to the core purpose of the federal Privacy Act. Accordingly, DHS must limit the information contained in the IBBC database, the individuals to whom the information pertains, and the retention of the information. Additionally, DHS should narrow the scope of its proposed Privacy Act exemptions, and remove the proposed unlawful routine uses disclosures from the IBBC system of records.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

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

/s/ *Christine Bannan*
Christine Bannan
EPIC Consumer Protection Counsel

[53] DHS IBBC SORN at 36953.
[54] *Id.* at 36953-54.