DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 5

[Docket No. DHS-2019-0031]

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

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

ACTION: Final rule.

SUMMARY: The Department of Homeland Security (DHS) is issuing a final rule to amend its regulations to exempt portions of an updated and reissued system of records titled, "Department of Homeland Security/U.S. Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of this 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, (202) 732-3300, Acting Privacy Officer, Immigration and Customs Enforcement, Washington, D.C. 20536. For privacy issues please contact: Jonathan R. Cantor (202)-343-1717, Acting Chief Privacy Officer, Privacy Office, Department of

Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

DHS U.S. Immigration and Customs Enforcement (ICE) published a notice of proposed rulemaking (NPRM) in the *Federal Register* (82 FR 20844, May 4, 2017) proposing to exempt portions of DHS/ICE-016 FALCON Search and Analysis (FALCON-SA) System of Records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. This system of records was published concurrently in the *Federal Register* (82 FR 20905, May 4, 2017), and DHS sought comments on both the NPRM and System of Records Notice (SORN). It should be noted that the NPRM was over-inclusive regarding Privacy Act exemptions. This final rule appropriately limits the exemptions to what is permitted under the Privacy Act.

Basis and Purpose of Regulatory Action

In finalizing this rule, DHS exempts portions of the updated and reissued FALCON Search and Analysis (FALCON-SA) system of records from one or more provisions of the Privacy Act. ICE Homeland Security Investigations (HSI) personnel use FALCON-SA to conduct research and analysis using advanced analytic tools in support of ICE's law enforcement mission. Providing an individual access to FALCON-SA records pertaining to that individual could inform the subject of an ongoing or potential criminal, civil, or regulatory investigation, or reveal investigative interest on the part of DHS or another agency. For these reasons, DHS will exempt portions of the FALCON-SA system of records from certain provisions of the Privacy Act of 1974.

II. Public Comments

DHS received two substantive comments on the NPRM and one substantive comment on the SORN.

NPRM

Both commenters stated that exempting the portions of the FALCON-SA system of records from 5 U.S.C. 552a(e)(1), which ensures that all information collected about an individual "is relevant and necessary," risks violating an individual's Fourth Amendment protection from unreasonable search and seizure. Further, one commenter expressed concern that "collection" systems like FALCON-SA could be considered warrantless investigations and raise reasonable expectation of privacy considerations. The relevance of this objection is unclear as generally there is no warrant requirement for an investigation. Also, 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.

Moreover, FALCON-SA is used for storing, searching, analyzing, and visualizing volumes of *existing* information gathered under processes that are covered by their own standard operating procedures, policies, and rules of behavior where applicable. It does not directly collect information from any individuals.[1] Further, to ensure that all information ingested into FALCON-SA is collected appropriately, all users complete FALCON-SA training that includes rules of behavior, appropriate use of system data,

[1] For more information on ingests, including an explanation of sources of information ingested into FALCON-SA, see: DHS/ICE/PIA-032 FALCON Search & Analysis System.

uploading and tagging records, disclosure and dissemination of records, and system security. Users must complete training in order to receive authorization to access FALCON-SA. All personnel who have access to the ICE Network are also required to take annual privacy and security training, which emphasizes the DHS Rules of Behavior and other legal and policy restrictions on user behavior.

One commenter indicated that FALCON-SA collects individuals' information without their consent, and therefore objected generally to Privacy Act exemptions for the FALCON-SA system of records. As noted above, FALCON-SA does not directly gather information from the individual, but rather ingests information collected through existing legal processes. DHS, in exempting portions of the FALCON-SA system of records from particular provisions of the Privacy Act, is not engaging in a search of any individual. To the extent comments address potential impacts or concerns with collection of information by other systems, DHS and ICE publish SORNs and rules for all systems of records that can be found at https://www.dhs.gov/system-records-notices-sorns.

Another commenter stated that the FALCON-SA System of Records allows ICE personnel to collect "any information [he or she] wants without disclosing where it came from or even acknowledging its existence." While DHS notes this concern, law enforcement exemptions allow ICE personnel to retain evidentiary information in the appropriate system(s) without public disclosure. When law enforcement agencies share information they collect with ICE, appropriate ICE personnel determine whether it should be ingested into FALCON-SA. If information is ingested, ICE personnel do not make any changes to the data, in order to preserve data accuracy and integrity. Under this final rule, information that is or will be stored in FALCON-SA will be exempt from disclosure so

that law enforcement investigations are not negatively impacted. DHS ensures that all FALCON-SA users are trained on the proper uses of the system. All ingests performed by a FALCON-SA user require ICE supervisory approval. FALCON-SA also implements extensive auditing of user actions in the system. The system automatically maintains an audit log, and any attempt to access information outside of the user's permissions will be automatically flagged throughout the enterprise. User actions are recorded and stored in audit logs accessible to supervisors and ICE IT security personnel, which are searched and analyzed to ensure proper use of the system. Audit data is also available to ICE Office of Professional Responsibility (OPR) investigators if there is an investigation into possible wrongdoing by a FALCON-SA user. Additional information on auditing and technical controls and safeguards can be found in the FALCON-SA Privacy Impact Assessment (PIA), available at https://www.dhs.gov/privacy-impact-assessments. While ICE cannot disclose the specific information collected by FALCON-SA without compromising individual cases, the FALCON-SA PIA was published to transparently explain how information is collected, stored, protected, shared, and managed by the system..

SORN

The comment received in regard to the SORN can be broken down into two main topics:

1) The system collects too broadly, and

2) The routine uses for disclosure circumvent Privacy Act safeguards and contravene legislative intent.

Regarding the first point, the comment suggested that FALCON-SA collects

"virtually unlimited" categories of records. ICE developed FALCON-SA to enhance ICE's ability to identify, apprehend, and initiate appropriate legal proceedings against individuals who violate criminal, civil, and administrative laws enforced by ICE. FALCON-SA supports the investigative work of ICE HSI agents and criminal research specialists by allowing them to search, review, upload, and analyze data pertinent to an investigative lead or an ongoing case. While "collection" is not an applicable concept in the context of actions that are undertaken through FALCON-SA directly, DHS acknowledges a general risk of over-collection of information. In circumstances when ICE directly collects information, ICE only collects the minimum amount relevant and necessary to further ICE's law enforcement mission. To that end, ICE maintains information about DHS personnel, other law enforcement personnel, victims, witnesses, and other associated individuals who may be relevant in the course of an investigation. ICE does not use FALCON-SA to collect any information directly from an individual or about an individual, but rather ingests information collected by other systems pursuant to the limitations in their own privacy compliance documentation. HSI personnel determine whether the information from other systems should be ingested into FALCON-SA. ICE has established system safeguards to prevent the inclusion of data that does not serve FALCON-SA's intended purpose, which is to support ICE HSI law enforcement investigations and analytical activities. As stated above, before being able to access FALCON-SA, users must first complete privacy and information security training that includes appropriate uses of system data, uploading and tagging records, disclosure and dissemination of records, and system security to mitigate any risk resulting from the collection of this information. Further, as stated above, ICE also implements extensive

auditing of user actions in the system.

The commenter expressed concerns about disclosures pursuant to routine uses proposed in the FALCON-SA SORN. First, disclosures pursuant to the routine use exception are never mandatory, but instead are at the discretion of the agency. Second, FALCON-SA users have a requirement to document all disclosures made per these routine use exceptions as well as disclosures made under any other authority.

Specifically, the commenter expressed concerns about Routine Uses H, J, and O. Routine Use H authorizes disclosure to federal, state, local, tribal, territorial, foreign, or international agencies for background investigations. Under this Routine Use, DHS only shares information about individuals' criminal, civil, and administrative law violations in response to other agencies' background investigations. This type of disclosure is limited to information that was collected for law enforcement purposes. Limited sharing to assist in law enforcement investigations is consistent with the purpose for collection.

Routine Use J authorizes disclosure to international and foreign partners in accordance with law and formal or informal international arrangements. DHS enters into formal or informal information sharing agreements that are consistent with the system's law enforcement purposes. Further, information sharing partners must execute a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), or an equivalent agreement stipulating that they will only use DHS information consistent with the purposes for which the information was collected.

Routine Use O authorizes disclosure to the media and members of the public with the prior approval of the Chief Privacy Officer, if the disclosure is a matter of legitimate public interest. Like all Routine Uses, disclosures are not mandatory. Media disclosures

are limited in scope and subject to restrictions and procedures located in the DHS Privacy Policy Guidance Memorandum 2017-01[2] and other laws, regulations, and policies. Absent a waiver by the subject of the record, ICE may only release information to the media in those specific situations detailed in the Routine Use. Similar to other law enforcement agencies, for example, ICE may release the name, age, gender, and the summary of a criminal charge if the subject of a record has been charged with a crime and that information falls within ICE's purview. ICE may also release limited fugitive information, which would be beneficial to public safety.

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. 101 *et seq.*; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. 301.

Subpart A also issued under 5 U.S.C. 552.

Subpart B also issued under 5 U.S.C. 552a.

2. Amend appendix C to part 5 by adding paragraph 81 to read as follows:

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

[2] Available at https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

* * * * *

81. The DHS/ICE-016 FALCON Search and Analysis (FALCON-SA) System of Records consists of electronic and paper records and will be used by DHS and its components. The FALCON-SA System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The FALCON-SA 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 (c)(4): (d); (e)(1), (e)(2), (e)(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), (e)(4)(I); and (f) pursuant to 5 U.S.C. 552a(k)(2). 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. Information on a completed investigation may be withheld and exempt from disclosure if the fact that an investigation occurred remains sensitive after completion.

(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 and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. 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. Compliance

with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(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.

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

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security
[FR Doc. 2019-18749 Filed: 8/29/2019 8:45 am; Publication Date: 8/30/2019]