Privacy Impact Assessment

for the

Investigative Case Management (ICM) System

DHS Reference No. DHS/ICE/PIA-045(a)

August 9, 2021

Homeland Security

Abstract

U.S. Immigration and Customs Enforcement (ICE), a component agency within the U.S. Department of Homeland Security (DHS), has updated a major Information Technology (IT) system known as Investigative Case Management (ICM). ICM serves as the core law enforcement case management tool for ICE Homeland Security Investigations (HSI) agents and personnel supporting the HSI mission. HSI conducts transnational criminal investigations to protect the United States against threats to national security and to bring to justice those seeking to exploit U.S. customs and immigration laws worldwide. ICE is updating this Privacy Impact Assessment (PIA) to reflect changes to ICM's information sharing framework with U.S. Customs and Border Protection (CBP), update the "Overview" section of the PIA to better reflect the user base of the system, and document a planned connection to HSI's Digital Records Manager (DRM).

Overview

ICE HSI developed ICM[1] to support its mission to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. ICM serves as the core law enforcement case management tool primarily used by HSI agents and personnel supporting the HSI mission. HSI conducts domestic and transnational criminal investigations to protect the United States against threats to national security; to prevent the illicit cross-border movement of goods, people, and monetary instruments; and to bring to justice those seeking to exploit U.S. customs and immigration laws worldwide. The ICE Office of Professional Responsibility (OPR) has read-only access to ICM as well as audit capability to conduct internal administrative or criminal investigations related to misconduct and/or misuse of ICM. Certain personnel assigned to support HSI at the National Law Enforcement Communications Center (NLECC) have access to ICM to provide communication support.[2] Additionally, certain attorneys in the ICE Office of the Principal Legal Advisor (OPLA) also have read-only access to the system in support of their work on mission-related matters.

Like its predecessor case management system, TECS,[3] ICM enables HSI personnel to create an electronic case file that organizes and links records and documents associated with a particular investigation, so the records can be easily accessed from a single location. It also enables

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM, DHS/ICE/PIA-045 (2016), *available at* https://www.dhs.gov/privacy-documents-ice.

[2] The NLECC is an office run by CBP that acts as a federal law enforcement dispatch service. NLECC provides secure radio, email, and telephonic communications and support to federal law enforcement personnel.

[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TECS SYSTEM: PLATFORM, DHS/CBP/PIA-021 (2016), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

personnel to link records to multiple investigations in order to draw connections between cases, which enhances the investigative process and facilitates coordination and deconfliction.

ICM Users

ICM users are HSI personnel or individuals with a need to know who are either detailed to HSI or personnel subject to HSI oversight assigned to a federal task force in support of HSI's mission. ICM's primary purpose is to support HSI's exercise of its broad legal authority to investigate and enforce a diverse array of federal criminal laws. HSI uses this authority to investigate all types of cross-border criminal activity to protect the United States against threats to national security and to bring to justice those seeking to exploit U.S. customs and immigration laws worldwide. HSI documents and manages its investigative activities in ICM. In addition to criminal investigations, HSI uses the system to manage its civil law enforcement activities and to support criminal prosecutions arising from its investigations. As explained in the previous ICM PIA, ICM is also used in a limited capacity by OPR. Additionally, certain personnel assigned to support HSI at the NLECC have access to ICM to provide communication support.

Reason for the PIA Update

The ICM PIA is being updated to reflect the planned implementation of an ICM interface for Digital Records Manager Module, the planned connection to CBP's user account management system, and updates to the Overview and ICM Users sections to better reflect the actual user base of ICM. The changes are contained in the section above and as follows.

Digital Records Manager (DRM) Interface

ICM plans to implement an interface for a multimedia management system HSI is developing called DRM.[4] The Digital Records Manager will enhance the storage, organization, intake, and output of certain electronic records formats associated with criminal investigations. Examples of multimedia electronic formats include videos, audio, and PDFs. The DRM will aid HSI in the current government-wide effort to become paperless. This new system will provide storage for multimedia files traditionally maintained in the Investigative Case Management system; however, it will not change how HSI uses these records. These multimedia files, which are related to the investigative case file, will be directly uploaded into the Digital Records Manager rather than into ICM. Any multimedia files currently uploaded into ICM will be transferred to the Digital Records Manager as part of the DRM development cycle. The HSI case files themselves will still reside within ICM. The connection between ICM and DRM allows for a folder to be created in the Digital Records Manager to match a corresponding case file in ICM. DRM will

[4] Multimedia is the integration of multiple forms of media including text, graphics, audio, and video. *See* DHS INSTRUCTION MANUAL 262-12-001-01, DHS LEXICON TERMS AND DEFINITIONS, *available at* https://www.dhs.gov/publication/dhs-lexicon.

contain all multimedia files associated with the case file. DRM will also be able to query ICM when a user attempts to access a DRM folder to ensure that the user has access to multimedia files related to the case in question.

New Direct Connection for Transmitting ICM Supervisor Information to U.S. Customs and Border Protection (CBP)

With the modernization of CBP's Identity, Credential, and Access Management (ICAM) system, ICE and CBP are developing a direct connection between ICM and CBP to submit the supervisor information of ICM users directly to CBP's ICAM or any future successor system.[5] No information about members of the public will be collected or shared, and all information shared through this connection is already emailed to CBP as a spreadsheet. This information is limited to DHS employee information. The goal of this intra-Department information sharing initiative is to maintain the most up-to-date supervisor information for ICM users who also use CBP systems. This ensures that the only ICE users who can access CBP's systems through pre-existing connections within ICM are supervisors with a valid need to know.

Privacy Impact Analysis

Authorities and Other Requirements

Pursuant to the Homeland Security Act of 2002 (Pub. L. 107-296, Nov. 25, 2002), the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include, but are not limited to, laws residing in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this authority to ICE in DHS Delegation Number 7030.2, Delegation of Authority to the Assistant Secretary for the Bureau of Immigration and Customs Enforcement and the Reorganization Plan Modification for the U.S. Department of Homeland Security (January 30, 2003).

System of Records Notice (SORN)

ICM data is covered under the existing DHS/ICE-009 External Investigations SORN.[6]

System Security Plan

ICM and the HSI Data Warehouse (HDW), which is a data storage environment that serves as the repository for ICM system data, have each completed Security Control Assessments.[7] The Investigative Case Management system has entered into DHS Ongoing

[5] ICAM is a Commercial-off-the-Shelf (COTS) tool that provides a centralized authentication and access service for CBP system owners to control secure access to CBP systems and/or resources.
[6] *See* DHS/ICE-009 External Investigations, 85 Fed. Reg. 74362 (November 20, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[7] Having this storage function supported by HDW improves the functioning and speed of ICM. For more

Authorization and HDW received an 18-Month Authority to Operate (ATO) which is being renewed in Summer 2021.

Characterization of the Information

This PIA update does not change the characterization of information in ICM.

Uses of the Information

This PIA update covers the upcoming development of an interface to the HSI Digital Records Manager. ICE plans to develop an ICM interface to the DRM which will increase the variety and upload capacity of records related to cases. The system will allow for more file types to be uploaded, as well a greater upload efficiency (multiple files can be uploaded at a time) and larger file size. ICE and CBP are also developing a direct connection between the Investigative Case Management system and CBP to submit the supervisor information of ICM users directly to CBP's ICAM or any future successor system.

Neither of these technical changes impact how the information is being used in ICM.

Notice

This PIA update does not change how ICM provides notice to subjects of records.

Data Retention by the Project

This PIA update does not change the retention period for information maintained in ICM prior to the system changes. Records related to investigative case files are retained for twenty (20) years.[8] Any biometric records will be retained for seventy-five (75) years before destruction.[9]

Information Sharing

This PIA update does not change the external sharing of information maintained in ICM.

Redress

This PIA update does not change redress for individuals with information contained within ICM.

---

information about the HDW, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM, DHS/ICE/PIA-045 (2016), *available at* https://www.dhs.gov/privacy-documents-ice.

[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM, DHS/ICE/PIA-045 (2016), *available at* https://www.dhs.gov/privacy-documents-ice.

[9] *See* DHS/ICE-009 External Investigations, 85 Fed. Reg. 74362 (November 20, 2020) *available at* https://www.dhs.gov/system-records-notices-sorns.

Auditing and Accountability

This PIA update covers a new connection between ICM and the CBP Identity, Credential, and Access Management (ICAM) system as well as ICAM's successor user account management system. The Investigative Case Management system will submit supervisor and profile information of ICM users to CBP's ICAM system and any future successor systems to ensure only those ICE employees with a need to know are accessing CBP systems. Previously, HSI manually emailed this information to CBP as a spreadsheet. No information about members of the public is associated with this information transfer.

Privacy Risk: There is a risk that data will be shared with external parties at CBP without a need to know.

Mitigation: This risk is mitigated. The information shared between ICM and the above systems solely consists of information that is already shared manually between ICE and CBP. Also, all information is shared solely within the DHS network, thereby limiting the risk to potential exposure or compromise.

To the extent that ICE needs to share information with external third parties, any information shared is controlled by the provisions of a Memorandum of Understanding, Memorandum of Agreement, or other data-sharing agreement. ICE's information sharing agreements contain provisions indicating that individuals who receive access to ICE systems (or information from the system) may not further disseminate any data unless they have prior approval from HSI. Any information shared externally is done so in accordance with routine uses in the DHS/ICE-009 External Investigations SORN, and/or as permitted by law. Risks about external sharing are specifically outlined in the original ICM PIA.

Privacy Risk: There is a risk that data is not appropriately secured when shared, and therefore could be accessed by unauthorized parties.

Mitigation: This risk is mitigated. To the extent that ICE needs to share this information with external third parties, appropriate security measures have been taken during electronic transmission so that the risk of compromise is minimal. Information transferred between systems is always encrypted during transfer. All parties sharing information through these connections will have firewalls, intrusion detection systems, intrusion prevention systems, and appropriate access controls to prevent unwanted access to the shared information. All security and access controls are compliant with the DHS 4300A Sensitive Systems Handbook.[10] Also, all sharing of information is done in accordance with appropriate SORN routine uses to ensure that information is only shared with authorized recipients. A corollary to this risk is that information shared externally may not be

[10] *See* DHS 4300A Sensitive Systems Handbook, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

retained and/or destroyed in accordance with the appropriate records retention schedules. This risk is mitigated through applicable information sharing agreements requiring that information is retained and/or destroyed according to the associated records retention schedule. Risks about external sharing are specifically addressed in the original Investigative Case Management PIA. With this PIA update, all information is shared solely within the DHS network, thereby limiting the risk to potential exposure or compromise.

As an additional note, the information shared between ICM and the above systems solely consists of information that is already manually shared between the respective agencies. There is no change in the sensitivity of the accessible information.

Contact Official

Patrick J. Lechleitner
Acting Executive Associate Director
Office of Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-3000

Responsible Official

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717