Privacy Impact Assessment

for the

Analytic Tools in Support of the Protective Mission

DHS Reference No. DHS/ICE/PIA-066

August 20, 2025

Homeland Security

Abstract

1. The abstract is the single paragraph that will be used to describe the program and the Privacy Impact Assessment.[1]
The U.S. Immigration and Customs Enforcement has experienced an increased level of external threat activity directed towards the agency's Senior Leaders and its personnel. Recent threats have expanded to include physical attacks on U.S. Immigration and Customs Enforcement facilities and the homes of U.S. Immigration and Customs Enforcement employees. The *Analytic Tools in Support of the Protective Mission* program will lawfully collect information from publicly available, open source, social media environments and will only use the information to identify potential threats against the agency, its personnel and facilities.

Overview

2. The overview provides the context and background necessary to understand the project's purpose and mission and the justification for operating a privacy sensitive project.
The U.S. Immigration and Customs Enforcement has experienced a significant increase in the amount of external threat activity directed towards it. Much of the threat activity originates from social media and online posts and has since expanded to physical attacks on U.S. Immigration and Customs Enforcement facilities, employees and the households of employees. To prevent criminals from successfully targeting U.S. Immigration and Customs Enforcement Senior Leaders, personnel, detainees, equipment and facilities, the U.S. Immigration and Customs Enforcement requires real-time threat mitigation and situational awareness capabilities, and vulnerability assessments. The U.S. Immigration and Customs Enforcement has designated personnel from the Office of Professional Responsibility and Homeland Security Investigations to have responsibility for reviewing and developing daily intelligence reports that identify potential threats and dangerous activities that can disrupt the U.S. Immigration and Customs Enforcement in executing its lawful activities. These personnel are also responsible for providing reports to the U.S. Immigration

[1] Pursuant to Section 208 of the E-Government Act of 2002, agencies are required to conduct a Privacy Impact Assessment before developing or procuring Information Technology systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public. The Office of Management and Budget issued Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, which defines "information in identifiable form" as information in an Information Technology system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements. Furthermore, an individual is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence."

and Customs Enforcement Director, facility operators, and field office managers. The assessment helps to provide situational awareness of potential threats to leadership, U.S. Immigration and Customs Enforcement personnel, detainees, equipment and facilities.

The Office of Professional Responsibility is responsible for addressing internal and external threats against members of U.S. Immigration and Customs Enforcement Senior Leadership and personnel. U.S. Immigration and Customs Enforcement personnel use internet-based services, content aggregators, and government and commercially developed tools that provide a variety of methods for monitoring publicly available information on social media sites for textual information that provides agency situational awareness, while respecting individual users' privacy settings. All the tools employed by the Office of Professional Responsibility and Homeland Security Investigations personnel use threat-based keywords to search across platforms and identify publicly available content made in public forums which match those keywords.

All information collected is derived from publicly available social media postings or other publicly available content, deemed relevant to and within scope to draft reports designed to shape the agency's situational awareness. The U.S. Immigration and Customs Enforcement generally does not include personally identifiable information in its analysis. However, there are certain instances that will be discussed further, including when content is deemed threatening, when it may be necessary to include personally identifiable information in a report. Unless otherwise authorized by law, the U.S. Immigration and Customs Enforcement does not store or disseminate information related to First Amendment protected speech or activities. U.S. Immigration and Customs Enforcement personnel reviews content captured by digital analytic tools to determine whether it is relevant for threat-based situational awareness.

3. What specific legal authorities and/or agreements permit the collection of information by the project in question?

The legal authorities for the U.S. Immigration and Customs Enforcement to collect and maintain the publicly-available, open-source, social media information collection includes, the Homeland Security Act of 2002, Public Law Number 107-296, 166 Stat. 2135, 6 United States Code § 101 et seq. (as amended); pertinent provisions of Title 18 of the United States Code, including but not limited to sections 111-115, Assaults on Federal Officers; Section 119, Protection of Individuals Performing Certain Official Duties.

4. Will this information be maintained as part of system of records,[2] as defined in the Privacy Act, 5 U.S.C. §552a?

The applicable System of Records Notices for this collection are:

- DHS/ICE-006 Intelligence Records System;[3] and
- DHS/ICE-009 External Investigations.[4]

5. From which population does the project collect, maintain, use, and/or disseminate personally identifiable information[5]?

☒ a. Members of the public

☒ b. U.S. Department of Homeland Security employees and/or contractors

☒ c. Other federal employees

6. What personally identifiable information is collected, maintained, used, or disseminated?

[2] The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
[3] *See* DHS/ICE-006 INTELLIGENCE RECORDS SYSTEM, 90 FR 34282 (July 21, 2025), *available at* System of Records Notices (SORNs) | Homeland Security.
[4] *See* DHS/ICE-009 EXTERNAL INVESTIGATIONS, 85 FR 74362 (November 20, 2020), *available at* System of Records Notices (SORNs) | Homeland Security.
[5] Personally identifiable information means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. *See* OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information.

- Uniform Resource Locator
- User identity
- Display name.

Homeland Security Investigations and the Office Professional Responsibility do not intentionally collect personally identifiable information when using analytic tools in support of the protective mission. The focus of collection is situational awareness, which generally means the nature of the event/threat, the possible target/location, and when the event is likely to occur. Some social media posts may be captured as "screen shots," in which case an individual's user identity, or other personally identifiable information made publicly available by the individual, may be collected. Such personally identifiable information is used or disseminated as part of the protective mission to inform impacted locations along with the source Uniform Resource Locator which may contain personally identifiable information, such as the user identity or display name, to capture the source information verbatim. Furthermore, Homeland Security Investigations and the Office of Professional Responsibility do not use a member of the public's personally identifiable information for keyword searches and do not index data based on personally identifiable information.

7. What is the intended use of personally identifiable information?

Personally identifiable information will be used to identify potential threats to the U.S. Immigration and Customs Enforcement leadership, personnel, detainees, equipment, and facilities. The mission is to collect and report relevant threat information to inform agency decision-making regarding events that may affect operational readiness and the security of U.S. Immigration and Customs Enforcement personnel, detainees, equipment and facilities. Efforts are focused on employee safety and facility security to prevent injury to persons or property destruction.

As part of the search, it may be necessary, particularly when social media is used to identify or maintain situational awareness of credible threats against U.S. Immigration and Customs Enforcement employees, to use personally indefinable information.[16] For example, the U.S. Immigration and Customs Enforcement may create keyword lists that are processed by analytic tools to identify publicly available content containing information related to threats against employees and facilities. Keyword lists may be developed for high interest events (e.g., trials or conferences where there may be an increased threat risk). There may be cases in which personally identifiable information may be included as keywords to identify the target or perpetrator of threats.

Any biographical personally identifiable information collected of an U.S. Immigration and

Customs Enforcement employee would be limited to only that which is necessary to identify and mitigate a potential risk. For example, a keyword may be the name and home address of a member of U.S. Immigration and Customs Enforcement Senior Leadership. A social media post with the name and address of a specific individual may increase the credibility of a threat by demonstrating a potential ability to carry it out.

In most instances, U.S. Immigration and Customs Enforcement personnel carrying out the protective mission will not collect or create reports with personally identifiable information because the collection and dissemination of personally identifiable information is not necessary to report on operational readiness and security of U.S. Immigration and Customs Enforcement personnel and facilities. The processes U.S. Immigration and Customs Enforcement uses to ensure an U.S. Immigration and Customs Enforcement nexus and to minimize collections, as well as the training and oversight of information collection, retention and use are described throughout this Privacy Impact Assessment.

8. How long and under which retention schedule is the information retained?

Material collected and created for the Protective Mission will be managed in accordance with the applicable records management legislation as codified at 44 United States Code Chapters 21, 29, 31, and 33, the Freedom of Information Act (5 United States Code 552), and the Privacy Act (5 United States Code 552a), and shall be scheduled for disposition in accordance with 36 Code of Federal Regulations 1228.

Investigative records created from this information collection will be retained in accordance with the National Archives and Records Administration, Federal Records Schedule number, N1-36-86-01 (Section 161.3; Item b, Investigative Case Files), which have a 20-year retention cycle. The non-investigative record material created in this collection will be maintained in accordance with National Archives and Records Administration's Federal Records Schedule number, DAA-567-2016-0003-0008 for Special Law Enforcement Intelligence Records and have a 25-year retention cycle.

9. With whom will personally identifiable information be shared?

☐ Within the Component/Office	Specify:
☐ Other-U.S. Department of Homeland Security Component(s)/Office(s)	Specify:
☐ State, local, tribal, or territorial entities	Specify:

☐ Public	Specify:
☐ Private sector	Specify:
☐ Foreign governments	Specify:
☐ Foreign entities	Specify:
☐ Other:	Specify:

10. How are individuals provided notice prior to the collection of information? If notice is not provided, explain why not.

The U.S. Immigration and Customs Enforcement provides notice of collection and maintenance of personally identifiable information through the publication of applicable privacy compliance documentation, including the DHS/ICE-006 Intelligence Records System of Record Notice and DHS/ICE-009 External Investigations System of Records Notice. In addition, the publication of this Privacy Impact Assessment provides specific notice of the collection, use, dissemination, and maintenance of personally identifiable information with respect to the U.S. Immigration and Custom Enforcement's protective mission. As a general matter, Homeland Security Investigations and the Office of Professional Responsibility do not retain and report on personally identifiable information captured incidentally in furtherance of the protective mission. The focus is on law enforcement intelligence identifying events and activities that may affect operational readiness and the safety and security of U.S. Immigration and Customs Enforcement personnel, detainees, equipment, and facilities. However, certain instances or reporting, as described above, may necessitate collection and retention of personally identifiable information. As such, Homeland Security Investigations and the Office of Professional Responsibility will not provide direct notice to the individuals whose information has been captured but rather does so through this Privacy Impact Assessment. In other instances, it may not be feasible or desirable to provide direct notice to individuals or groups at the time their information is collected from publicly available sources because to do so could tip off threat actors to sensitive law enforcement activity.

11. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out?

Any individual may decline or opt out of having their information gathered and included in this collection can do so by not posting material online or limiting access to who can view their posts.

12. What procedures are in place to allow individuals to correct inaccurate or erroneous information?

Pursuant to the Privacy Act, a U.S. Person may submit a request for amendment of any erroneous or inaccurate information to the U.S. Immigration and Customs Enforcement Privacy Office. The request should cite the Privacy Act and clearly state or identify the specific information or detail that is believed to be erroneous; if the information is inaccurate, the requests should also give the correct detail to replace the error.

Mail the completed request to:

U.S. Immigration and Customs Enforcement
Office of Information Governance and Privacy
Attn: Privacy Unit
500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
http://www.ice.gov/management-administration/privacy

13. What administrative, technical, and physical controls are used to protect the information?

The U.S. Immigration and Customs Enforcement implements appropriate information security safeguards commensurate with the risk that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of the information within the collection.

Administratively, the information and material created and maintained in this collection has been categorized by the government as Controlled Unclassified Information/Law Enforcement Sensitive and must be protected in accordance with the information security safeguarding or dissemination controls cited in the policies for Controlled Unclassified Information and Law Enforcement Sensitive information.

U.S. Immigration and Customs Enforcement information technology system security measures provide system-by-system basis, and all systems have varying degrees of access controls. Additionally, all U.S. Immigration and Custom Enforcement systems must abide by U.S. Department of Homeland Security and U.S. Immigration and Customs Enforcement security policies. Moreover, because these systems contain Law Enforcement Sensitive information (information that, if disclosed, could be detrimental to U.S. Immigration and Customs Enforcement law enforcement activities), additional scrutiny is placed upon user access restrictions in the systems to ensure that only authorized users are granted access. These systems

go through security accreditations and the Privacy Impact Assessment process to ensure that only authorized users with a need-to-know will have access to data stored in the system, including social media information and publicly available data.

Other safeguards include technical security measures for information technology systems, which include security access controls that can limit what a user can and cannot access. This is commonly known as *user permissions* and can be managed based upon the users' need-to-know.

14. How does the Component ensure that personally identifiable information is used appropriately?

The U.S. Immigration and Customs Enforcement ensures compliance with personally identifiable information use in the collection of information by instituting rigorous standards for training, Rules of Behavior, information sharing, auditing, and supervisory oversight. Homeland Security Investigations and the Office of Professional Responsibility have established Rules of Behavior specific to the use of social media platforms in executing the protective mission, in consultation with the U.S. Immigration and Customs Enforcement Privacy Office and the U.S. Immigration and Customs Enforcement Office of the Principal Legal Advisor, to ensure that the practices protect the privacy, civil rights, and civil liberties of individuals. U.S. Immigration and Customs Enforcement personnel who collect data from social media platforms certify annually that they have read and understand U.S. Department of Homeland Security and U.S. Immigration and Customs Enforcement policy and privacy guidance on the use of social media information.

Moreover, the U.S. Immigration and Customs Enforcement Privacy Office—in consultation with the U.S. Department of Homeland Security Privacy Office—will: (1) provide oversight of keyword usage and collection minimization strategies; (2) implement real-time data correction mechanisms to address inaccuracies; (3) establish periodic privacy audits to evaluate the effectiveness of mitigation efforts; and (4) ensure efficacy of the tool through metrics. If the identified risks are deemed acceptable within the U.S. Immigration and Customs Enforcement's operational requirements, the agency may continue its current approach while refining safeguards as necessary.