9111-28

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. DHS-2017-0002]

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: Department of Homeland Security (DHS), Privacy Office.

ACTION: Notice of Proposed Rulemaking.

SUMMARY: The Department of Homeland Security is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "Department of Homeland Security/U.S. Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2017-0002 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

- Fax: 202-343-4010.
- Mail: Jonathan R. Cantor, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

INSTRUCTIONS: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

DOCKET: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Amber Smith, Privacy Officer, (202-732-3300), U.S. Immigration and Customs Enforcement, 500 12th Street, SW, Mail Stop 5004, Washington, D.C. 20536, e-mail: ICEPrivacy@dhs.gov, or Jonathan R. Cantor (202-343-1717), Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background:

The Department of Homeland Security (DHS) is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the "DHS/U.S. Immigration and Customs Enforcement (ICE)-016 FALCON Search and Analysis System of Records" and this proposed rule. In this rule, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

The FALCON Search and Analysis (FALCON-SA) System of Records describes the operation of an ICE information technology system of the same name, which is

owned by ICE's Office of Homeland Security Investigations (HSI). This system contains a repository of data that is ingested on a routine or ad hoc basis from other existing sources, and an index created from that data. FALCON-SA incorporates tools that allow the data to be queried, analyzed, and presented in a variety of formats that can help illuminate relationships among the various data elements. The purpose of FALCON-SA is to help ICE HSI personnel conduct research and analysis using advanced analytic tools in support of their law enforcement mission.

FALCON Overview

In 2012, ICE HSI created a new IT environment called "FALCON" to support ICE's law enforcement and criminal investigative missions. The FALCON environment is designed to permit ICE law enforcement and homeland security personnel to search and analyze data ingested from other Government applications and systems while employing appropriate user access restrictions at the data element level and robust user auditing controls.

In February 2012, ICE deployed the first module of FALCON with the launch of FALCON-SA. FALCON-SA enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. ICE agents, criminal research specialists, and intelligence analysts use FALCON-SA to conduct research that supports the production of law enforcement intelligence products; provides lead information for investigative inquiry and follow-up; assists in the conduct of ICE criminal, civil, and administrative investigations; assists in the disruption of terrorist or other criminal activity; and discovers previously unknown

connections among existing ICE investigations. ICE's use of the system is always predicated on homeland security, law enforcement, and/or intelligence activities. FALCON-SA is an internal system used only by ICE.

Since the launch of FALCON-SA, ICE has created other user interfaces, including FALCON-Tip Line, FALCON-DARTTS, and FALCON-Roadrunner, under the FALCON umbrella. Like FALCON-SA, these other interfaces also use data maintained in the FALCON general data storage environment. This environment is where FALCON data is aggregated and user access is controlled through a combination of data tagging, access control lists, and other technologies. Using a central data store for FALCON data eliminates the need for multiple copies of the data and streamlines the application of many security and privacy controls. Only data accessed via FALCON-SA is covered by the DHS/ICE-016 FALCON-SA System of Records Notice (SORN). However, the other interfaces are covered by other ICE SORNs, as specified in the System Location section of the SORN. Separate SORNs are appropriate because the data, purposes, and routine uses differ for each FALCON interface.

FALCON-SA Data

Information included in FALCON-SA is ingested either on a routine or ad hoc basis. Routine ingests are regular updates to datasets that originate from other Government (typically ICE or DHS) data systems. A list of routine ingests into the FALCON general data storage environment that are accessible via FALCON-SA is available in the FALCON-SA Privacy Impact Assessment at www.dhs.gov/privacy.

Ad hoc ingests are user-driven ingests of particular data that may be relevant to a given user or group's investigative or analytical project in FALCON-SA. The nature of

the data in ad hoc ingests varies from data collected from a commercial or public source (e.g., Internet research or from a commercial data service such as CLEAR), to public reports of law enforcement violations or suspicious activity (tips), to digital records seized or subpoenaed during an investigation. All ad hoc ingests are tagged by the FALCON-SA user with the appropriate category description, and that tag drives the retention policy for that data. The ad hoc ingest category description list is included in the FALCON-SA Privacy Impact Assessment at www.dhs.gov/privacy.

FALCON-SA records may include some or all of the following types of personally identifiable information: identifying and biographical data such as name and date of birth, citizenship and immigration data, border crossing data, customs import-export history, criminal history, contact information, criminal associates, family relationships, photographs and other media, and employment and education information.

FALCON-SA also contains an index, which is a numerical and alphabetical list of every word or string of numbers/characters found in the FALCON-SA database, with a reference to the electronic location where the corresponding source record is stored. FALCON-SA uses this index to conduct searches, identify relationships and links between records and data, and generate visualizations for analytic purposes. FALCON-SA also contains metadata that is created when ingesting data. The metadata is used to apply access controls and other system rules (such as retention policies) to the contents of FALCON-SA. The metadata also provides important contextual information about the date the information was added to FALCON-SA and the source system from where the data originated.

The data sets in FALCON-SA include tips submitted to ICE either through an online form on the ICE website or by calling the HSI Tip Line. These tips are generally created electronically using the FALCON-Tip Line interface. Alternatively, they may be manually entered by HSI's Cyber Crimes Center when the tips pertain to child exploitation crimes. Once HSI adjudicates the tips for action, they are then accessible to all HSI users via the FALCON-SA interface.

Uses of FALCON-SA

ICE HSI agents, criminal research specialists, and intelligence analysts query FALCON-SA for a variety of purposes: to conduct research that supports the production of law enforcement intelligence products; to provide lead information for investigative inquiry and follow-up; to assist in the conduct of ICE criminal, civil, and administrative investigations; to assist in the disruption of terrorist or other criminal activity; and to discover previously unknown connections among existing ICE investigations. These queries can be saved in FALCON-SA to eliminate the need to recreate them each time a user logs on.

Strong access controls and a robust audit function ensure that ICE's use of the system is predicated on homeland security, law enforcement, and intelligence activities. This requirement is enforced by a governance group composed of leadership from HSI with oversight by ICE's legal, privacy, and civil liberties offices.

While ICE previously relied on the DHS/ICE-006 ICE Intelligence Records System (IIRS) SORN, last published at 75 Fed. Reg. 9233 (Mar. 1, 2010), to maintain FALCON-SA records, ICE recently determined a separate system of records notice will provide greater transparency and allow ICE to more accurately describe the records

accessible via FALCON-SA. FALCON-Tip Line records were previously covered by the DHS/ICE-007 Alien Criminal Response Information Management (ACRIMe) SORN, but the FALCON-SA SORN will now cover those records instead. This change is due to Tip Line records having migrated out of the ACRIMe system into the FALCON environment and that once created, the official repository for FALCON-Tip Line records is the FALCON general data storage environment.

This SORN will cover data that is accessible via FALCON-SA's user interface only, and does not cover data that is accessed via other FALCON interfaces, such as Roadrunner and DARTTS, which are covered by the DHS/ICE-005 Trade Transparency and Analysis Records (TTAR) SORN.

Additional information about FALCON-SA can be found in the Privacy Impact Assessments published for FALCON-SA and FALCON-Tip Line, available at http://www.dhs.gov/privacy-documents-ice.

Consistent with DHS's information sharing mission, information stored in the FALCON-SA SORN may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, information may be shared with appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in the system of records notice.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect,

maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

The Privacy Act allows Government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/ICE-016 FALCON-SA System of Records. Some information this system of records relates to official DHS national security, law enforcement, immigration, and intelligence activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS retains the ability to obtain information from third parties and other

sources; and to protect the privacy of third parties. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

A system of records notice for DHS/ICE-016 FALCON-SA System of Records is also published in this issue of the Federal Register.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend 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: 5 U.S.C. 552; 5 U.S.C. 552a; 5 U.S.C. 301; 6 U.S.C. 101 et seq.; E.O. 13392.

2. Add new paragraph 77 at the end of appendix C to read as follows:

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

* * * * *

77. The DHS/ICE-016 FALCON Search and Analysis (FALCON-SA) System of Records consists of electronic and paper records and will be used by ICE law enforcement and homeland security personnel. The DHS/ICE-016 FALCON-SA System of Records contains aggregated data from ICE and DHS law enforcement and homeland security IT systems, as well as data uploaded by ICE personnel for analysis from various public, private, and commercial sources during the course of an investigation or

analytical project. This information may include some or all of the following types of personally identifiable information: identifying and biographic data such as name and date of birth; citizenship and immigration data; border crossing data; customs import-export history; criminal history; contact information; criminal associates; family relationships; photographs and other media; and employment and education information. The records also include tips received by ICE from the public concerning suspicious or potentially illegal activity, as well as telephone call detail records, which contain call transactions and subscriber data, obtained via lawful process during the course of an investigation. This information is maintained by ICE for analytical and investigative purposes and is made accessible to ICE personnel via the FALCON-SA system interface. The system is used to conduct research that supports the production of law enforcement intelligence products; provide lead information for investigative inquiry and follow-up; assist in the conduct of ICE criminal and administrative investigations; assist in the disruption of terrorist or other criminal activity; and discover previously unknown connections among existing ICE investigations.

The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (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). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); and (g). When a record received from another system has been exempted in that source system under 5 U.S.C. 552a(j)(2) or (k)(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 administrative 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 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 administrative 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 classified and other 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 and/or threaten individuals' safety 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.

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

Dated: May 1, 2017.

Jonathan R. Cantor,
Acting Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2017-09026 Filed: 5/3/2017 8:45 am; Publication Date: 5/4/2017]