Privacy Impact Assessment

for the

Criminal Case Management System (CCMS)

DHS Reference No. DHS/CBP/PIA-081

August 15, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) Criminal Case Management System (CCMS) serves as the primary investigative case management system for all criminal cases in various stages of investigation across CBP.[1] CCMS allows CBP to record, maintain, link, coordinate, de-conflict, and share timely criminal case information, as well as centrally manage evidence, document criminal case development, and track prosecutorial and investigative outcomes. CBP is conducting this Privacy Impact Assessment (PIA) to assess the potential privacy risks and mitigation measures associated with CCMS because it collects, stores, and uses personally identifiable information (PII) about members of the public.

Overview

CBP enforces hundreds of U.S. laws and regulations, including customs, immigration, trade, and narcotics laws. As part of its broad mission authorities, CBP enhances border security, national security, and public safety through the criminal, civil, and administrative enforcement of hundreds of federal laws and regulations. CBP has the authority to investigate various criminal and immigration law violations and make recommendations for prosecutions. CBP also has authority to conduct undercover investigations to exercise its investigatory authorities.[2] To support its management of information collected, generated, and maintained as part of its investigatory processes, CBP has developed CCMS.

Historically, CBP maintained its criminal case files in various unofficial, siloed, or now-defunct case management systems. CBP created CCMS to standardize CBP criminal case management across the CBP enterprise. The primary users of CCMS are CBP sworn law enforcement agents/officers as well as case analysts (i.e., individual users that may support a criminal case investigation by conducting research and analysis duties) within the U.S. Border Patrol (USBP), Air and Marine Operations (AMO), and Office of Field Operations (OFO). For this Privacy Impact Assessment, CBP agents/officers and case analysts will collectively be referred to as "users."

CCMS enables the creation of electronic case files to organize and link records and documents potentially relevant to a criminal case. CCMS allows CBP employees to record, store, link, coordinate, de-conflict, and share (internally) timely criminal case information, as well as centrally manage evidence, document criminal case development, and track prosecutorial and

[1] CCMS will not serve as the case management solution for internal investigations conducted by the Office of Professional Responsibility (OPR), Office of the Inspector General (OIG), or any other internal investigation regarding CBP contractors or employees.
[2] Based on certain authorities delegated to U.S. Border Patrol under Title 8 and 19 of the U.S. Code.

investigative outcomes. CCMS is not an intelligence database, prosecutions module,[3] or administrative/civil case tracking system. It will be used solely for CBP criminal investigative efforts that require a sustained, longitudinal investigative effort.

CCMS creates an electronic case file that organizes and links all records and documents associated with a particular case in a central repository. CCMS links records between multiple investigations to draw connections between cases, enhancing the overall investigative process, and facilitating cross-agency coordination and deconfliction.[4] CBP users are responsible for identifying, collecting, and documenting data held in other CBP systems that may be relevant to an investigation. Upon review and approval by the user's supervisor, users may import data from CBP source systems into CCMS. This data then becomes part of the respective CCMS case file.

CCMS maintains comprehensive criminal investigation case files or Subject Records that contain Entities[5] and case documents. Any Entity or case document may be linked to other Entities within CCMS, such as a case file, another Subject Record, or another case document. This ensures all investigative information related to a subject is available to users and supports coordination and deconfliction between criminal cases. Case documents include Reports of Investigation (ROI), evidence, court records, and incident reports including arrest reports, seizure reports, agent case notes, and electronic surveillance reports.

Web-based Application

CCMS is an internal web-based application that runs within the Automated Targeting System (ATS)[6] security boundary.[7] Users with an operational or administrative need to access CCMS must request and receive approval from their supervisor, and complete mandatory training on the use of CCMS before they are granted access. All users of CCMS are required to maintain access the Automated Targeting System.

One of the primary benefits of CCMS is its ability to identify related investigations and ensure they are properly deconflicted. This ensures the respective investigative teams do not

[3] For information on CBP's prosecutions module, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE CBP PORTAL (E3) TO ENFORCE/IDENT, DHS/CBP/PIA-012 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[4] Deconfliction is the process of determining whether multiple law enforcement agencies are investigating the same person or crime. The system will provide notification to each agency involved of the shared interest in the case, and provide relevant contact information. This is an information and intelligence sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation.

[5] There are six types of Entities: Person, Business, Aircraft, Vehicle, Vessel, and Thing. Entities are described in full later in the Privacy Impact Assessment.

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM (ATS), DHS/CBP/PIA-006 (2007 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[7] Although CCMS is maintained within the Automated Targeting System security boundary, it is completely partitioned from all data holdings and sources within the Automated Targeting System.

inadvertently interfere with one another's investigative work. Deconfliction of new Entities is vetted within the system autonomously. This deconfliction search only includes Entities within CCMS, not a full search of Automated Targeting System holdings. If the Entity matches an existing Entity assigned to another case, the users are notified for deconfliction. Unless restricted, CCMS records are visible to all other users within their provisioned Field Office/Sector/Branch to promote deconfliction and coordination of law enforcement work. This process is discussed in further detail in Section 3.4. When appropriate, users may limit the visibility of records related to certain sensitive investigations to a select subset of users. Limiting in this manner may occur, for example, in a particularly sensitive investigation when it is appropriate for only the team of CBP agents/officers engaged in the case and their supervisors to have access to the case records. Supervisors always have access to the records and cases their subordinates create. All user activity is tracked in audit logs.

Case Files

CCMS documents law enforcement information that relates to an individual, organization, business, or group suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more violations of a law CBP enforces or administers. Users document this law enforcement information in case files. Users open case files to document information obtained by CBP while conducting law enforcement and border security investigations. CCMS is used to track and manage these CBP cases, as well as to identify when other law enforcement partners are potentially investigating other elements of a criminal statute, in which case all partners coordinate on bringing a complete case forward for indictment.

The CCMS case file only contains information that documents law enforcement and investigative activities and is not an intelligence reporting system. Law enforcement intelligence information collection, processing, and analysis will continue to be maintained and conducted in the Intelligence Reporting System-Next Generation (IRS-NG).[8] All information collected when assisting other law enforcement agencies in pursuit of criminal case development pertaining to a particular CBP investigation, beyond the initial apprehension and processing, will be documented and maintained in CCMS.

The primary building block of a case file in CCMS is an "Entity." There are six types of Entities: Person, Business, Aircraft, Vehicle, Vessel, and Thing. Within CCMS, for each entity, there are categories that may be added to document information directly relevant to the investigation, such as people, phone numbers, social media username/handle, and firearms. Users select an Entity category and may input information associated with that category. For example, in the person Entity a user may input the biographic information of an individual associated with

[8] *See* the forthcoming U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE INTELLIGENCE REPORTING SYSTEM-NEXT GENERATION (IRS-NG), which will be *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

the case. This could be name as well as descriptive information such as height, weight, and race, only as relevant to the investigation. Additionally, a user may include the photograph of the individual in the person Entity (again, only as relevant to the investigation). Other Entity categories, such as phone number or vehicle, allow users to add additional information as well as link information between Entities. Users create Entities within a case file and can create as many Entities associated with a case as needed.

Users then use the information from the Entities to create Reports of Investigation in the same case file. A Report of Investigation is a narrative documenting investigative activity. It may describe case details and statuses, summaries of events (e.g., subject encounters, witness or victim interviews, surveillance activities), agent/officer observations, descriptions of evidence, and any other information relevant to a case. Additionally, users may use CCMS to record investigative steps and findings. This includes attaching supporting documentation which may include video or still images related to an investigation.

When an event or incident processed in a CBP system of record (such as e3 or Unified Secondary[9]) is determined by a user to warrant further law enforcement inquiries or investigative activities, the initial case predication (the report, record, or incident which preceded or led to the initiation of the case) is uploaded into CCMS. A copy of the original event or incident record, and any relevant reports and documents from the enforcement system(s) will then become part of the new criminal case file.

Users may open cases when the required justification standard is met to investigate a continuing violation of law CBP enforces or administers. Justification is determined based on supervisory approval for investigation when there is a likelihood of an ongoing violation of law. CBP users may open a case only with supervisory approval. With approval, the user may open, manage, refer, or close case files; complete reports and other case-related data entry in a timely manner; ensure accuracy and completeness of reports and other law enforcement records within a case file; and coordinate law enforcement efforts when an investigation affects multiple areas of responsibility.

Oversight

CBP developed CCMS so that supervisors may view the actions of their subordinate users. Supervisors are required to review and approve many user actions within the system. This helps ensure the accuracy of the information as well as the accountability of users. Supervisors may view all case files created by their subordinates. Supervisors approve the opening, referral, closure, or other status changes of a case file. Case files are reviewed by the user and their supervisor on a

[9] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE UNIFIED SECONDARY SYSTEM, DHS/CBP/PIA-067 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

quarterly basis. Supervisors review and approve or return reports, Subject Records, or other information submitted for correct structure, accuracy, and completeness.

Case files are closed when no new information is discovered after a period of six months from the date of initiation; when prosecution is declined; or when prosecution and all appeals are complete. Supervisors may authorize the reopening of a case if the case has not been referred for prosecution, been declined for prosecution, or the prosecution has concluded if new information regarding potential criminal activity related to the investigation is discovered or developed. For example, supervisors are authorized to reopen closed cases when it is determined that a recent e3 and/or TECS event (or events related to a previously closed case) warrant opening a new criminal case file. Opening and closing of case files are documented in a Report of Investigation and approved by the supervisor.

Deconfliction and Information Sharing

CBP developed CCMS to deconflict and share case file information within CBP and externally in support of prosecutions. Deconfliction takes place automatically based on Entity. The system automatically searches across all open Entities regardless of Field Office/Sector/Branch cases to ensure investigative information is deconflicted, thereby aligning future discovery, exculpatory information, and relevant information required to be disclosed. This means that if a user opens a new case file and creates an Entity for "John Smith" with a January 1, 2000, date of birth, the system will automatically search all case files to identify any matching Entities. If there is a matching Entity, the system will notify the user to contact the owner of the existing case file to deconflict.

Unless restricted, CCMS records are visible to all other users within their provisioned Field Office/Sector/Branch to promote deconfliction and coordination of law enforcement work. Access to cases may be further restricted or expanded by the owning case agent/officer with supervisor approval. Cases with source data derived from copies of protected databases external to DHS (i.e., Financial Crimes Enforcement Network (FinCEN)[10] data and/or other agency criminal case management systems) to include Law Enforcement Technical Collection (LETC)[11] records, will be restricted by the responsible case agent/officer, limiting access to case records only to the case agents/officers and their supervisors. Users may search for and view all cases initiated with the same duty station in a read-only mode unless the case is restricted.

When a case involves one or more jurisdictions with a nexus to the case, CBP may disclose information within the case file outside of DHS, generally with other federal, state, local, or

[10] For more information about FinCEN, *see* FinCEN Privacy Impact Assessment for Data Collection, Storage, and Dissemination, *available at* https://www.fincen.gov/sites/default/files/shared/FinCEN_DCSD_PIA.pdf.
[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR BORDER SURVEILLANCE SYSTEMS, DHS/CBP/PIA-022 (2014 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

international law enforcement agencies. All external disclosures are accounted for and documented in the case file. Only trained and provisioned CBP users have access to CCMS. External stakeholders (e.g., Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), ICE Homeland Security Investigations (HSI)) will not have access to the system, though case information may be shared with stakeholders as it relates to joint case development, as appropriate. All information sharing is documented in CCMS in accordance with CBP information sharing policies.

Section 1.0 Authorities and Other Requirements

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

Pursuant to the Homeland Security Act of 2002, the Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. CBP is responsible for the enforcement of many laws, but primarily conducts criminal investigations pursuant to Title 6 of U.S. Code (U.S.C.): Domestic Security; and Title 8 of U.S. Code: Aliens and Nationalities, and implementing regulations and Title 19 of U.S. Code: Customs Duties, and implementing regulations.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Data retained and linked in CCMS is covered under the following System of Records Notices.

User account information:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[12]

Enforcement and/or incident records that may be indicate a potential violation of law:

- DHS/CBP-023 Border Patrol Enforcement Records (BPER)[13]
- DHS/CBP-013 Seized Assets and Case Tracking System[14]

[12] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[13] *See* DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[14] *See* DHS/CBP-013 Seized Assets and Case Tracking System, 73 Fed. Reg. 77764, (December 19, 2008), *available at* www.dhs.gov/system-records-notices-sorns.

- DHS/CBP-011 U.S. Customs and Border Protection TECS[15]

Investigatory files:

- DHS/CBP-006 Automated Targeting System[16]

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. CCMS is a module within the Automated Targeting System security boundary. The Automated Targeting System received an Authority to Operate (ATO) on January 16, 2023.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

CBP is developing a National Archives and Records Administration (NARA) approved record retention schedule for criminal case records. Per the Border Patrol Enforcement Records (BPER) and TECS System of Records Notices, CBP anticipates retaining records of arrests, detentions, and removals for seventy-five (75) years. Investigative information that does not result in an individual's arrest, detention, or removal is retained for twenty (20) years after the investigation is closed, consistent with the N1–563–08–4–2. CCMS user account management records are retained for ten (10) years.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

All information collected and maintained in CCMS is in support of a criminal investigation. The collection of information for purposes of a criminal investigation is exempt from the requirements of the Paperwork Reduction Act (PRA).

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

CCMS maintains information about the following individuals: subjects of investigations, associates of subjects of investigation directly relevant to the investigation, witnesses, informants,

[15] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[16] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.

victims, and other third parties directly relevant to the investigation (e.g., individual who reports a crime). CCMS maintains personally identifiable information in case documents (such as Reports of Investigation) and Entity records. For example, a Vehicle Entity record may contain the name and address of the person to whom the vehicle is registered.

The types of information contained in Entity records (to include documents, exhibits) and case records directly relevant to an investigation includes:

- *Biographic data*, including subject name, alias, date of birth, Social Security Number, A-Number, address, phone number, email address, social media username/handle, driver's license number, passport number, vessel registration number, pilot's license number, criminal history, and immigration status and history.
- *Descriptive data*, including eye color, hair color, height, weight, and any other unique physical characteristics (e.g., scars, marks, tattoos).
- *Financial data*, including data on suspicious financial activity, currency transaction reports, Bank Secrecy Act (BSA) derived information, cryptocurrencies, peer-to-peer applications, and currency or monetary instrument reports.
- *Evidence and descriptions of evidence* obtained during an investigation, including: statements of subjects and witnesses, photographs, emails, phone records, bank records, travel history, and other related documents. This may include audio, video, photographs, and maps. Depending on the nature and volume of the evidence, the user may scan and upload the evidence or link the evidence to other records in CCMS. In the case of large volume of records (i.e., boxes of files), the user may cite excerpts from the original source documents. Evidence may also reference or link to (i.e., Seized Assets and Case Tracking System (SEACATS))[17] physical items seized (i.e., vessels, narcotics, or firearms), as well as descriptions and photographs of physical evidence. These physical items are tracked in the Seized Assets and Case Tracking System and stored in CBP evidence rooms for use during a prosecution. Any of the materials described above may contain personally identifiable information. Evidence may also include attributes and metadata e.g., Phone Number and Device Data, Seized Assets and Case Tracking System ID that are associated via the Laboratory Information Network (LIN)[18] unique ID to the case. This evidence may include recorded audio or video statements/interviews, property of individuals related to the case such as the data

[17] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE SEIZED ASSETS AND CASE TRACKING SYSTEM, DHS/CBP/PIA-040 (2017), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE LABORATORY INFORMATION NETWORK (LIN), DHS/CBP/PIA-054 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

and metadata collected from portable electronic device, computers, vehicles, drones, etc., documents, contraband, currency, credit cards, monetary instruments, bank statements, and wire transfer records and weapons. Additional information may be from interviews of suspects, witnesses, and from sworn affidavits.

- *Forensic data* may include the Laboratory Information Network case numbers and analyst reports, latent print reports, DNA data reports and comparative analyses reports (if available), digital forensics data reports, gunshot residue (GSR) reports, crime scene reports including photographs and video, and chemical analysis reports of suspected controlled substances. Additionally, digital forensic information from the DOMEX[19] and PenLink[20] programs may be uploaded into CCMS.
- *Surveillance data* may include video or still images from surveillance technology, Latitude/Longitude location from sensors, license plate numbers, video and still images from body worn cameras, addresses of businesses and residences related to the investigation.
- *Law Enforcement Technical Collection (LETC) data* includes audio recordings of radio communications associated with illicit activity, non-audio information obtained using radio frequency sensors, including metadata and associated event information, and geolocation of signals through available radio frequency and location data.
- *Location-related data*: Most location data maintained in CCMS is collected by CBP agents/officers during surveillance activities or witness accounts. CCMS may also contain specific types of location data from surveillance tools and technologies when used to support an investigation.
    - License plate reader (LPR) data.[21] CCMS may contain limited location data from license plate reader cameras operated by CBP and placed for surveillance during a particular investigation or obtained during a joint investigation with a local, state, tribal or federal law enforcement partners with access to license plate reader databases containing data collected only from law enforcement sources. This data may include images of vehicles license plates associated with a subject of an investigation (a person or vehicle), date and time, and GPS coordinates for the

[19] *See* U.S. Customs and Border Protection, CBP Directive No. 3340-049A, Border Search of Electronic Devices (January 4, 2018), *available at* https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.
[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE USBP DIGITAL FORENSICS PROGRAMS, DHS/CBP/PIA-053 (2018 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[21] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CBP LICENSE PLATE READER TECHNOLOGY, DHS/CBP/PIA-049 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

location where the license plate was photographed. The sources for this data are detailed in Section 2.2. The case agent/officer may upload the images into CCMS as case documents and link the images to Subject Record. The case agent/officer may also describe this information and any related actions in arrest reports, other incident reports, or Reports of Investigation.

- Location tracking tools.[22] CBP uses various technologies to support the location tracking of individuals, vehicles, and contraband during a criminal investigation. These location tracking tools, including covert tracking devices, do not store identity information about an individual nor do they maintain a list of individuals who are the subject of a CBP investigation. These tools maintain a list of devices that are the subject of a criminal investigation by various device identification numbers (e.g., serial number, Mobile Directory Number, International Mobile Equipment Identity, Mobile Equipment ID) and their current locations using GPS and/or assisted Cellular Tower coordinates.

2.2 What are the sources of the information and how is the information collected for the project?

During a criminal investigation, CBP may collect information from many internal and external sources, including, for example, surveillance activities, individuals, and other DHS sources and federal agencies.

Surveillance Activities

Case agents/officers document observations and surveillance activities directly related to an investigation primarily in Reports of Investigation. Other examples of documentation include:

1. CBP agents/officers may set up surveillance video cameras to record individuals entering and exiting a specific location where there is suspected criminal activity. The CBP agent's/officer's description of the probative video footage would be documented in a Report of Investigation, and the footage may be uploaded to CCMS.
2. CBP agents/officers may conduct electronic surveillance, such as a monitored/recorded phone call or videotape of a meeting between a subject and an undercover CBP agent/officer. These activities are generally conducted when one party (e.g., an CBP agent/officer, cooperating defendant, or confidential informant) has consented to the monitoring or pursuant to a warrant. The electronic surveillance is first documented on an audio/video recording device and/or application and is

[22] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR BORDER SURVEILLANCE SYSTEMS, DHS/CBP/PIA-022 (2014 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

converted to an electronic medium ingestible by CCMS or a physical copy (CD, thumb drive, etc.) and is stored in an evidentiary vault and/or uploaded into CCMS for evidentiary purposes.

Individuals

Some of the investigative data maintained in CCMS comes from subjects of criminal investigations, associates of subjects directly relevant to an open investigation, victims, registered informants, and other third parties who are questioned or interviewed during the investigation. This includes information obtained from documents provided by or retrieved from individuals. Information collected from these sources may be found in case documents. For example, a case agent/officer may document the information collected in an informant interview in a Report of Investigation. The agent may also learn of a previously unknown criminal associate during this interview and create a new Subject Record with that information. Alternatively, the case agent/officer may be given an item or document by an individual directly relevant to an investigation (e.g., a photograph or receipt) and summarize and/or upload a copy of the document into CCMS.

DHS Record Sources

During an investigation, CBP may collect information from paper or electronic records from CBP holdings and other DHS Components (typically U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Transportation Security Administration (TSA), and U.S. Coast Guard (USCG)). This may occur via queries to the systems maintained by the other Components to which CBP has user access, or via manual requests made to Component personnel. CBP requests and collects this information from DHS Components pursuant to section (b)(1) of the Privacy Act of 1974 and only if it is directly relevant to an investigation. CBP will not disclose non-CBP information to other law enforcement partners without express approval of the owning Component.

CBP sources most of the data maintained in CCMS from its own internal data holdings, or those of other DHS Components. Case agents/officers manually input all relevant information for a case into CCMS. Despite residing within the Automated Targeting System security boundary, CCMS does not search or access the data holdings available for targeting, screening, and vetting purposes within the Automated Targeting System.

Data from the systems below are used as evidence or supporting documentation in sworn affidavits[23]:

CBP Portal (E3) to ENFORCE/IDENT (e3) collects and transmits data related to law

[23] CBP Form G-166c.

enforcement activities to the ICE Enforcement Integrated Database (EID)[24] and the DHS Automated Biometric Identification System (IDENT),[25] which will be replaced by the Homeland Advanced Recognition Technology System (HART).[26] CBP uses e3 to collect and transmit biographic, encounter, and biometric data of individuals encountered by U.S. Border Patrol.

TECS System: The TECS Platform facilitates information sharing among federal, state, local, and tribal government agencies, as well as with international governments and commercial organizations related to CBP activities. CBP's mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement at the border of hundreds of laws on behalf of numerous federal agencies. Through the TECS Platform, users may input, access, or maintain law enforcement, inspection, intelligence-gathering, and operational records. TECS collects and maintains information on individuals (1) prior to arrival, (2) at the time of arrival, (3) throughout the inspection process, and (4) prior to departure; this data is broadly referred to as "Traveler Data."

Automated Targeting System (ATS) is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. Automated Targeting System data includes:

- Information about importers and cargo and conveyances used to import cargo to the United States from destinations outside its borders;
- Information about exporters and cargo and conveyances used to transport cargo from the United States to destinations outside its borders;
- Information about vehicles and persons crossing land border locations. This data includes license plate numbers for vehicles entering the United States, vehicle and registered owner data (derived from state Department of Motor Vehicle records);
- Information about travelers entering the United States from destinations outside its borders. This data includes passenger manifests, immigration control information

[24] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.
[25] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DHS/OBIM/PIA-001 (2012), *available* at https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim. DHS is in the process of replacing IDENT with the Homeland Advanced Recognition Technology System as the primary DHS system for storage and processing of biometric and associated biographic information.
[26] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF BIOMETRIC IDENTITY MANAGEMENT, PRIVACY IMPACT ASSESSMENT FOR THE HOMELAND ADVANCED RECOGNITION TECHNOLOGY SYSTEM (HART) INCREMENT 1, DHS/OBIM/PIA-004 (2020), *available at* https://www.dhs.gov/privacy-documents-office-biometric-identity-management-obim.

and Passenger Name Record (PNR) information[27] (for which the Automated Targeting System is the source system); and

- Watch-listed data and data regarding other high-risk parties.

Unified Secondary (USEC) is used to process individuals referred for a secondary admissibility, customs, or agricultural inspection at a United States at Ports of Entry.

Seized Assets and Case Tracking System (SEACATS) is the information system of record for the full lifecycle of all enforcement incidents related to CBP operations. The system tracks the physical inventory and records disposition of all seized assets, as well as the administrative and criminal cases associated with those seizures, and functions as the case management system capturing the relevant information and adjudication of the legal outcomes of all fines, penalties, and liquidated damages. The system also serves as the financial system of record for all collections related to these enforcement actions.

CBP License Plate Reader Technology (LPR) includes (1) license plate number; (2) digital image of the license plate as well as the vehicle's make and model; (3) state or province of registration; (4) camera identification (i.e., camera owner and type); (5) GPS coordinates of the image capture, or other location information taken at the time the information was captured; and (6) date and time of observation. License plate reader technology may also capture (within the image) the environment surrounding a vehicle, which may include drivers and passengers.

Tasking, Operations, and Management Information System (TOMIS)[28] contains case-relevant information pertaining to CBP aircraft and vessels. CCMS may reference Tasking, Operations, and Management Information System supporting evidence including flight records containing aircraft utilized; takeoff/landing dates, times, and locations; flight crew; and flight crew mission narrative. In addition to flight records, CCMS may reference records pertaining to the CBP vessel utilized; departure/arrival dates, times, and locations; crew manifests; and mission narrative.

PenLink (PLX) is used primarily by U.S. Border Patrol agents to maintain the metadata

[27] Uses of Passenger Name Record information within CCMS is subject to use limitations consistent with internal CBP policies and procedures.

[28] Tasking, Operations, and Management Information System (TOMIS) is a web-based task and operations management system designed to provide consistent and standardized mission and case tracking and reporting services to Air & Marine Operations. TOMIS is a unified data processing and reporting environment for Air & Marine Operations, and is designed to be a robust, secure, and scalable system to facilitate important information transfers vital to the law enforcement mission. The core function of TOMIS is to provide a single tool for Air & Marine Operations aviation and maritime field operatives to schedule and process detailed pre- and post-mission data, process enforcement and non-enforcement events, perform mission functions related to aviation and maritime asset management, automate Air & Marine Operations subject targeting, and interface seamlessly with other in-house and external agency information technology products and initiatives. TOMIS does not collect or maintain personally identifiable information.

from a forensic acquisition report, which is a report created from the image copy by a digital forensic tool. By using PenLink, U.S. Border Patrol standardized the way it collects, retains, and uses information derived from digital forensic cases and data obtained from telecommunications providers pursuant to subpoenas or warrants. CCMS may reference PenLink records pertaining to digital forensic cases, or CCMS may be referenced by PenLink as the source system that is the basis for issuing subpoenas and search warrants.

ICE Student and Exchange Visitor Information System (SEVIS).[29] Case agents/officers may access the Student and Exchange Visitor Information System during a related investigation. Case agents/officers may access Student and Exchange Visitor Information System information and information from the Certificates of Eligibility (Forms I-20 and DS-2019).[30]

USCIS Computer Linked Application Information Management System (CLAIMS)[31] is an electronic case management application tracking and processing system. USCIS uses the system as automated support for the variety of tasks associated with processing and adjudicating immigration benefit applications. Case agents/officers may use the system during an investigation of a subject.

USCIS Person Centric Query Service (PCQS)[32] allows users to submit a single query and view all transactions involving an immigrant or nonimmigrant across multiple DHS and external systems. The Person Centric Query Service returns a consolidated view of an individual's past interactions with DHS Components and other agencies as they moved through the U.S. immigration system.

Non-DHS Sources of Information

CCMS may also maintain documents and information collected by another federal, state, local or tribal agency, that either has no statutory authority or investigative interest in pursuing a criminal investigation into an alleged crime over which CBP has investigative jurisdiction, though may maintain information directly relevant to a CBP investigation. Such collected documents,

[29] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT AND EXCHANGE VISITOR INFORMATION SYSTEM (SEVIS), DHS/ICE/PIA-001 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.
[30] I-20, "Certificate of Eligibility for Nonimmigrant Student Status" and DS-2019, "Certificate of Eligibility for Exchange Visitor (J-1) Status" The I-20 is used by SEVP for F-1 and M-1 nonimmigrants, while the DS-2019 is used by Department of State for J-1 nonimmigrants. These forms are not publicly available; they are provided only by designated school officials or sponsors.
[31] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE COMPUTER LINKED APPLICATION INFORMATION MANAGEMENT SYSTEM (CLAIMS 3) AND ASSOCIATED SYSTEMS, DHS/USCIS/PIA-016 (2008 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.
[32] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES, PRIVACY IMPACT ASSESSMENT FOR THE PERSON CENTRIC QUERY SERVICE, DHS/USCIS/PIA-010 (2016 and subsequent updates), *available at* https://www.dhs.gov/uscis-pias-and-sorns.

information, evidence, and personally identifiable information may be used by CBP and maintained in CCMS for the continuance of the investigation through case adoption. For example, a CBP case agent/officer on a Drug Enforcement Administration (DEA) task force may uncover a suspected crime related to CBP's enforcement authorities. If the DEA declines investigating the CBP-related case, the CBP case agent/officer may initiate a complementary investigation in collaboration with the DEA's investigation.

Department of Justice, Federal Bureau of Investigation, National Crime Information Center (NCIC) System[33] contains information on criminal targets, immigration violators, and stolen articles. The National Crime Information Center may also contain data from Nlets, a non-profit organization owned by the 50 states that facilitates the exchange of law enforcement information amongst local, state, tribal and federal law enforcement partners. The CBP case agent/officer may use National Crime Information Center information, including but not limited to warrants that are input by other law enforcement agencies, terrorist watchlist records, state and federal criminal history reports, and reports of missing persons.

Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS)[34] includes biometric, identity history, biographic, property, and case/incident history data. The Case agent/officer may collect Criminal Justice Information Services information, including but not limited to biometric, identity history, criminal history, biographic, and case history input by other law enforcement agencies. Case agents may utilize Criminal Justice Information Services information to conduct risk assessments on potential targets of investigation for officer safety reasons, and prosecutorial guidelines/enhancing factors.

Federal Bureau of Investigation (FBI) Next Generation Identification (NGI)[35] is the criminal history database for the FBI. Next Generation Identification contains over 100 million subjects and provides the criminal justice community with the world's largest and most efficient electronic repository of biometric and criminal history information. Case agents/officers may use Next Generation Identification during a criminal investigation.

Department of Defense Automated Biometric Identification System (ABIS)[36] is the Department of Defense's authoritative biometric repository for non-U.S. persons. It supports the

[33] *See* FBI-001 National Crime Information Center (NCIC), 64 Fed. Reg. 52343 (September 28, 1999), *available at* https://www.fbi.gov/foia/privacy-act/64-fr-52343.
[34] For more information about the FBI Criminal Justice Information Services, *see* https://www.fbi.gov/services/cjis.
[35] *See* FEDERAL BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR NEXT GENERATION IDENTIFICATION (NGI), *available at* https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments.
[36] *See* A0025-2 PMG (DFBA) DoD - Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/581425/a0025-2-pmg-dfba-DoD/. *See* A0025-2 SAIS DoD - Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009), *available at* https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/569938/a0025-2-sais-DoD/.

storing, matching, and sharing of biometric data collected as part of military operations, including fingerprint, iris, palm, facial images, and biographical information, as well as forensically collected latent fingerprint information. Latent fingerprints can link individuals to criminal activities. Forensic labs collect and process latent fingerprints and upload them to Automated Biometric Identification System for storage and subsequent matching against new biometric submissions.

Department of State, Consular Consolidated Database (CCD)[37] is a system used by consular personnel as a resource for verifying prior visa issuances and refusals. Consular management also uses Consular Consolidated Database for statistical reporting. Consular Consolidated Database also includes photographs captured by CBP during entry inspection, photographs from U.S. passports and U.S. visas, and photographs from other DHS encounters. Case agents/officers may use Consular Consolidated Database information during an investigation related to immigration and identity fraud, immigration status, and international crossing histories.

Law Enforcement Information Exchange (FED-LInX) – LInX is an advanced information sharing system and analytical data warehouse containing information from participating state and local law enforcement agencies located within a regional LInX system. LInX is a joint initiative sponsored by the Naval Criminal Investigative Service (NCIS) of the U.S. Department of the Navy, and various regional and local law enforcement agencies located throughout the nation. Case agents/officers utilize FED-LinX derived information to deconflict with local law enforcement agencies regarding targets of investigation.

Department of Treasury, Financial Crimes Enforcement Network (FinCEN)[38] - Pursuant to the USA Patriot Act of 2001, the Financial Crimes Enforcement Network was tasked with developing a highly secure network to allow filing institutions to electronically file certain Bank Secrecy Act forms (reports). The Bank Secrecy Act E-Filing system portal provides the electronic filing capability to financial institutions for meeting their Bank Secrecy Act reporting responsibilities and makes the information available to law enforcement. Most of the information in the system is data obtained from the individual and not from federal, state, tribal, and local agencies. Case agents/officers utilize Financial Crimes Enforcement Network information to further elucidate financial crimes and money laundering conspiracies derivative of specified unlawful activities. Additionally, suspicious activity reports, currency transaction reports, and other Bank Secrecy Act related data may be relevant to ongoing criminal investigations germane to the CBP mission.

2.3 Does the project use information from commercial sources or

[37] U.S. passport and visa photos are available via the Department of State's Consular Consolidated System. *See* U.S. Department of State, Privacy Impact Assessment for the Consular Consolidated Database (December 2008), *available at* https://2001-2009.state.gov/documents/organization/93772.pdf. Other photos may include those from DHS apprehensions or enforcement actions, previous border crossings, and immigration records.
[38] See *supra* note 10.

publicly available data? If so, explain why and how this information is used.

Yes. CBP case agents/officers may collect, use, and maintain in CCMS commercially available data and open-source information; however, users may not query commercial or public sources from within CCMS, and the system does not ingest data directly from these sources. Some users have access to commercial or public sources as part of their official duties and may manually incorporate this information into reports and/or Subject Records contained in CCMS if the case agent/officer determines that the information is relevant to an investigation. Such incorporation is at the discretion of the case agent/officer and is not the result of an automated collection process. In some instances, a screenshot of information from online sources may be captured and uploaded to the case file.[39] Per CBP policy and directives, CCMS users may directly or indirectly (via a commercial data provider) access publicly available information, including social media websites, during investigations and incorporate information directly relevant to an investigation into CCMS.

CBP personnel also may use data from commercial sources and publicly available data to verify information contained in CCMS; for example, to verify a subject's former and current place of residence or to identify personal property owned by the subject. Further, commercial or publicly available data may be used to enhance existing case information, such as providing additional identifying details such as date of birth, or public records including but not limited to criminal history records, for example.

2.4 Discuss how accuracy of the data is ensured.

CCMS built-in deconfliction processes help to connect investigative efforts. They also help to ensure data quality by identifying and resolving potentially conflicting information among investigations, and by ensuring that the system maintains the most complete information available to CBP on a particular subject of interest.

Prior to creating a new case or Subject Record in CCMS, users are required to query the system to determine if a case or Subject Record already exists. If a case file or Subject Record does not already exist, users may create a new record. If there is an existing case file or Subject Record, the system will provide the user with the name and contact information for the owning Case agent/officer, enabling the two to consult to determine whether to open a related case under the existing investigation or open a completely unique investigation. This deconfliction process ensures that the two case agents/officers do not have two concurrent cases on the same subject or organization for the same suspected criminal activity. If there is an existing Subject Record, the user is only able to create sub-records and link the information to the master case file to their own

[39] CBP operates in accordance with established DHS and CBP policies pertaining to the use of publicly available and social media information. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY FOR OPERATIONAL USE OF SOCIAL MEDIA DIRECTIVE 110-01, *available at* https://www.dhs.gov/privacy-policy-guidance.

cases, Subject Records, and/or case documents. CCMS also alerts record owners each time another user queries or views their Subject Records. This helps to ensure consistency and identity resolution in the information that CBP maintains about its investigative targets and related investigations.

Cases involving the same person or organization subject to multiple investigations may be combined, resulting in all information pertaining to a given subject being linked, documented, and displayed in one case. For instance, if an individual is suspected of both drug and human smuggling, that individual's records may be combined into one case charging multiple violations of law. Deciding to combine one or more cases is done on a case-by-case basis and ultimately decided by all involved stakeholders, include CBP agents/officers and prosecuting attorneys.

To ensure the integrity of an investigation, CBP policy requires CCMS users to take necessary steps to ensure that data entered into the system meets the highest possible data quality standards and to correct inaccurate data. This also serves to promote individual privacy interests by potentially exculpating individuals who are not involved in criminal activity. During each step of the investigation, CBP case agents/officers compare new information with information already in the system and external investigative case files before entering additional information into the CCMS record. This comparison process helps to ensure accuracy and deconflict inaccurate information before recording inaccurate information in the CBP system of record. Users are required to import certain types of Subject Records by importing those records from other CBP systems of record and only after verifying the accuracy of the data (i.e., Seized Assets and Case Tracking System for Subject Records pertaining to seized assets and e3 and TECS for Person Subject Records). This process ensures data quality both within CCMS and across connected CBP systems.

Additionally, CCMS allows users to regulate each other's data quality. For example, if two users have identified the same individual in Person Subject Record, CCMS allows users to compare the information and resolve discrepancies to ensure data accuracy.

Case agents/officers may also upload original source information from hard copy investigative case files. Hard copy files, which contain proper data classification markings, are maintained in locked cabinets in a secured building with access limited to those who have a need to know. As exists currently with TECS, hard copy case files contain, in part, printouts of electronic information (e.g., Reports of Investigation, Subject Records, arrest/seizure reports) also maintained in an electronic system. These hard copy files also may contain information derived from other sources including court documents, reports from other agencies, investigative notes, and other documents that are not maintained in an electronic system. Thus, case information may be checked against the original source data to ensure accuracy. CCMS allows record owners to modify their own Subject Records to correct inaccurate data.

Lastly, CBP policy requires that Subject Records and case documents must be reviewed and approved by a supervisor prior to being available for use in an investigation, and controls to implement this policy are built into the CCMS system. For example, Reports of Investigation created by case agents/officers are initially created as drafts; the draft must be approved by a supervisor before it is considered final and available for viewing by other CCMS users. In contrast, Subject Records created by case agents/officers are immediately viewable to other case agents/officers because of the need to deconflict, though these records are flagged to indicate the information in the records is pending/not final until a supervisor reviews and approves them.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information in CCMS will not be accurate, complete, or timely.

Mitigation: This risk is partially mitigated. While law enforcement investigatory files may include information that is eventually determined to be irrelevant to the prosecution of the criminal case, information must have probative value at the time that it is collected. It may be the case in investigations that information considered probative at one point in time may later be determined to be irrelevant to a case. However, it is also possible that information considered probative in a case may ultimately be exculpatory in either the immediate case or a linked case. Supervisory review and oversight help to ensure that the data maintained in the system is directly relevant to an investigation at the time of collection.

Additionally, and for purposes of deconfliction, all new and updated records are flagged as preliminary until a supervisor approves their addition to the case file. In addition, case agents/officers are required to verify data prior to submitting records for approval, and to contact other case agent/officers to resolve any discrepancies identified when viewing other CCMS records. Data in the system may be checked against original source systems/original sources, including hard copy investigative case files, to ensure accuracy. With respect to commercially available and open-source data, CBP users must validate all commercial or open-source data against authoritative sources, such as other federal records, before considering that information to be credible and retainable.

Privacy Risk: There is a risk that CBP's surveillance activities, such as license plate reader and video technology, may result in an overcollection of information that is stored in CCMS and is not related to a law enforcement violation.

Mitigation: This risk is mitigated. While additional data that may not be relevant to an investigation may initially be captured because of authorized surveillance activities, CBP law enforcement personnel may only extract and load into CCMS data that is relevant to an investigation and adds probative value to the case. In accordance with CBP evidence handling

policies, CBP maintains copies of video footage and audio recordings in the CBP system of record.[40] License plate reader data is obtained from CBP-owned and operated license plate reader technology, or from other law enforcement agencies, in support of investigative and border enforcement related activities. Any images or videos that are not related to a particular investigation are not placed in CCMS.

Privacy Risk: There is a risk that CBP may create Subject Records on individuals who are not a target of an investigation.

Mitigation: This risk is partially mitigated. Case agents/officers are trained on the proper use of the system and how/when to create Subject Records (i.e., only on individuals who are a target of an investigation). Supervisors must review and approve Subject Records and Reports of Investigation, which helps to ensure that Subject Records are only created on individuals who are a target of an investigation. When updating or changing a Subject Record, the case agent/officer will annotate the comments section the reason for the correction (i.e., former target of investigation later determined to be victim or identity theft).

Case agents/officers can also unlink one Subject Record from another. For example, the Subject Record of a witness initially thought to be a criminal associate of a target and linked to the Subject Record of that target may be unlinked so the witness's record no longer appears in search results for the subject.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Case agents/officers use CCMS to document and inform CBP criminal investigative activities and in support of any criminal prosecution which may arise from these investigative activities. Case agents/officers use Subject Records and supportive files, including a Report of Investigation and incident reports, to document investigative information, draw connections between subjects and cases, and inform future criminal case activities. These records and files use the following information in the following ways:

- *Biographic data* in Subject Records is used for case and identity deconfliction.
- *Identity deconfliction* is done to ensure one individual does not have two Subject Records. Incident reports, including arrest and seizure records, as well as case files containing photographs or copies of evidence, help CBP maintain organized and complete investigative files. These reports, records, and other case files are used to

[40] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR CBP LICENSE PLATE READER TECHNOLOGY, DHS/CBP/PIA-049 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

support resulting criminal prosecutions by the U.S. Department of Justice, state, or local prosecutors.

- *Information obtained from electronic device search:* CBP uses the digital forensic data obtained from electronic devices in support of its investigative activities. This information may be included in Subject Records, Reports of Investigation, and/or linked to a case. The data is used primarily to identify connections between subjects and criminal associates in support of a criminal investigation.
- *Location tracking and License Plate Reader data:* Location tracking data and License Plate Reader data are also used in support of CBP's criminal investigative activities. Relevant data is included in Subject Records and Reports of Investigation and, in the case of pictures or other external documents, may be uploaded to case files. It may be used to track patterns of movement, indicate the location of a target at a specific time, and inform immediate action as needed.
- *External Law Enforcement Agencies* may use case data in support of their investigations and/or agency missions, as described more fully in Section 6.0. CBP may disclose information to appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where CBP determines that the information would assist in the enforcement of civil or criminal laws.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, CCMS does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No other DHS Components have assigned roles or responsibilities within CCMS. However, to the extent external users are participating on a Task Force and assigned to CBP (with CBP credentials), they may be given access to CCMA in support of a CBP investigation. Any Task Force Officer must also have access to TECS and the Automated Targeting System consistent with their onboarding policies and procedures.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk of unauthorized access to CCMS, or inappropriate use or disclosure of information maintained in the system.

Mitigation: This risk is mitigated. CBP requires user training, access controls, and oversight and information security controls to ensure only individuals who are authorized to access CCMS do so and to ensure appropriate use and disclosure of information maintained in CCMS.

All CCMS users are required to complete DHS security and privacy training annually. In addition to this training, users must complete system-specific training before they gain access to the system. CCMS grants users role-based permissions for different levels of system access, and all users must complete role-based system training. Roles are defined by job position (i.e., supervisor, case agent/officer, case analyst) and duty location, and users are granted the lowest level of privileges necessary to perform their job-related responsibilities.

To access and use data from other CBP systems of record connected to CCMS (e.g., e3, TECS, Seized Assets and Case Tracking System), users must also have access to that system. This is generally managed through the Automated Targeting System entitlement provisioning process.

For external systems, such as National Crime Information Center (NCIC),[41] users are required to have National Crime Information Center certification before they may access the National Crime Information Center data (i.e., criminal history, wants/warrants). National Crime Information Center Certification is required to demonstrate that the user understands the special rules for handling National Crime Information Center information. If a user's National Crime Information Center certification has expired, the user may still access CCMS but will not be able to run National Crime Information Center queries until their National Crime Information Center certification is complete.

When determined appropriate by the case record owner and their supervisor, the case agent/officer may limit access to that information, with the caveat that a case agent/officer may not limit their supervisor's access to the information.

To ensure oversight and information security, CCMS has robust auditing features to help identify and support accountability for user misconduct. The audit logs capture user activity including, but not limited to, uploading records or data, extracting information from the system, resolving Entities, conducting searches, and viewing records. If warranted, the CBP Office of Professional Responsibility will access system audit logs and take disciplinary action against any user who violates CBP policies and DHS rules of behavior.

CCMS users will receive an email and a notification message in their notification queue

[41] The National Crime Information Center is a Department of Justice, criminal records database which allows other law enforcement agencies to enter or search for information about stolen property, missing or wanted persons, and domestic violence protection orders; to obtain criminal histories; and to access the National Sex Offender Registry.

when another user has queried their Subject records, documents, and/or case. This allows users to monitor when other users access their records, including Reports of Investigation and Subject Records, and inquire as to why another user has conducted a particular query or viewed a record. This may reveal misconduct on the part of users who may be inappropriately browsing the system, but also serves as a deterrent as users know it is likely inappropriate activity that will be challenged or reported. Query notifications may also reduce duplication of effort. Users are trained to report suspected misuse of CCMS to management and/or file a report directly with the Office of Professional Responsibility.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The publication of this Privacy Impact Assessment provides notice of the existence, content, and uses of CCMS. In addition, notice of CBP's investigative authorities can be found in the following published CBP System of Records Notices:

- DHS/CBP-024 Intelligence Records System (CIRS)[42]
- DHS/CBP-006 Automated Targeting System[43]
- DHS/CBP-023 Border Patrol Enforcement Records (BPER)[44]
- DHS/CBP-013 Seized Assets and Case Tracking System[45]
- DHS/CBP-011 U.S. Customs and Border Protection TECS[46]

Because CCMS is a law enforcement system that collects and maintains sensitive information related to criminal investigations, it is not feasible or advisable to provide notice to individuals at the time their information is entered into the system. When CBP agents/officers interact with individuals in connection with an investigation, those individuals are generally aware that their information will be recorded in a CBP system of record.

---

[42] *See* DHS/CBP-024 Intelligence Records System (CIRS) System of Records, 85 Fed. Reg. 80806 (December 14, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[43] *See* DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[44] *See* DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.
[45] *See* DHS/CBP-013 Seized Assets and Case Tracking System, 73 Fed. Reg. 77764 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[46] *See* DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 Fed. Reg. 77778 (December 19, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.

CBP agents/officers collect biographical information during processing and encounters with individuals. In addition, information is frequently collected through other lawful means, such as by subpoenas and search warrants. If information is obtained from individuals through federal government-approved forms or other means, such as information collected pursuant to seizures of property, notices on the relevant forms generally state that the information may be shared with other law enforcement entities.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Due to the law enforcement purposes for which the information is collected and used, opportunities to decline or opt out of collection are limited. CCMS users enter data during an authorized law enforcement investigation. The only means by which the individual may withhold consent to any particular use of information is by refusing to provide the information. Furthermore, there is a potential risk that could arise if an individual is notified that information is being collected about them by CBP for a law enforcement or intelligence purpose. The notification may cause the individual to flee or destroy or conceal evidence required by CBP, compromising the ability of DHS agencies to perform their missions, and could put DHS personnel and resources at risk of injury, death, loss, or destruction. In such cases, CBP will intentionally withhold notification to the individual until they arrested or indicted.

All persons are provided general notice through this Privacy Impact Assessment and the Privacy Impact Assessments and System of Records Notices referenced within this document.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be aware their information may be maintained in CCMS or understand how CBP uses their information.

Mitigation: This risk is partially mitigated. Individuals who are questioned directly by CBP personnel have notice by virtue of the encounter itself that CBP is collecting information. Although there is a potential risk that a language barrier may cause communication issues when CBP encounters an individual, attempts are normally made to communicate with individuals in their native language or through an interpreter. In addition, the United States has agreements with some nations that require notification to the foreign government's consular office when a national of that country has been arrested, and in other cases the individual always has the right to request consular notification and assistance. The engagement of consular officials may assist individuals from other nations in understanding the criminal proceedings against them, obtaining legal counsel, and obtaining other resources.

There is a countervailing risk that may arise if individuals under criminal investigation are notified that information is being collected about them by CBP for law enforcement purposes.

Such notification may compromise an investigation, especially if the individual decides to flee, alter patterns of life, modify illicit techniques used to carry out the ongoing criminal conspiracy, or destroy or conceal evidence because of this notice for example. This risk could directly affect the ability of CBP to perform its mission. Furthermore, release of such information could pose officer safety issues for CBP and other DHS law enforcement personnel. In such cases, CBP may intentionally withhold notification to the individual until they are arrested or indicted.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

All CCMS records will be treated as permanent records until a records retention schedule is approved by National Archives and Records Administration (NARA). CBP expects to retain investigative information that does not result in an individual's arrest, detention, or removal, for twenty (20) years after the investigation is closed, consistent with the N1-563-08-4-2; user account management records for ten (10) years following an individual's separation of employment from federal service; statistical records for ten (10) years; and audit files for fifteen (15) years. Per the Border Patrol Enforcement Records and TECS System of Records Notices, records of arrests, detentions, and removals are retained in the original CBP system of record for seventy-five (75) years.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information in CCMS will be retained for longer than is needed to accomplish the purpose for which the information was originally collected.

Mitigation: This risk is partially mitigated. CBP is developing and finalizing a retention schedule for CCMS. The retention schedule must balance the need to retain information that may be of probative value to an investigation, as well as records that may be exculpatory in nature, with the records retention policies of the Agency.

The proposed 20-year retention period for CCMS is consistent with the retention schedules for other investigative records within DHS. The 20-year period provides reasonable assurance that the records of individuals who may be encountered multiple times over a prolonged period of time will be linked. This retention period will assist CBP in effectively enforcing U.S. criminal and immigration laws by ensuring that information pertaining to individuals who are encountered repeatedly over a span of time can be linked. Further, closed cases may contain information that may be relevant to a new or existing case and need to be readily searchable and accessible to ensure that information of probative or exculpatory value is available to case agents/officers.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal

agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

CBP may disclose information maintained in CCMS with appropriate federal, state, local, tribal, and foreign government agencies, or multi-lateral governmental organizations responsible for investigating or prosecuting violations of law or to support the enforcement of border security and immigration laws. All external disclosures are made consistent with the provisions of the Privacy Act (5 U.S.C. § 552a) and the published routine uses listed in the System of Records Notices (listed in Section 1.2).

In addition to federal, state, tribal, local, and foreign law enforcement agencies, CCMS information may be shared with relevant law enforcement fusion centers and international organizations such as INTERPOL. All external sharing of CCMS information will be documented in the appropriate case file using applicable disclosure procedures per DHS and CBP policy and applicable statute. This sharing is done manually by the case agent/officer only, and not via system-to-system connections.

Consistent with the above listed System of Records Notices, CBP may also disclose limited information to the extent necessary to obtain information from third parties such as witnesses or recipients of subpoenas. Information is only disclosed in these situations where the case agent/officer conducting the investigation believes that the parties to whom they are making the disclosure have information relevant to the investigation. CBP personnel may disclose only the information necessary to receive the information they need while performing their official duties.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

All external disclosures to federal, state, local, foreign, and private entities of information maintained in CCMS and other CBP systems of record will be in strict compliance with the routines uses of the respective System of Record Notices in Section 1.2.

The published routine uses in applicable System of Record Notices enable CBP to disclose information within CCMS as necessary to effectuate prosecutions with the Department of Justice and coordinate other open investigations with other law enforcement partners. Published routine uses allow CBP to share information with the Department of Justice, including Offices of United States Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body.

Published routine uses also permit CBP to share information with appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information,

indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

6.3 Does the project place limitations on re-dissemination?

Yes. Prior to each sharing of information with a federal, state, or local agency, a Memorandum of Understanding or other written authorization places limitation on the use and re-dissemination of the information. Federal agencies that receive CCMS information are subject to the Privacy Act of 1974 and, as such, may not re-disclose information without clear authority to do so.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures outside of DHS must be accounted for in a paper or electronic record which includes the date, nature, purpose of each disclosure, and the name and address of the individual agency to which disclosure is made. All users are required to complete and retain DHS Form 191, Privacy Act Disclosure Record, when making an external disclosure. Currently, users complete an electronic form and maintain it in their hard copy case files. In the future, users will be able to complete this form electronically from within the system and store it in the case file.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that CCMS data will be inappropriately shared with external parties, and that external sharing will not be properly recorded as required by the Privacy Act of 1974 and DHS and CBP policy.

Mitigation: This risk is mitigated. CCMS data may be manually shared with other law enforcement agencies outside of CBP in accordance with formalized agreements (e.g., a Memorandum of Understanding) or pursuant to *ad hoc* requests that conform with the requirements the Privacy Act of 1974. Formalized agreements must be reviewed and approved by various oversight offices, including the CBP Privacy Office. This helps to ensure the sharing is supported by legal authorities and consistent with the purposes for which the information was collected.

Users are required by law and policy to share information with only those external partners who have a demonstrated law enforcement, intelligence, or national security need to know, and consistent with published Routine Uses in a System of Records Notice and in coordination with third agencies, as appropriate. Prior to sharing information with an external partner, the case agent/officer is required to complete DHS Form 191, Privacy Act Disclosure Record, to document the external disclosure. Further, CBP personnel are trained on the appropriate sharing of personally identifiable information and are required to contact the CBP Privacy Office if they are not certain whether information sharing is appropriate.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Procedures for individuals to request access to their information, which may be maintained in CCMS or in another CBP system of record, are identified in the cited System of Record Notices. Requests for access to information may be made to CBP's Freedom of Information Act Office online at https://www.dhs.gov/foia-contact-information or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229

When seeking records from CCMS or any other CBP system of records, the request must conform to Part 5, Title 6 of the Code of Federal Regulations. An individual must provide their full name, current address, and date and place of birth. They must also provide:

- An explanation of why the individual believes DHS would have information on them;
- Details outlining when they believe the records would have been created;
- And if the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying their agreement for access to their records.

The request must include a notarized signature or be submitted pursuant to 28 U.S.C. § 1746, which permits statements to be made under penalty of perjury as a substitute for notarization. Without this information, CBP may not be able to conduct an effective search and the request may be denied due to lack of specificity or lack of compliance with applicable regulations. Although CBP does not require a specific form, guidance for filing a request for information is available on the DHS website at http://www.dhs.gov/file-privacy-act-request and at http://www.dhs.gov/file-foia-overview.

All or some of the requested information may be exempt from access pursuant to the Privacy Act to prevent harm to law enforcement investigations or other interests as permitted by law.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking to correct records contained in a system of records, or seeking to

contest their content, may submit a request in writing to CBP's Freedom of Information Act Office via Freedom of Information Act online at https://www.dhs.gov/foia-contact-information or by mailing a request to:

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229

Once an individual has a copy of their records as provided under FOIA, individuals seeking to correct or amend inaccurate or erroneous information maintained in a CBP system of records may contact the CBP Privacy Office directly at privacy.cbp@cbp.dhs.gov.

7.3 How does the project notify individuals about the procedures for correcting their information?

CBP provides general notice on its public-facing website about the procedures for submitting Freedom of Information and Privacy Act requests. However, CCMS contains investigatory material compiled for law enforcement purposes and is generally exempt from the access, correction, and amendment provisions of the Privacy Act. Notification to individuals that they are or have been the target of a law enforcement investigation could undermine the law enforcement mission of CBP.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will be unable to participate meaningfully in the use of their data as maintained in CCMS, or determine whether CCMS maintains records about them.

Mitigation: This risk cannot be fully mitigated. Because CCMS contains data maintained for a law enforcement purpose, individuals' rights to be notified of the existence or non-existence of data about them, and to direct how that data may be used by CBP, are limited. Notification to affected individuals could compromise the existence of ongoing law enforcement activities and alert individuals to previously unknown investigations of criminal or otherwise illegal activity. This could cause individuals to alter their behavior in such a way that certain investigative tools, such as wiretaps or surveillance, will no longer be useful.

Permitting individuals to direct the agency's use of their information could similarly interfere with the intended law enforcement use of the system. Nevertheless, the publication of this Privacy Impact Assessment and associated System of Records Notices provides general notice about CBP's collection and uses of criminal investigation information.

In addition, in exempting records maintained in CCMS from access, correction, and

amendment under the Privacy Act, CBP has indicated that the exemptions will be applied on a case-by-case basis at the time of the access, correction, or amendment request. In appropriate circumstances, therefore, individuals may have an opportunity to access or correct their records, consistent with law enforcement necessity.

Further, to the extent a case moves forward for prosecution, individuals have various opportunities to contest the information as part of the criminal proceedings that may result from the information.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Through access controls, notification of queries, auditing, and supervisor review, CBP ensures that CCMS is used in accordance with the practices stated in this Privacy Impact Assessment. Based on strict role-based access controls, CBP prevents unauthorized access to information within CCMS as defined by users' need to know and job responsibilities. Access to CCMS is controlled by an Entitlement Role for database access as well as Application Role for application access, granted via the Provisioning Application. Data within CCMS is compartmentalized by the user's Field Office/Sector/Branch to include the user's Port/Unit. Users may only view data to which they are provisioned or granted access to a criminal case file outside their respective Field Office/Sector/Branch for collaborative investigative efforts by another user. In addition, the case agent/officer who creates record in CCMS may limit the access by others to that information, except for the agent/officer's supervisor. Users are required to complete system-specific, role-based training before being granted an account.

CCMS users receive a notification whenever another user has viewed a document of theirs in the system. If a case agent/officer suspects or has reason to believe their records have been misused, the user can report the suspected misconduct to their Supervisor and the Office of Professional Responsibility for further investigation.

In addition to access controls and notification of queries, there is a set of auditing requirements that are tracked and saved in audit logs for viewing later by the Office of Professional Responsibility if allegations of misuse are made against a user. CCMS keeps copies of audit and log file data in a separate data repository for 15 years to ensure CBP may track and investigate misconduct and misuse of the system. Misuse of the system may subject a user to criminal and civil penalties, as well as discipline in accordance with the CBP Table of Offenses and Penalties, up to and including removal.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All CBP personnel must complete annual privacy and security training and review and sign the DHS Rules of Behavior. In addition, CBP personnel take specific CCMS training as part of an introduction to the system, which explains the system structure, information retention, user permissions, and user roles. Specific to CCMS, to ensure data accuracy all users are required to undergo training in the use of the system before they are granted access. Once access to CCMS has been granted, users have ongoing access to a training environment that replicates the functionality of the system using "dummy" data.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

CCMS uses Single Sign-On (SSO) to validate CBP users with using CBP issued Personal Identity Verification (PIV) card[47] and assigned HASH ID. Single Sign-On is a method of access control that enables a user to log in at a single point and gain access to the resources of multiple software systems by using credentials stored on shared, centralized authentication servers. Personal Identity Verification card authentication provides an extra layer of security by storing a user's credential on a physical card that must be present at login. Users are given role-based permissions, and each user has an individual "desktop" in the application with the top-level view presenting links to all of the case files for that user's assigned cases.

A system administrator establishes user accounts and updates user role-based permissions, as needed. Access roles are assigned based on the user's job responsibilities and implemented by a system administrator. Only CBP personnel whose official duties necessitate access to CCMS covered by this Privacy Impact Assessment will be granted access to the system. In addition, CBP supervisors oversee and approve the assignment of user accounts to CBP personnel. Access roles are reviewed regularly to ensure that users have the appropriate level of access. Individuals who no longer require access are removed from the access list.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All new information sharing agreements, to the extent required, will be reviewed by the CBP Privacy Office, the Office of Chief Counsel, all key stakeholders, and the CCMS Program Manager. Each CBP Memoranda of Understanding (MOU) will clearly articulate who will be accessing the shared information and how it will be used. Any change to the terms of an existing

[47] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE PERSONAL IDENTITY VERIFICATION/IDENTITY MANAGEMENT SYSTEM (PIV/IDMS), DHS/ALL/PIA-014 (2006 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

Memoranda of Understanding will be reviewed in the same manner as described above.

Contact Official

Benjamin M. Blanchard
Assistant Chief
United States Border Patrol
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
Privacy Officer
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection
privacy.cbp@cbp.dhs.gov

Approval Signature

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

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
privacy@hq.dhs.gov