DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2021-ICEB-2021-0012]

Privacy Act of 1974: Implementation of Exemptions; U.S. Department of Homeland Security/U.S. Immigration and Custom Enforcement-018 Analytical Records System of Records

AGENCY: U.S. Immigration and Custom Enforcement U.S. Department of Homeland Security.

ACTION: Final rule.

SUMMARY: The U.S. Department of Homeland Security (DHS) is issuing a final rule to amend its regulations to exempt portions of a newly established system of records titled, "DHS/ U.S. Immigration and Customs Enforcement (IC)-018 Analytical Records System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the system of records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: This final rule is effective **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT: For general questions please contact: Jordan Holz, ICEPrivacy@ice.dhs.gov, Privacy Officer, U.S. Immigration and Customs Enforcement (ICE), 500 12th Street SW, Mail Stop 5004, Washington, D.C. 20536. For privacy issues please contact: Lynn Parker Dupree (202) 343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

Background

The U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) published a notice of proposed rulemaking in the Federal Register, (86 FR 15134, March 22, 2021), proposing to exempt portions of the system of records titled, "DHS/ICE-018 Analytical Records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. The DHS/ICE-018 Analytical Records system of records notice was published concurrently in the Federal Register, (86 FR 15246, March 22, 2021), and comments were invited on both the Notice of Proposed Rulemaking (NPRM) and System of Records Notice (SORN).

Public Comments

DHS received four comments on the NPRM, two of which also referenced the SORN.

NPRM

All comments related to the NPRM state that exempting the SORN from portions of the Privacy Act will restrict the public's ability to demand transparency regarding ICE analytical systems.

The first concern commenters presented was that ICE's claiming of Privacy Act exemptions create a lack of transparency in ICE operations and the analytical systems themselves, stating: "[t]he American public has the right to know how our tax dollars are being spent and if their tax dollars are being spent wisely and ethically in regards to immigrants" and "[e]xemptions under the Privacy Act will not just protect DHS' system of records but also the data, software, and systems owned by private companies, perpetuating further a lack of transparency in deportations and other investigations under the guise of 'national security.'"

As discussed in the SORN and below, individuals about whom ICE maintains information in its records systems may still submit a Privacy Act amendment request or a request for access to information. While ICE has exempted this system of records from the access and amendment provisions of the Privacy Act, it will still consider these requests on a case-by-case basis to ensure that agency data is complete, accurate, and current.

Further, to provide the greatest access to information, ICE considers individuals' requests under both the Privacy Act and the Freedom of Information Act (FOIA). To this end, the public can seek records described in the Analytical Records SORN under FOIA. In contrast to the broad scope of FOIA, 5 U.S.C. 552, the Privacy Act is narrowly focused on individuals' personal information maintained in agency systems of records. As stated in the comment, the Privacy Act is meant to "…ensure accuracy of and individuals' access to information that agencies gather about them." FOIA's broad scope allows the public access to governmental information generally. This includes information on data, systems, and connections within the agency. Subsections (t)(1) and (t)(2) of the Privacy Act prohibit agencies not only from restricting an individual's access to his/her record under FOIA based solely on claimed Privacy Act exemptions, but also from withholding records under the Privacy Act based on FOIA exemptions. Information about filing a FOIA request with ICE is available at www.ice.gov/foia.

The publication process for the Analytical Records SORN as required by the Privacy Act promotes the accountability, responsibility, legislative oversight, and open government requested by commenters. Subsection (r) of the Privacy Act requires agencies, when establishing or significantly modifying a system of records, to provide adequate advance notice to the Office of Management and Budget (OMB), the Committee on Oversight and Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate. This

advance notice is separate from the public comment period ICE is engaging in here. The advanced notice that ICE provided to OMB and the committees of jurisdiction in Congress allows each body to make an evaluation of the probable or potential effects of ICE's proposal on the privacy or other rights of individuals.

Finally, in addition to the publication of SORNs here in the Federal Register, ICE also provides transparency into its systems through the publication of Privacy Impact Assessments (PIA). PIAs are conducted in accordance with the E-Government Act of 2002 (Pub. L. 107-347) by ICE Privacy personnel, are reviewed by the DHS Privacy Office, and signed by the DHS Chief Privacy Officer. PIAs describe how ICE information technology systems work, what information they collect, how ICE uses that information, any external parties with whom the information is shared, and the privacy risks and corresponding mitigations employed by ICE. ICE and all DHS PIAs are published on the DHS website, www.dhs.gov/privacy.

The second concern raised by commenters is the perceived inability for an individual to access ICE records about him/her due to the exemptions claimed in this rule. Commenters state "[e]xemptions intended to prevent the subject of an investigation from being aware of the investigation undermine the presumption of innocence enjoyed by individuals in the United States by proposing that individuals being investigated should be denied rights…" and that they "…take exception to the fact that the DHS is not required to establish requirements, rules, or procedures with respect to such access." The commenters' concern is amplified as the exemptions may not just apply to individuals under investigation, but their associates and family members as well.

As recognized in the comments, DHS is exempting this system as law enforcement sensitive to ensure that information and records produced in response to Privacy Act requests are not used to disrupt or frustrate ICE investigations. As stated in the accompanying SORN, "DHS/ICE will consider individual requests to determine

whether or not information may be released." ICE will consider all Privacy Act requests, whether access or amendment requests, on a case-by-case basis. As such, ICE has established access requirements, rules, and procedures outlined in the SORN accompanying this rule. The Privacy Act exemptions claimed here in no way alter or abrogate an individual's due process and fair trial rights guaranteed by the U.S. Constitution.

SORN

The comments filed in response to the proposed rule also raised objections regarding the DHS/ICE-018 Analytical Records SORN. Two objections are outside the scope of this rulemaking and so will not be addressed here. One objection from a commenter is that the SORN does not examine ICE's relationship with a private software vendor. ICE will not respond to this objection as a final rule is not the proper forum to discuss ICE contractual relationships. Additionally, ICE will not examine U.S. Citizenship and Immigration Services' (USCIS) biometrics NPRM, as requested by a commenter, as that proposed rule has been withdrawn (86 Fed. Reg. 24750, May 10, 2021).

The comments ICE received on the SORN were focused on four distinct areas of concern: 1) The SORN expands ICE's existing authority and ability to collect records on individuals; 2) The SORN lacks transparency, in that the SORN did not address issues important to the commenters; 3) ICE analytical systems use artificial intelligence and machine learning, with specific concern that these analytical systems will be used for "predictive policing" or "constant and ongoing surveillance of immigrants and citizens;" and, 4) The SORN's routine uses are so overly broad that "they provide no limit on permissible sharing."

The Analytical Records SORN expands ICE's existing Records Collection

A commenter expressed concern that the Analytical Records SORN was "expanding the sources from which data is gathered as well as the categories of individuals covered and records included and allows use of algorithmic processes." ICE did not intend the SORN to be understood as solely a consolidation of two previously published SORNs. Rather, as stated in the background section of the SORN, ICE is establishing a new system of records that clarifies and more accurately reflects the nature of records ICE collects, maintains, processes, and shares in large analytical data environments.

The purpose for ICE's publication of the Analytical Records SORN is to give the public notice of the types of records ICE maintains in support of analytical and algorithmic processes. Information derived from the ICE Tip Line and trade data, previously covered by the DHS/ICE-016 FALCON-Search and Analysis (FALCON-SA) SORN and DHS/ICE-005 Trade Transparency and Research (TTAR) SORN, respectively, are now covered under the Analytical Records SORN. Beyond those two categories of information, the Analytical Records SORN does not provide stand-alone coverage for any other ICE collection efforts. As stated in the SORN, ICE analytical systems ingest data collected through other efforts and authorities and covered by other SORNs. Differences in the categories of individuals or records described in the DHS/ICE-016 FALCON-SA SORN and DHS/ICE-005 TTAR SORN and those described in the Analytical Records SORN are reflective of these other ingestions.

The SORNs covering the ingested information restrict ICE's use of that information to what is compatible with the original purpose of the collection. Technological advancements allow ICE to institute protections at the record level that follow the data as it passes from the originating systems into ICE analytical systems. As such, the initial protections and restrictions on the use and sharing of the ingested information as described in those originating SORNs are retained by ICE as a record is

ingested into its analytical systems. To reiterate an example given in the SORN, data available through an ingest from ICE's Investigative Case Management System (ICM) would be covered by the DHS/ICE-009 External Investigations SORN (85 FR 74362, November 20, 2020) and each record stored from that ingest is tagged as belonging to that system of record. An analytical system may filter, search, graph, or link that data with other datasets, but only for a purpose described in DHS/ICE-009, such as generating leads for investigations. If ICE personnel wish to share an analytical product from an ICE analysis system with a third party, the tags of the underlying data, and its accompanying restrictions, must similarly be respected. Therefore, ICE analytical systems covered by the Analytical Records SORN do not expand ICE collections, use, or sharing of personal data.

The Analytical Records SORN does not provide an adequate accounting of DHS collection, use, and sharing of data

The commenters maintain that the Analytical Records SORN does not describe the access controls and auditing mechanisms within ICE's analytical systems in sufficient granularity. They also raise objections that the SORN does not discuss different analytical systems, such as ICE's FALCON-SA system and ICE's "complex network of interlocking systems" including ICE's connections to DHS's Homeland Advanced Recognition Technology system (HART).

The publication of the Analytical Records SORN is an effort to provide broader transparency of the ICE analytical environment so that ICE does not continue to rely on disparate and segregated notices from previously-published SORNs. The Analytical Records SORN reflects the realities of cloud computing and modern technological processes, where access and control are derived from user privileges rather than the physical location of data. As stated in the SORN, ICE's analytical processes may span multiple information technology systems within the ICE domain and records may be

derived from multiple collection points. Moreover, the purpose of a SORN is to provide notice to the public regarding personally identifiable information maintained by an agency; it is not meant to outline or provide a full description of the technical capabilities and nuances of an IT system. Granular detail of system connections, algorithmic processes, access controls, and auditing functions can be found in the applicable system's PIA, which can be found at www.dhs.gov/privacy. All PIAs link to their associated SORN(s), providing clear notice as to which systems are covered under the Analytical Records SORN.

The SORN allows for ICE to conduct unlimited surveillance and "predictive policing"

Several commenters expressed concern with ICE's use of advanced analytics and artificial intelligence to engage in controversial policing tactics. The first tactic, "predictive policing," is the practice of using statistics and analysis to forecast crime or identify where crime may occur in the near future.[1] Certain state or local police departments have used these methods to determine where to deploy resources or to identify those who are likely to commit crimes in the future by examining past behaviors.

The Analytical Records SORN does not support predictive policing. The SORN lists the purposes of the collection, use, and sharing of information in ICE analytical systems. The purposes of the systems are to identify current violations of law and regulation or generate leads for ongoing investigations. There is no purpose stated in the SORN that allows for its systems to engage in future state risk modelling.

Commenters expressed concern with a second controversial policing tactic, "ongoing and constant surveillance of immigrants and citizens." This is similarly not supported by the Analytical Records SORN. As stated in the SORN and above, the Analytical Records SORN does not expand ICE collections of personal data. ICE

[1] Tim Lau, Predictive Policing Explained (April 1, 2020), *available at* https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

analytical systems ingest data that has already been collected through other efforts and authorities. The restrictions on use of that data are listed in the SORN relevant to that collection and are transferred to the ICE analytical systems for linkage and further analysis. ICE analytical systems are meant to process data that has already been collected in a more efficient manner using advanced analytics and modern processing techniques. They are not used to monitor or surveil the public.

The SORN's Routine Uses are overly broad

Finally, a commenter objected that the routine uses listed in the Analytical Records SORN are "so expansive… they provide no limit on permissible sharing." The commenter, unfortunately, has not articulated any specific routine use that is inconsistent with the Privacy Act or ICE's statutory authorities for ICE to address. Generally, however, any routine use listed in the SORN must be compatible with the purpose of the system of records, as stated in the SORN, the purpose for which ICE originally collected the information, and ICE's statutory mission. Each routine use is analyzed and vetted for compatibility by ICE and DHS. As the Analytical Records SORN consolidates two previous ICE SORNs, the vast majority of routine uses in the new Analytical Records SORN are the same as the routine uses listed in those previously published SORNs. This means that the Analytical Records SORN routine uses were examined on multiple occasions by government oversight bodies that determined they were neither overly broad nor outside the stated purpose of the system of records.

As described in the SORN, if data is ingested from another system of records, the ICE analytical system, through record tagging and controls, ensures any subsequent sharing is compatible with the original SORN's purposes. This provides additional safeguards in the flow of information and limits the permissible sharing of data.

After consideration of public comments, the Department will implement the rulemaking as proposed.

List of Subjects in 6 CFR Part 5

Freedom of information, Privacy.

For the reasons stated in the preamble, DHS amends Chapter I of Title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for part 5 continues to read as follows:

Authority: 6 U.S.C. sec. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. sec. 301. Subpart A also issued under 5 U.S.C. sec. 552. Subpart B also issued under 5 U.S.C. sec. 552a.

2. In appendix C to part 5, add paragraph 86 to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

86. The DHS/ICE-018 Analytical Records System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE-018 Analytical Records System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings there under; national security and intelligence activities. The DHS/ICE-018 Analytical Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, State, local, tribal, foreign, or international government agencies. The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3) and (4), (d), (e)(1), (e)(2) and (3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g) pursuant to 5 U.S.C. 552a(j)(2). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions

of the Privacy Act, subject to limitations set forth in 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f) pursuant to 5 U.S.C. 552a(k)(2). Where a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here. Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

(a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and/or efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process.

(b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities. Further, permitting amendment to counterintelligence records after an investigation has been completed would impose an

unmanageable administrative burden. In addition, permitting access and amendment to such information could disclose security-sensitive information that could be detrimental to homeland security.

(c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.

(d) From subsection (e)(2) (Collection of Information from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.

(e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.

(f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(i) From subsection (g)(1) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

Lynn Parker Dupree,
Chief Privacy Officer,
U.S. Department of Homeland Security.

[FR Doc. 2021-24328 Filed: 11/5/2021 8:45 am; Publication Date: 11/8/2021]