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 Data Privacy and Integrity Advisory Committee

May 14 Meeting on the Information Sharing Environment

Docket No. DHS-2021-0016

May 14, 2021

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the May 14, 2021 meeting of the Department of Homeland Security ("DHS") Data Privacy and Integrity Advisory Committee ("DPIAC").[1]

The Chief Privacy Officer tasked the DPIAC to provide "written guidance on best practices to ensure the effective implementation of privacy requirements for information sharing across the DHS enterprise."[2] The tasking includes three sub-prompts, asking DPIAC to address how the DHS Privacy can "better engage offices and Components", "provide better oversight of the privacy protections included in information sharing agreements" including specific metrics for reviewing Information Sharing Access Agreements (ISAAs), and a request for "other considerations necessary to effectively implement privacy requirements into DHS information sharing activities".[3] The October 27, 2020 tasking came just a few days before the public release of a DHS Office of Inspector General ("OIG") audit which found that DHS Privacy "has not conducted adequate

[1] 86 Fed. Reg. 19897, https://www.federalregister.gov/documents/2021/04/15/2021-07681/dhs-data-privacy-and-integrity-advisory-committee.
[2] Dena Kozanas, Taskings for the Data Privacy and Integrity Advisory Committee, Dept. of Homeland Security (October 27, 2020), https://www.dhs.gov/sites/default/files/publications/dpiac_tasking_memo_final_w_sig_0.pdf.
[3] *Id*.

oversight to ensure consistent execution of its privacy program across DHS components."[4] In particular, DHS Privacy has not reviewed any ISAAs from four of the five DHS components audited, amounting to thousands of unreviewed agreements.[5]

DPIAC must provide guidance for DHS Privacy so that the office's review of ISAAs is not simply a rubber-stamping operation without meaningful oversight. EPIC urges DPIAC to recommend 1) a triage system for reviewing ISAAs which prioritizes the most sensitive information, information from marginalized groups, and least secure receiving entities; and 2) that DHS Privacy compile statistics on the number and content of ISAAs and make that information available to the public.

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.[6] EPIC also has a sustained interest in DHS's biometrics policies and practices.[7] EPIC previously urged DPIAC to advise CBP to halt the

---

[4] Joseph V. Cuffari, DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives, OIG-21-06 Office of Inspector General (Nov. 4, 2020), https://www.oversight.gov/sites/default/files/oig-reports/DHS/OIG-21-06-Nov20.pdf.

[5] *Id* at 12-14.

[6] *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.

[7] *See e.g.*, Comments of EPIC to the Transportation Security Administration, Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck, Docket ID: TSA-2013-0001 (June 22, 2020), https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018), https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program),

implementation of its facial recognition program.[8] Recently, EPIC commented on the October 27, 2020 meeting in which the current tasking was assigned, calling for a full investigation of fusion centers.[9]

I. DPIAC should recommend a triage system for reviewing ISAAs that prioritizes the most sensitive information, information from marginalized groups, and least secure receiving entities.

DHS Privacy will need to implement a triage system to review the thousands of ISAAs signed without prior consultation with the office. According to OIG, four of the five DHS components under audit did not send any of their proposed ISAAs to DHS Privacy for review, and the remaining component sent only some of their ISAAs for approval.[10] OIG was unable to determine how many ISAAs the components had actually entered into, but just two of those components compiled over 2,000 agreements.[11] DHS Privacy has thousands of ISAAs to review for compliance with privacy requirements and to identify any privacy incidents. One component privacy officer began a review of ISAAs shortly after OIG's audit, leading to the discovery of at least four major privacy incidents.[12]

The current situation results from failures at both DHS Privacy and component privacy offices. According to DHS policy, the Chief Privacy Officer is responsible for reviewing all ISAAs

---

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 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.

[8] Comments of EPIC to the Data Privacy and Integrity Advisory Committee, December 10, 2018 Meeting, Docket No. DHS–2018–0066 (Dec. 10, 2018), https://epic.org/apa/comments/EPIC-Comments-DHS-DPIAC-Face-Rec-Report-Dec-2018.pdf.

[9] Comments of EPIC to the Data Privacy and Integrity Advisory Committee, October 27, 2020 Meeting and New Tasking, Docket No. DHS-2020-0039 (Nov. 10, 2020), https://epic.org/apa/comments/EPIC-DPIAC-Meeting-Oct-2020-Comments.pdf.

[10] November 4, 2020 OIG Report at 13.

[11] *Id* at 14.

[12] *Id*.

for compliance with documentation requirements and with privacy policy.[13] Privacy officers at the components are instructed to send all draft ISAAs to the CPO for review.[14] However, in the past "the DHS Privacy Office only review[ed] ISAAs as they are submitted by the components, without taking additional steps to identify ISAAs that are not submitted."[15] As a result, component privacy officers believed that submitting ISAAs was unnecessary, and there was no tracking system in place to ensure that ISAAs did not slip through the cracks. DHS Privacy did not implement and communicate clear procedures for obtaining review of ISAAs. The office now has thousands of finalized agreements to review for compliance with formal requirements and privacy laws and regulations.

The vast number of unreviewed ISAAs may contain terms which run against DHS privacy policies or authorize excessive disclosure to entities that cannot be trusted with PII due to risks of data breach. Excessive disclosure is not a theoretical risk, in 2019 DHS Privacy found that FEMA was sending too much PII to a contractor and had engaged in unauthorized disclosure of PII to a "non-governmental partner".[16] The office found that FEMA had no standardized procedures for creating or approving ISAAs, no centralized database for storing ISAAs, and no process for conducting compliance audits of existing agreements.[17] These institutional shortcomings allowed two different incidents of inappropriate disclosure of PII from over 100,000 disaster survivors.[18] A comprehensive review of ISAAs is necessary to uncover similar incidents and ensure compliance with baseline privacy requirements.

[13] DHS Directive 047-01, Privacy Policy and Compliance, July 7, 2011.
[14] DHS Instruction 047-01-001, Privacy Policy and Compliance, July 25, 2011.
[15] November 4, 2020 OIG Report at 13.
[16] Privacy Compliance Review of the Federal Emergency Management Agency's Information Sharing Practices, Oct. 21, 2019, https://www.dhs.gov/sites/default/files/publications/dhs-privacy-pcr-fema-infosharing-10-23-2019.pdf.
[17] *Id* at 8.
[18] *Id*.

a. DHS Privacy should prioritize the most sensitive categories of Personally Identifiable Information including biometric data and location data.

In order to cull through the large volume of ISAAs and prioritize the highest risk data dissemination practices, DHS Privacy should start by identifying ISAAs that authorize transmission of particularly sensitive PII. Those ISAAs that provide access to biometric information including facial recognition images or technology, iris images, fingerprints, DNA profiles, and other biometric identifiers should be the highest priority as biometric information is particularly sensitive. Facial recognition, in particular, should be a high priority as the technology is uniquely powerful and can allow for comprehensive surveillance. DHS Privacy should also prioritize any ISAAs that give access to historical or real-time location information, including cell site location information recorded by DHS or purchased from a third-party data broker.[19]

b. DHS Privacy should prioritize reviewing agreements that provide access to information from marginalized and over-surveilled groups.

The disclosures through ISAAs include information from marginalized and over-surveilled groups that traditionally have little power to control how their information is used and often lack any recourse when their information is abused. The information DHS and other government agencies obtain for one purpose is too easily abused for other purposes when there is not meaningful oversight over how information the government collects is used. For example, only recently has the government ended an agreement that formalized the practice of taking information obtained from detained immigrant children and using that information to find and deport their family members.[20]

---

[19] *See e.g.*, Hamed Aleaziz and Caroline Haskins, *DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People*, Buzzfeed (Oct. 30, 2020), https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

[20] *See* Department of Homeland Security, *HHS and DHS Joint Statement on Termination of 2018 Agreement* (Mar. 12, 2021), https://www.dhs.gov/news/2021/03/12/hhs-and-dhs-joint-statement-termination-2018-agreement; *See also* Letter from 112 organizations to DHS Secretary Kirstjen M. Nielson (Nov. 28, 2018), https://epic.org/privacy/DHS-HHS-Coalition-Letter-Nov2018.pdf.

Immigrants, in general, disclose a large amount of information on immigration forms with the expectation that the information will be used for their stated immigration purposes. Much of this information is collected into the HART database, which contains a large volume of biometric information from immigration, border surveillance, and counter-terrorism sources.[21] Biometric information collected at border crossings should only be used for limited identification purposes at the border, and should not be disclosed for non-immigration purposes.

DHS Privacy should ensure that any ISAAs providing access to immigration information comply with the Fair Information Practice Principles and limit disclosure of immigrants' information to immigration purposes. Similarly, information collected from border communities should be closely scrutinized. DHS Privacy should also prioritize reviewing ISAAs relating to counter-terrorism to provide more protection to Muslim communities. The review should further prioritize information from gang and drug databases and investigations as the burden of gang and drug surveillance falls heaviest on Black and Latinx communities. The office should pay particular attention to disclosure of immigrant information and information from other marginalized groups to non-federal entities and private companies.

c. DHS Privacy should prioritize reviewing ISAAs authorizing disclosures to federal contractors and private entities with a history of privacy issues.

Those entities with a demonstrated history of data breaches or other privacy harms should be the highest priority. For example, DHS Privacy should flag for immediate review any ISAAs authorizing information transfers to Perceptics, LLC, the federal contractor that made off with 184,000 facial recognition images during a Customs and Border Protection facial recognition pilot

[21] Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA, DHS/OBIM/PIA-004 (Feb. 24, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-obim004-hartincrement1-february2020_0.pdf.

program.[22] Prioritizing entities with a history of data breach will not resolve the threats to individuals as their personal information is spread across a wide variety of entities, but it is an effective means of harm reduction.

A triage system similar to the one outlined here would allow DHS privacy to address the most pressing privacy threats fastest, identifying those ISAAs that expose the most sensitive information and/or authorize disclosure to the least reliable entities. The same system is the starting point for gathering comprehensive data on the number and nature of DHS ISAAs to provide both the agency and the public with a better understanding of how personal information flows out from the agency.

II. DPIAC should recommend that DHS Privacy compile and publish information about ISAAs across DHS to provide the public with a better understanding of how the agency disseminates information.

Although DHS Privacy has a substantial task before it, the thousands of ISAAs to review provide an opportunity to compile information on DHS's data dissemination practices. It appears the agency itself has no comprehensive account of how components send PII to other federal agencies and non-federal entities, as evidenced by OIG's inability to determine how many ISAAs are currently in place. DHS Privacy, either as part of its' review, or as an extension of that review, should compile the following information and provide it to the public in a clear and accessible report.

a. Type and frequency of entities receiving information from each component.

DHS Privacy should compile the different types of entities that sign ISAAs, and provide statistics on how many ISAAs each type of entity has engaged in. The categories should include:

[22] *See*: Joseph V. Cuffari, Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot, OIG-20-71, Dept. of Homeland Sec. (Sept. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

federal entities, federal contractors, state government entities, state and local law enforcement, non-governmental organizations, and for-profit entities. The office should also compile, to the extent practicable, the number of entities with identified risks or known histories of privacy incidents including data breaches, inappropriate use or sale of PII, and other documented violations of privacy protections.

b. Type and frequency of information accessed through ISAAs.

DHS Privacy should compile the types of information disclosed through ISAAs and the frequency of those disclosures. Types of information should include a specific breakdown of biometric information (fingerprints, facial recognition images, iris images, DNA profiles, etc.), location information, personal information (address, phone number, family members etc.).

c. Source databases for information commonly accessed through ISAAs.

DHS Privacy should identify the DHS databases contributing information through ISAAs and provide links to the relevant System of Record Notices (SORNs) for those databases. The office should also clearly identify how information from DHS databases is disclosed, whether by providing access to the database, as the DHS Data Framework envisions for federal entities,[23] or through discreet data transfers. The public should know how often information compiled in identified DHS databases is disseminated outside the agency.

d. Privacy protections included in ISAAs.

Although DHS has a set of requirements for ISAAs that includes privacy protections, the Privacy Office should compile statistics on how often privacy protections are actually included in ISAAs, and which protections are most frequently written into the agreements. DHS Privacy should

[23] Privacy Impact Assessment Update for the DHS Data Framework – External Sharing, DHS/ALL/PIA-046(c) (Mar. 30, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-data%20framework-march2016%20%28003%29.pdf.

also evaluate how often privacy protections are tailored for the entity receiving agency information and how often ISAAs include specific privacy auditing procedures.

III. Conclusion

EPIC urges DPIAC to ensure that any review of ISAAs is a meaningful activity that provides real oversight and produces useful information for the public. DPIAC should recommend a triage system to identify the ISAAs that pose the greatest risks to individuals and prioritize reviewing those agreements first. DPIAC should not endorse a process which simply rubber-stamps ISAAs, encouraging further lax procedures and after-the-fact review. Please address any questions to Jake Wiener at wiener@epic.org.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

Jake Wiener
Jake Wiener
EPIC Law Fellow