Privacy Impact Assessment Update

for the

Joint Integrity Case Management System (JICMS)

DHS Reference No. DHS/CBP/PIA-044(a)

February 4, 2025

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) uses the Joint Integrity Case Management System (JICMS) to record claims of employee misconduct, manage criminal and administrative investigations, and track employee and contractor disciplinary actions. The CBP Office of Professional Responsibility (OPR) is responsible for the overall operation of JICMS. CBP published a comprehensive Privacy Impact Assessment (PIA) for JICMS on July 18, 2017.[1] CBP is publishing this Privacy Impact Assessment update to (1) assess the privacy risks and mitigations associated with the new Use of Force Incidents Team System (UFITS) module, (2) describe new technologies, (3) update the list of JICMS users, and (4) update reporting functionality.

Overview

The CBP Office of Professional Responsibility is responsible for ensuring compliance with all CBP-wide programs and policies relating to corruption, misconduct, or mismanagement, as well as for executing internal security, integrity, and management inspections programs. The Office of Professional Responsibility's Investigative Operations Directorate (IOD) is responsible for conducting investigations of alleged criminal and serious, non-criminal misconduct by CBP employees and contractors. The Investigative Operations Directorate is comprised of Special Agents assigned to CBP headquarters and over twenty field offices. Office of Professional Responsibility field offices are managed by Special Agents in Charge and Resident Agents in Charge located strategically throughout the United States, where the threat of internal corruption is most pervasive. The Investigative Operations Directorate coordinates its internal investigative activity with the DHS Office of Inspector General (OIG); U.S. Immigration and Customs Enforcement (ICE) Office of Professional Responsibility; the U.S. Department of Justice, Federal Bureau of Investigation (FBI); and numerous other federal, state, and local law enforcement authorities. Investigative Operations Directorate Special Agents participate full-time as members of numerous Border Corruption and Public Corruption Task Forces.

Although the Joint Intake Center (JIC)[2] located at CBP previously served as the central "clearinghouse" for receiving, processing, and tracking allegations of misconduct involving personnel and contractors employed by CBP and ICE, the Joint Intake Center has been renamed

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE JOINT INTEGRITY CASE MANAGEMENT SYSTEM (JICMS), DHS/CBP/PIA-044 (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[2] To report misconduct, individuals may call the toll-free CBP Intake Center Hotline at 1-877-2INTAKE Option 5; send an e-mail message to JointIntake@cbp.dhs.gov; write to the CBP Intake Center at P.O. Box 14475, 1200 Pennsylvania Avenue, NW, Washington, D.C. 20044; call the DHS OIG at 1-800-323-8603 or 1-844-889-4357 (TTY); send a fax to (202) 254-4297; access the online DHS OIG Complaint/Allegation Form at http://www.oig.dhs.gov/hotline; or write to DHS OIG/MAIL STOP 0305, Attn: Office of Inspector General - Hotline, 245 Murray Lane SW, Washington, D.C., 20528-0305.

the CBP Intake Center and is managed by the CBP Investigative Operations Directorate specifically for CBP employee investigations only as of March 4, 2022. All reports of misconduct, including use of force-related misconduct, are managed directly by each respective DHS Component and coordinated with the DHS OIG and referred to the appropriate office for investigation, fact-finding, or immediate management action. ICE has developed its own intake process, and created new contact mediums (e.g., web portal, email, phone) for reporting misconduct to the ICE Office of Professional Responsibility, Integrity Coordination Center.[3] ICE will continue to address and process complaints submitted through the CBP Intake Center that are ICE's responsibility.

While JICMS remains a shared case management system used by CBP and ICE, the cases are tracked separately within each DHS Component, with ICE inputting information into JICMS through its intake process. JICMS provides a single system that facilitates all aspects of the documentation, investigation, and tracking of employee and contractor misconduct, criminal and administrative allegations, and any associated disciplinary actions. While JICMS is predominantly used to maintain information about issues related to DHS personnel, information from members of the public may be included if it is pertinent to an investigation of alleged misconduct, including complainants, witnesses, alleged perpetrators, or any other persons identified as relevant to an investigation. While the use of JICMS remains a shared system, the CBP and ICE Offices of Professional Responsibility retain sole responsibility for its overall operation pertaining to each agency's separate intake process and administrative and criminal investigations.

Reason for the PIA Update

CBP is updating this Privacy Impact Assessment to (1) assess the privacy risks and mitigation strategies associated with the deployment of a new Use of Force Incidents Team System module; (2) describe new tools and technologies used as part of the investigatory process, (3) update the list of JICMS users to document the information sharing arrangement between CBP and the DHS Office of the Immigration Detention Ombudsman (OIDO) and the removal of the DHS National Protection and Programs Directorate (NPPD) (now known as the Cybersecurity and Infrastructure Security Agency (CISA)), and (4) document the information shared between JICMS and the CBP Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)[4] for reporting purposes.

1. Use of Force Incidents Team Module

[3] To report misconduct, individuals may email ICEOPRIntake@ice.dhs.gov, call 1(833)-4ICEOPR (1-833-442-3677), or visit https://www.ice.gov/about-ice/opr.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE MANAGEMENT INFORMATION SYSTEM-ENTERPRISE DATA WAREHOUSE (EMIS-EDW), DHS/CBP/PIA-034 (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

CBP officers and agents are expected to protect the civil rights and civil liberties of every individual with whom they interact. Though CBP officers and agents are authorized to use force in the conduct of their duties as necessary to ensure the safety and security of both the public and themselves, that force must be used judiciously. When an authorized officer or agent has a reasonable belief during an encounter with a member of the public that the individual poses an imminent danger of serious physical injury or death to themselves or another person, the officer or agent may use force to carry out their law enforcement duties. To the extent that the application of force, including lethal force, is necessary, the CBP officer or agent applying that force is accountable for the outcome.

CBP developed the Use of Force Incidents Team System as a module within JICMS to document information related to use of force incidents and to support CBP Office of Professional Responsibility Investigative Operations Directorate investigations. The Use of Force Incidents Team System functions solely as a case management and tracking tool for the Office of Professional Responsibility's investigation of significant use of force incidents.[5] CBP will continue to separately use the Enforcement Action Statistical Analysis and Reporting (E-STAR) as the mechanism for CBP personnel to report and track the occurrence of use of force events.[6] Data associated with Investigative Operations Directorate investigations managed in the Use of Force Incidents Team System is provided to the CBP Law Enforcement Safety and Compliance Directorate (LESC),[7] as well as the CBP National Use of Force Review Board (NUFRB),[8] to facilitate oversight and review of use of force incidents. Reviews conducted by the National Use of Force Review Board under the direction of the Law Enforcement Safety and Compliance Directorate are undertaken to ensure that CBP officers and agents comply with agency use of force requirements. These requirements are outlined in CBP's *Use of Force Policy, Guidelines and Procedures Handbook*.[9] Additionally, these reviews are designed to identify and assess issues with

[5] A significant use of force incident is a reportable incident that involves injuries or deaths that create a large amount of public attention.

[6] The Enforcement Action Statistical Analysis and Reporting system is formerly known as the "Assaults and Use of Force Reporting System (AUFRS)". *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE E-STAR SYSTEM, DHS/CBP/PIA-045 (2023), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[7] The CBP Law Enforcement Safety and Compliance Directorate is dedicated to optimizing the safety, readiness, accountability, and operational performance of CBP law enforcement personnel by articulating use of force policy, establishing appropriate controls and standards, and supplying the highest quality education, weapons, and other tactical equipment.

[8] The CBP National Use of Force Review Board consists of personnel from the CBP Office of Field Operations, the United States Border Patrol, the CBP Office of Air and Marine Operations, the CBP Laboratory and Scientific Services Directorate, the Department of Justice-Civil Rights Division, ICE Office of Professional Responsibility, CBP Office of Professional Responsibility, the CBP Office of Chief Counsel, the DHS Office of Civil Rights and Civil Liberties, the CBP Office of Public Affairs, and the CBP Law Enforcement Safety and Compliance Directorate.

[9] *See* CBP Use of Force Policy, Law Enforcement Safety and Compliance Directorate, Operations Support, 4500-002A (January 2021), *available at* https://www.cbp.gov/sites/default/files/assets/documents/2021-Jul/cbp-use-of-force-policy_4500-002A.pdf.

current training, tactics, equipment, or policy; so that the Law Enforcement Safety and Compliance Directorate can redraft or better articulate use of force policy, establish appropriate controls and standards, and supply the highest quality education, weapons, and other tactical equipment to CBP personnel in the field.

Law Enforcement Safety and Compliance Directorate personnel are not provided access ,to JICMS, and, therefore, do not have access to the Use of Force Incidents Team System module. To support Law Enforcement Support Center / National Use of Force Review Board reviews, the Office of Professional Responsibility Investigative Operations Division downloads the relevant case data to a secured CD-ROM which is then hand-delivered to the Law Enforcement Support Center. At the conclusion of a National Use of Force Review Board review, the Law Enforcement Safety and Compliance Directorate destroys the CD-ROM, and any information that may have been extracted from it. At the conclusion of a review, the National Use of Force Review Board provides CBP OPR with a decision memo, which the Office of Professional Responsibility Investigative Operations Division uploads into the Use of Force Incidents Team System for memorialization.

While law enforcement agencies outside of DHS are not provided access to JICMS, it is not uncommon for those agencies that work closely with CBP in some instances to be involved in use of force incidents. This close coordination could result in the inclusion of information from and about personnel from other Federal, State, and Local law enforcement agencies in the Use of Force Incidents Team System module as a result of a National Use of Force Review Board review of a use of force incident. The inclusion and use of information from external law enforcement partners by the CBP Office of Professional Responsibility Investigative Operations Division is outlined in the original JICMS Privacy Impact Assessment.[10]

2. OPR Information Technology Tools

In addition to JICMS, the CBP Office of Professional Responsibility Investigative Operations Division utilizes additional information technology tools simultaneously that provide the capability to conduct and support investigations of alleged criminal and serious, non-criminal misconduct by a CBP employees and contractors. One example is the CBP Office of Professional Responsibility Investigative Operations Division's use of audio and video software to create recordings of subject and witness interviews. The files are temporarily captured on standalone CBP authorized desktop workstations until the final recordings are then saved to a shared drive, where the record is added to the JICMS case record.

The second example is an off-network storage solution related to cyber investigative matters that typically address a broad spectrum of activities, from employee bribery and conspiracy

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE JOINT INTEGRITY CASE MANAGEMENT SYSTEM (JICMS), DHS/CBP/PIA-044 (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

cases linked to drugs and human smuggling operations to claims of excessive force, other criminal activities, and government systems misuse. Many of those cases are investigated and the data is stored in a secure authorized system off the DHS network in a controlled environment to maintain the integrity of the information.

Most of the cyber investigations electronic media examination service requests related to employee investigations originate from internal CBP Office of Professional Responsibility Investigative Operations Directorate case agents assigned to JICMS cases; however, the CBP Office of Professional Responsibility Investigative Operations Directorate Cyber Investigations Unit coordinates with the Office of Professional Responsibility Investigative Operations Directorate case agent to assist other federal, state, and local law enforcement agencies with media examinations. During an employee investigation, Office of Professional Responsibility cyber investigators may encounter and collect evidence from a variety of sources that are pertinent to the investigation, including but not limited to computer hard drives, mobile phones, DVDs, SIM cards, digital cameras, social media sources, email service providers, mobile phone service providers, server logs, and other services or devices that may store information related to the investigation. Other requests could include eDiscovery, data recovery, network log analysis, network surveillance, open-source intelligence, and remote data collection.

The Office of Professional Responsibility cyber investigator enters the JICMS case number associated with the investigation, the assignment, the name, email address, and social media handle or ID for the CBP employee under investigation, the contact information for the Office of Professional Responsibility cyber investigator, the Office of Professional Responsibility case agent, and/or the other law enforcement partner agency personnel in a separate administrative case management system. The coordination of each case and information collection is recorded in a Report of Investigation that the Office of Professional Responsibility case agent uploads into JICMS. CBP Office of Professional Responsibility investigations may include incidental collections of personally identifiable information pertaining to members of the public who may be considered witnesses or other subjects of the investigation involved in a particular employee investigation.

When the original requestor and Office of Professional Responsibility mutually concur that a request is complete, the Office of Professional Responsibility closes the services request record in the separate administrative case management system, tracks the outcome of each case in JICMS, and archives forensic image duplications in storage for the appropriate CBP agency records retention period noted in the Data Retention by the Project section of this Privacy Impact Assessment.

3. JICMS User Updates

CBP has implemented an information sharing arrangement with the DHS Office of the Immigration Detention Ombudsman,[11] which was established by Congress in accordance with Section 106 of the Consolidated Appropriations Act of 2020.[12] Members of the public, or their representatives, submit cases directly to the Office of the Immigration Detention Ombudsman by various methods,[13] that are currently tracked in the Immigration Detention Case Management System[14] to maintain a neutral and confidential process. Authorized personnel employed by the Office of the Immigration Detention Ombudsman have been granted system access for JICMS only to review specific cases related to immigration detention facilities owned or operated by CBP, and those employees are collocated with CBP at the CBP Intake Center.

Cases assigned to the Office of the Immigration Detention Ombudsman are assigned in two ways. When an employee investigation relates to operations within a CBP immigration detention facility, the Office of Professional Responsibility Investigative Operations Directorate may assign the specific case to the Office of the Immigration Detention Ombudsman for review, or the Office of the Immigration Detention Ombudsman intake specialists can open and manually enter the case directly in JICMS. The Office of Professional Responsibility Investigative Operations Directorate triages the cases in JICMS to determine the urgency and nature of each complaint, ranging from cold temperatures in CBP facilities to a report of missing property or allegations of employee misconduct. The Office of the Immigration Detention Ombudsman intake specialist enters the information related to the case, contacts their case managers to coordinate the review of the investigation, and creates an interim Report of Investigation that is uploaded to JICMS. The Office of the Immigration Detention Ombudsman records the JICMS case number in the Immigration Detention Case Management System and, conducts an inspection of CBP facilities and gathers information that includes personally identifiable information of individuals involved in the incident that led to the investigation. The Office of Professional Responsibility Investigative Operations Directorate supervisor must review and approve the initial Report of Investigation during the file creation process in the JICMS system.

CBP is also updating this Privacy Impact Assessment to remove the National Protection and Programs Directorate as a JICMS user. The previous Privacy Impact Assessment stated that the National Protection and Programs Directorate is a JICMS system user. The Cybersecurity and Infrastructure Security Agency, formerly known as the National Protection and Programs

[11] The Office of the Immigration Detention Ombudsman is an independent office responsible for objectively and impartially reviewing cases submitted by, or on behalf of, individuals affected by potential misconduct, excessive force, violations of rights of individual detainees, or violations of law, standards of professional conduct, contract terms, policies related to immigration detention, or standards that occurred while in immigration detention by DHS officers, or other contracted, subcontracted, or cooperating entity personnel.
[12] Consolidated Appropriations Act 2020, Pub. L. No. 116-94, December 20, 2019.
[13] Such as via an Office of the Immigration Detention Ombudsman Case Intake Form (DHS Form 405).
[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE IMMIGRATION DETENTION CASE MANAGEMENT SYSTEM, DHS/OIDO/PIA-001 (2021), *available at* https://www.dhs.gov/publication/dhsoidopia-001-immigration-detention-case-management-system.

Directorate, did not use or require access to the system. CISA currently utilizes the DHS Joint-Threat Information Management System (J-TIMS)[15] in lieu of JICMS. There are no other changes to report for access by organizations within or outside of DHS.

4. Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)

Information within JICMS is automatically shared with the CBP Enterprise Management Information System-Enterprise Data Warehouse, which allows CBP to consolidate and present statistical information using reports and graphs with dashboard technology. CBP created a restricted and access-controlled dashboard in Enterprise Management Information System-Enterprise Data Warehouse specifically for the CBP Privacy and Diversity Office, Privacy Division that includes individual level data and displays the status of each employee investigation specifically related to privacy incidents only. This dashboard provides an electronic method for the CBP Office of Professional Responsibility Investigative Operations Directorate to notify and support the CBP Privacy Officer and allows the CBP Privacy Office to immediately identify an appropriate course of action depending on the type of privacy incident investigation, which includes CBP's coordination and notice to the DHS Chief Privacy Officer, remedy options, resource allocation, notification to impacted individuals, risk mitigation, interagency engagement, and the timeliness, content, means, sources, and general appropriateness of other external notification in accordance with the DHS Instruction Guide 047-01-008, Privacy Incident Handling Guidance.[16]

Privacy Impact Analysis

Authorities and Other Requirements

The legal authorities and other requirements associated with CBP's collection, use, maintenance, and dissemination of information within JICMS have not changed since the last Privacy Impact Assessment was published in 2017 and allow CBP and ICE to house information pertaining to use of force incidents and significant incidents within JICMS.

[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE JOINT-THREAT INFORMATION MANAGEMENT SYSTEM (J-TIMS), DHS/ALL/PIA-084 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.
[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY, PRIVACY INCIDENT HANDLING GUIDANCE, DHS INSTRUCTION GUIDE 047-01-008, (December 4, 2017), *available at* https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf

System of Record Notice (SORN) coverage for JICMS is provided by the DHS/ALL-020 Internal Affairs System of Records Notice[17] and the associated Final Rule for Privacy Act exemptions.[18]

CBP completed a system security plan and granted the most recent Authority to Operate (ATO) for the JICMS system on July 14, 2023.

Prior to 2003, JICMS case files were covered by the National Archives and Records Administration (NARA) record retention schedule N1-36-92-1-2 and CBP retained the temporary records that were destroyed 25 years after the case was closed; however, CBP established a NARA approved records retention schedule for significant internal investigation files and routine internal investigation files that are recorded after 2003. The full schedule is outlined under the Data Retention by the Project section of this Privacy Impact Assessment.

As a law enforcement system, JICMS is not covered by the Paperwork Reduction Act (PRA).

Characterization of the Information

JICMS collects, uses, disseminates, and maintains information from employees and contractors supporting CBP and DHS Headquarters, as well from as members of the public. In addition to the list of data elements outlined in the 2017 JICMS Privacy Impact Assessment, CBP collects some additional information due to its deployment of the Use of Force Incidents Team System module.

CBP collects and maintains information about the following categories of individuals and types of records in JICMS. In addition to those elements outlined in the 2017 JICMS Privacy Impact Assessment, CBP may collect the following information from:

1. Subjects of Investigation
    - Medical information pertaining to the subject allegation or complaint;
    - Medical Status;
    - Provider of Medical Assistance;
    - Hospital where Care Given;
    - Medical Examiner's Office;
    - Record of Adverse Actions;

[17] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.
[18] *See* Final Rule for Privacy Act Exemptions, 74 FR 42575 (August 24, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

- Map-based incident location information; and
- Social Media Information.[19]

Complainants, Witnesses, and Individuals Associated with a Case

- Subject Type (the position title, *e.g.*, Border Patrol Agent, CBP Officer, Port Director);
- Office Name;
- Series, Grade, Position Title;
- Work Location;
- Other Disciplinary Actions;
- Arrest Date;
- Incident Date;
- Reported Date;
- Map-based incident location information;
- Financial Information
- State Driver's License Number;
- Vehicle Identification;
- Vehicle License Plate;
- Medical information pertaining to the subject allegation or complaint;
- Medical Status;
- Provider of Medical Assistance;
- Hospital where Care Given;
- Medical Examiner's Office;
- Civil and Criminal History Information;
- Photographic Facial Image; and
- Social Media Information.

[19] Initial complaints may include information, including screen prints, from social media. In addition, CBP investigators may use social media information throughout the course of an investigation. Investigators document the use of social media information in the Report of Investigation (ROI).

2. DHS Headquarters, CBP, Office of the Immigration Detention Ombudsman, and ICE Employees and Contractors Conducting Investigations:
    - Duty station;
    - HashID;[20]
    - Entry on Duty (EOD) Date; and
    - Post of Duty (POD).
3. Supporting Documents Related to Case

If a use of force, significant incident report, or other event is identified that results in the opening of an investigation in JICMS, CBP may collect local police reports, medical examiner reports, and other investigative documentation from outside law enforcement entities.

Sources of the Information

The original sources of the information and how the information is collected for the system have stayed the same since the 2017 JICMS Privacy Impact Assessment and serve as the sources of information for Use of Force Incidents Team System investigations. These individuals may be DHS employees, contractors, or members of the public. Information from social media sources, such as statements, pictures, or videos posted by an individual involved in a case, may also be incorporated into JICMS. The Office of Professional Responsibility Investigative Operations Division's focus is solely on identifying information that is germane to either proving or disproving allegations of misconduct and will only use social media to gather evidence directly relevant to the activity that predicates their investigations.

Information from Other Systems

Data supporting CBP Use of Force Incidents Team System investigations is collected directly from the individuals involved in the incident, including CBP personnel, victims, and witnesses, as well as from the Enforcement Action Statistical Analysis and Reporting system. The Enforcement Action Statistical Analysis and Reporting allows CBP personnel to personally report assaults made against them during an encounter while on-duty or off-duty, as well as use of force incidents. It will enable Air and Marine Interdiction Agents, CBP Officers, U.S. Border Patrol Agents, and other personnel to provide the circumstances surrounding the incident, while capturing information pertaining to the individuals involved.

The sources of information for ICE Use of Force Incidents Team System investigations vary by case, but data associated with ICE use of force incidents is generally received from the

[20] A HashID is a unique identifier assigned to DHS, CBP, and ICE personnel to provide them with access to the Joint Integrity Case Management System and is derived from the employee's Social Security Number.

ICE Significant Event Notification (SEN) system.[21] ICE's Office of Homeland Security Investigations (HSI) created the system to allow ICE field and headquarters managers to provide timely information about critical incidents, activities, and events that involve or impact ICE field staff.

ICE Use of Force Incidents Team System investigations may also include and receive information from the ICE Use of Force, Assaults and Discharges SharePoint Solution (UFAD).[22] When an ICE employee fills out a report within the Significant Event Notification system, the employee will receive a popup notice that simultaneously opens the Use of Force, Assaults and Discharges SharePoint Solution, which is its system. ICE personnel use the Use of Force, Assaults and Discharges SharePoint Solution to document the narrative of any significant events that occur on duty. The Use of Force, Assaults and Discharges SharePoint Solution does not collect any personally identifiable information; the data is used for statistical purposes only.

To ensure the accuracy of information in the system, accuracy verification is conducted at each level of a JICMS case. As outlined in the original JICMS Privacy Impact Assessment, CBP and ICE case agents, officers, and supervisors perform separate checks to verify the accuracy, completeness, and propriety of information entered in JICMS.

Uses of the Information

The uses of information within JICMS outlined in the original Privacy Impact Assessment have not changed**.**

CBP and ICE use the information maintained in the Use of Force Incidents Team System module to record, investigate, and document the incident, from the receipt of an incident through the investigative process and to the final disposition as it relates to use of force incidents and significant incidents that occur involving CBP and ICE employees, contractors, and members of the public. As the original Privacy Impact Assessment mentions, the system also provides data for reporting allegations to management. All reports of misconduct with the use of force are coordinated with the DHS OIG and referred to the appropriate office for investigation, fact-finding, or immediate management action. JICMS provides enhanced querying and sorting capabilities, which enable routine and ad hoc reports using primary data elements. These reports are generated for statistical and performance-based purposes when managing cases. Investigators gather additional background information regarding individuals associated with a case to draft a Report of Investigation (ROI), which also serves as the final determination for an incident.

---

[21] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE SIGNIFICANT EVENT NOTIFICATION SYSTEM, DHS/ICE/PIA-023 (2010), *available at* https://www.dhs.gov/privacy-documents-ice.

[22] The ICE Office of Firearms and Tactical Programs (OFTP) and the Office of Professional Responsibility have developed the Use of Force, Assaults, and Discharges SharePoint Solution to create a central location for the timely and accurate reporting of use of force incidents involving ICE law enforcement personnel.

The DHS Office of the Immigration Detention Ombudsman will use the information shared between CBP and the Office of the Immigration Detention Ombudsman regarding (1) complaints received by the Office of the Immigration Detention Ombudsman against CBP and/or its employees, contractors, or; (2) audits, inspections, investigations, observations, and reviews related to detention standards, misconduct, or the violation of individuals' rights in short term holding facilities; (3) announced and unannounced inspections of CBP short term holding facilities and services; and (4) recommendations by the Office of the Immigration Detention Ombudsman to address concerns or recommend improvements regarding the treatment of detained persons, including operations of CBP short term holding facilities and services.

Each authorized user in CBP, ICE, DHS Office of the Immigration Detention Ombudsman, and DHS Headquarters maintain a limited permission level based upon their assigned roles and responsibilities within their component, and there are no additional changes to report with this Privacy Impact Assessment Update.

Notice

This Privacy Impact Assessment Update the DHS/ALL-020 Internal Affairs System of Records Notice,[23] and the corresponding Final Rule for Privacy Act exemptions provide public notice of the collection, use, and maintenance of this information in DHS systems.

Data Retention by the Project

CBP maintains significant internal investigation files, including those pertaining to national security, sexual assaults or abuse of detainees in CBP custody, critical incidents involving death or serious injury, public corruption, standards of detainee care, deprivation of civil rights under the color of law, matters attracting substantial media or Congressional attention, and misconduct on the part of senior agency officials, that are considered permanent records under the NARA records schedule number DAA-0568-2018-0001-0003. The records retention period is cut off when the case is considered closed or when all actions have been completed, whichever is later. CBP transfers records to the National Archives 20 years after the cutoff date.

In accordance with NARA guidance, the Office of Professional Responsibility Investigative Operations Division manages CBP routine internal investigation files, which include all internal investigation files except for those covered by the authority for significant internal investigation files under records schedule number DAA-568-2018-0001-0002. CBP maintains the routine internal investigation files, and the records retention period is cut off when the case is considered closed, and the temporary records are destroyed 25 years after the cutoff.

Information Sharing and Disclosure

[23] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 Fed. Reg. 23361 (April 28, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.

On August 5, 2022, CBP entered into a Memorandum of Agreement to share information located in JICMS with the Office of Immigration Detention Ombudsman. These records only pertain to the coordination of complaints, investigations, reviews, audits, inspections, and recommendations related to detention standards, misconduct, or the violation of individuals' rights in the short term CBP holding facilities.

There are no other changes to the internal and external information sharing and disclosure procedures to report for this system.

Individual Access, Redress, and Correction

Access, redress, and correction procedures have not changed for this system.

Auditing and Accountability

There are no changes to auditing or accountability for JICMS since the last Privacy Impact Assessment.

Contact Official

Jeffrey R. Egerton
Investigative Operations Division
Office of Professional Responsibility
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
CBP Privacy Officer
U.S. Customs and Border Protection
PRIVACY.CBP@cbp.dhs.gov

Approval Signature

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

_____

Roman Jankowski
Chief Privacy Officer
U.S. Department of Homeland Security
privacy@hq.dhs.gov