Privacy Impact Assessment

for the

Intelligent Computer Assisted Detection (ICAD) System

DHS Reference No. DHS/CBP/PIA-075

Date November 3, 2022

Homeland Security

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) operates the Intelligent Computer Assisted Detection (ICAD) system to provide situational awareness along the United States border. The ICAD system assists the United States Border Patrol (USBP) in detecting, identifying, and apprehending individuals who may have illegally entered the United States or otherwise violated applicable U.S. laws between ports of entry (POE). CBP provided notice to members of the public about ICAD in the Border Surveillance Systems (BSS)[1] Privacy Impact Assessment (PIA) but is publishing this new PIA to provide transparency about the system's application and functionality.

Overview

CBP uses sensors, cameras, and other technologies along the U.S. border to detect and identify individuals who may be attempting to enter the United States between POE, or to evade detection while, for example, moving narcotics or other contraband into the country. CBP's Intelligent Computer Assisted Detection (ICAD) system serves as the central application for receiving and displaying alerts generated by unattended ground sensors (UGS)[2] and other surveillance technologies. ICAD has been operational since 1998 at all twenty U.S. Border Patrol (USBP) sector communication centers. The privacy risks and mitigations associated with ICAD were previously discussed in the BSS PIA. ICAD's functionality includes the ability for an ICAD user to monitor sensors, manage surveillance assets, log tips received by members of the public, search ICAD images, and review sensor and dispatch activity along the U.S. border. Many sensors that communicate with ICAD include an image of the detected ICAD event, images are reviewed by CBP personnel to determine the nature of the detected event. For example, a cow could trigger a trail camera that will send an image to ICAD where CBP personnel will determine that there is no potentially illicit activity occurring. CBP can search ICAD images by date, time, and location to locate an image that may contain evidence of unlawful activity. ICAD does not apply facial recognition technology to images captured by ICAD sensors.

Sensors and Cameras

ICAD system receives alerts from a network of CBP and partner-owned[3] sensors and

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

[2] Unattended Ground Sensors include seismic, acoustic, magnetic, and day/night cameras that are used to automatically detect persons or vehicles and transmit activity reports or images via radio frequency, microwave, cellular or satellite communications to the ICAD application suite.

[3] State organizations deploy sensors in their respective Areas of Operation and although CBP is not responsible for the deployment and maintenance of these devices, ICAD is configured to receive alerts from these sensors.

cameras[4] installed along the U.S. border that detect intrusion activity between ports of entry (POE). CBP uses unattended ground sensors (UGS), such as seismic sensors, in areas where movement along or near the United States border is indicative of illicit activity (e.g., areas known to be used for illicit activity based on law enforcement intelligence or prior law enforcement actions). CBP also uses cameras that are triggered by movement or can identify and categorize movement. Cameras that can identify and categorize movement use algorithms to determine if an object is, for example, an animal or a person. Sensors and cameras relay suspicious activities to a receiver/decoder located at the USBP Sector Headquarters closest to the sensor. Some sensors use a cellular network and email sensor traffic while other sensors use microwave transmitters or even cloud services to deliver information about sensor activations. ICAD, located at each United States Border Patrol (USBP) Sector Headquarters interpret sensor information and display the data on ICAD workstations installed at USBP Stations and connected to the CBP network. USBP agents and CBP Communication Assistants review the information on the ICAD workstations. If CBP personnel determine that the alerts are potentially indicative of illicit activity, they will notify on-duty USBP agent(s) of the alerts who will go investigate the area.

In addition, ICAD sensors include rescue beacons.[5] These rescue beacons are deployed along the border, between ports of entry (POE) and in remote areas north of the border. An individual in distress, or witnesses with knowledge of an individual(s) in distress, may use the rescue beacon to request help. Rescue beacons are manually triggered unattended ground sensors (UGS) and identified as Rescue Beacons to ICAD users. Optionally, rescue beacons can be accompanied by cameras sensors. ICAD displays and stores the sensor activity and images.

Specifically, the Texas Department of Public Safety (TDPS) has a program known as "Drawbridge." Using federal funds, TDPS installed trail cameras along the Texas / Mexico border. TDPS shares the Drawbridge images with ICAD, so that CBP personnel may view the images.

[4] *See* Supra 1.

[5] *See* forthcoming Missing Migrant Program PIA for additional information CBP's use of rescue beacons, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

Image: USBP Rescue Beacon

ICAD automatically records the date, time, and location of the sensor activity. In addition, United States Border Patrol (USBP) agents may record details of their investigation of the sensor alarm. USBP agents or Communication Assistants on behalf of the USBP agent can add comments about the alert, which may include the name, date of birth, document identification number, license plate number, and other biographic data about individual(s) encountered when responding to an ICAD alert. The fields for comment are unstructured and used as a notetaking area for the USBP agent to reference later. These fields are not searchable in ICAD.

ICAD also hosts the Tracking, Sign Cutting & Modeling (TSM) application, a web-based application that stores information regarding USBP agent tracking efforts, sensor activations, reports from members of the public related to border crossings, as well as Small Unmanned Aircraft System (sUAS)[6] interdiction activity. TSM users can view individual tracking events and retrieve the particulars of an event including, the time, location information, the identity of the USBP agent(s) involved, event type, assets utilized during the tracking event, as well as information related to seizures and vehicles with any associated pictures, and any attachments

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE AIRCRAFT SYSTEMS, DHS/CBP/PIA-018 (2013 and subsequent update), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

(e.g., notes). TSM information is also available in Team Awareness Kit (TAK)[7] for use by USBP Agents in the field. Using the TAK mobile application, USBP agents can expeditiously update ICAD sensor activations with additional information, such as found animal tracks or signs of illicit intrusion. These updates are retained in the ICAD database.

In addition, to avoid redundant data entry and allow for faster data collection in TSM, some Border Surveillance Systems have the capability to create and edit TSM Events directly from their platform's user interface.

When an ICAD sensor sends an alert to the ICAD dispatch screen, the responsible USBP Communication Assistants relays the sensor alert details, via radio or TAK, including the description of any images or video captured by the sensors and cameras, to the USBP agent(s) operating near the sensor. When a USBP agent responds to an ICAD sensor alert, the alert information is updated, another TSM tracking event is added to the TSM application, and another dot is created on the eGIS[8] map. Each sensor alert and TSM sub-event documents the chain of detection events attributable to the suspected intrusion event and can be viewed on a map within TSM.

If a USBP agent apprehends an individual(s) suspected of illegally entering the U.S. or otherwise violating applicable U.S. law between ports of entry, the USBP agent(s) involved in the encounter will notify USBP Station personnel that the individual(s) has been apprehended and the alert in ICAD/TSM is updated to include the new status of "apprehended". In addition, USBP Station personnel will create a final TSM tracking event to record the apprehension location. Lastly, USBP Station personnel create an e3[9] apprehension record directly from TSM. e3 is the system of record for any PII associated with apprehended individuals during processing and includes information such as name, date of birth, date, time, GPS location, and number of individuals apprehended.

Citizen Report

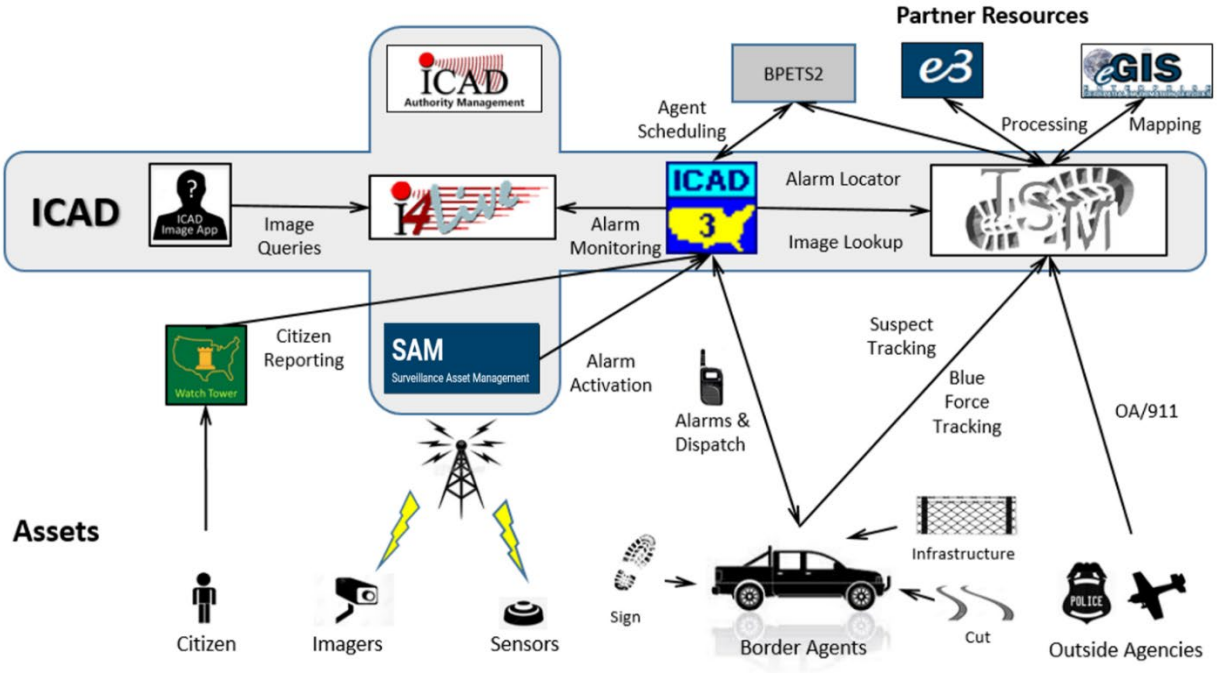
CBP also uses ICAD to log tips received from the public regarding potential unlawful entries or other suspected violations of law between ports of entry. CBP personnel, including

[7] TAK, a cost-effective, government off-the-shelf solution developed by the Department of Defense, enables tactical data to be generated, visualized, and shared, facilitating communication across multiple users to achieve shared tactical awareness. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE TEAM AWARENESS KIT (TAK), DHS-ALL-PIA-090 (2021), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE ENTERPRISE GEOSPATIAL INFORMATION SERVICES, DHS-CBP-PIA-041 (2017 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

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

USBP agents, duty officers, camera operators, intelligence agents, and other field staff may use the ICAD Citizen Report, a web-based form, to enter tips received from members of the public. For example, a citizen may contact USBP to report seeing an individual(s) cross the border between ports of entry. Communication Assistants at the USBP Station may enter the information into ICAD, creating an alert and begin tracking the event in TSM application. The Citizen's Report web-based form is not publicly available and is only available to CBP employees via the DHS One Network (DHS OneNet).[10] USBP uses the report to capture and report all Citizen's Report information nation-wide. When completed, the report is processed by ICAD like other sensor alarms and USBP agents may respond to the area to investigate the report.



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?

CBP collects the information maintained in ICAD in accordance with 6 U.S.C. §§ 202,

[10] DHS One Network (OneNet) is the secure IP intranet that facilitates IP and wireless convergence, making it possible for all DHS components to share data. OneNet provides a range of services, including network portals, managed network services, and Internet access and remote access for all components in DHS. OneNet further supports communication and interaction among the many DHS organizational entities, as well as external to DHS.

212; 8 U.S.C. §§ 1103, 1225, 1324, 1357, 1360, 1365a, 1365b, 19 U.S.C. §§ 2071, 1581-1583 and 1461. CBP uses ICAD to perform its law enforcement missions under the Homeland Security Act of 2002, as amended,[11] including but not limited to 6 U.S.C. § 212; Immigration and Nationality Act of 1952, as amended,[12] including but not limited to 8 U.S.C. §§ 1225, 1324, 1325, and 1357; and pertinent provisions of the customs laws and regulations.[13]

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

ICAD sensor alerts are not retrieved using a personal identifier, and therefore, do not constitute a system of records under the Privacy Act of 1974. However, ICAD maintains personally identifiable information (PII) on individuals associated with incidents occurring between along the U.S. border and this information may be retrieved by a personal identifier. SORN coverage for PII found in ICAD is provided by DHS/CBP-023 Border Patrol Enforcement Records, System of Records (BPERS), Oct 20, 2016, 81 FR 72601 and DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792, which provides coverage for CBP's collection of information to provide authorized individuals with access to DHS information technology resources. BPERS permits CBP to collect information related to sensor and camera alerts, as well as enter information collected during a citizen report.

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

ICAD is categorized as a major system in the CBP system inventory. The current Authority to Operate expires on September 17, 2022. A system security plan is in place.

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

USBP is currently working with the CBP Records Office to establish an approved NARA schedule for ICAD records retention.

[11] *See* 6 U.S.C. § 101, *et seq.*
[12] *See* 8 U.S.C. § 1101, *et seq.*
[13] *See*, *e.g.*, 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, and 1595a(d).

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.

ICAD does not collect information covered by the Paperwork Reduction Act.

Section 2.0 Characterization of the Information

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

ICAD collects information from sensor activations (images, coordinates, date, and time), dispatch information associated with United States Border Patrol (USBP) agent activity, and voluntary reports from members of the public regarding suspicious border activity. If a USBP agent apprehends an individual, the USBP agent may collect PII from that individual and record the information in a data entry template that can be associated with the USBP agent's dispatch record. Once an individual is apprehended, the subsequent record and updates of the individual's biometric and biographic information as well as details related to the apprehension fall under the e3 system of record. ICAD applications do not specifically ask for or require any PII to be collected from the public. However, ICAD has free-form text fields where users could insert PII, such as name and phone number.

Information maintained in ICAD originating from members of the public and/or subjects of an investigation may include, but is not limited to the following:

- Location at the time of the encounter;
- Description (physical characteristics of the individual and location, and of the encounter);
- Vehicle description; and
- License plate number.

Information maintained on ICAD users may include:

- Username;
- Employee IDs (star number, Hash ID);
- Email address;
- Phone number; and
- Location and timestamp (for auditing purposes).

In addition to sensor alerts, ICAD includes information voluntarily reported by members of the public pertaining to suspected illegal border activity. Individuals may anonymously report suspicious activity. All information provided by an individual, including basic contact information, is provided voluntarily to USBP. These citizen reports may include the reporting individual's basic contact information including:

- Name;
- Phone number;
- Address; and
- A description of the reported incident, along with information related to the CBP employee who handled the tip, if applicable.

The fields for caller name, address and phone number are required; however, USBP personnel will input "unknown" if the caller wishes to remain anonymous or does not provide their name. Maintaining the caller's information allows USBP agents to follow up with them for more information and helps to deter false reports; however, this information is not required.

ICAD is also used to track the current location and status of all sensors and surveillance equipment owned by USBP. Tracking, Sign Cutting & Modeling (TSM) tracks manned and unmanned deployments of larger surveillance assets (e.g., Remote Video Surveillance System (RVSS), Integrated Fixed Tower (IFT), etc.); these records may include the name of the USBP agent, the date, time, and location of any activity associated with these deployments.

ICAD may collect incidental, non-attributable images of members of the public if the individual is in view of an image sensor. These images are reviewed by USBP personnel and marked as "No Need," indicating that no further investigation is required and no additional PII is associated with the image.

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

United States Border Patrol (USBP) sensors and border surveillance systems generate information in ICAD, though most of this information is not personally identifiable. In instances this information is PII, it would most likely be images of individuals who come in close proximity to cameras. ICAD also contains information provided voluntarily from individuals who report suspicious activity to CBP. The remainder of the information in ICAD comes from USBP agents responding to alerts. USBP agents obtain information from observations at the scene as well as any individuals they encounter during their response. USBP agents relay this information to Communication Assistants who review and update ICAD information.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ICAD does not use any information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

CBP captures ICAD sensor activation data, as well as manually entered data from users (Communication Assistants or other CBP employee) related to suspicious activity observed by Agents or voluntarily reported from members of the public. CBP trains Communication Assistants and USBP agents to evaluate and ascertain which data is relevant and necessary to accomplish CBP's border security mission. USBP investigates sensor hits and citizen reports to determine if there is illicit activity.

CBP also follows chain of custody procedures to ensure the integrity of the records when records are used as evidence and therefore linked directly to a case or person. Communication Assistants or USBP agents may call back a caller reporting suspicious activity to confirm the details of the data collected by the Citizen's Report.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is the risk that USBP agents and Communication Assistants may enter inaccurate information into ICAD.

Mitigation: This risk is mitigated. The training and interviewing techniques employed by USBP agents and Communication Assistants reduce the risk of inaccurate information being entered into the system. Once data is entered into the system, a trained Communication Assistants or USBP agent reviews the information to ensure its accuracy. The Communication Assistant or USBP agent may follow up with the member of the public making the suspicious activity report to ensure the integrity and accuracy of the data. In addition, a USBP Supervisor reviews all Tracking, Sign Cutting & Modeling (TSM) events to ensure that the sensor alert has been resolved and is no longer displayed as an active tracking event in ICAD. While CBP cannot fully mitigate the accuracy risks surrounding suspicious activity reports sourced from members of the public, USBP agents use all information available to assess whether a report is worth investigation. As with all other leads, USBP agents conduct additional research to determine whether a potential violation of law exists; reports alone are insufficient to justify an enforcement action.

Privacy Risk: There is a risk that ICAD may capture information about individuals or activities that are beyond the scope of CBP's authorities. Sensors may capture information about individuals engaging in lawful activities along the U.S. border. For example, sensors may collect

images of an individual hiking or biking along paths that parallel the border.

Mitigation: This risk is partly mitigated. ICAD sensors are oriented toward the U.S. border and away from communities and places of worship and commerce frequented by local residents, as much as operationally feasible. While ICAD sensors may record lawful activity at or near the U.S. border, CBP does not associate the data from the ICAD sensors with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

CBP primarily uses information obtained from ICAD to enhance comprehensive situational awareness along the U.S. border for border security and national security purposes, and to assist in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating the law. CBP uses ICAD to track the movement of individuals and incidents near the border and dispatch available USBP agents to provide operational support. CBP uses sensor data to detect and interdict persons illegally crossing the border. CBP may share ICAD information with coordinating agencies, such as local, state, tribal law enforcement, to assist in an interdiction or operation, as appropriate and described by the routine uses of the respective SORNs that govern the case file or investigative report (e.g., e3/ENFORCE).[14]

Alarm events populate within a web-based dashboard in near real-time, displaying sensor details and the associated imagery specific to the USBP station responsible for responding to the sensor alert. Authorized ICAD users (access and roles are assigned at the Sector/Station level) may perform individualized searches of ICAD images and alerts up to 30 days old, using numerous filters and search characteristics to differentiate and narrow search results. ICAD users review the ICAD images to determine the nature of the detected event (e.g., person, animal, or vehicle). ICAD users also search for images within ICAD for use as evidence in a legal proceeding. ICAD does not use facial recognition technology. Once a sector/station determines an image rises to a level needing investigation, the sector/station will assign an agent to respond to the alert.

USBP agents can access ICAD as a series of web applications or through the Agent Visualization Platform / Team Awareness (TAK) mobile application installed on CBP-issued handheld devices. Using the TAK mobile application, USBP agents can view ICAD sensor alerts via Enterprise Geospatial Information Services (eGIS).[15] There is a bi-directional communication between the TAK server and ICAD, specifically the Tracking, Sign Cutting & Modeling (TSM) application. TAK users will be able to share photographs to ICAD/TSM.

[14] DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601
[15] *See* Supra 9.

ICAD events are shared extensively with CBP's eGIS system, which stores the data locally and displays it as an eGIS[16] map layer in the application. For example, ICAD sensor alerts and TSM tracking events are displayed on an eGIS map layer, providing increased situational awareness; better allocation of resources (including assets and personnel) and expeditious sharing of information between USBP agents.

All ICAD data can be viewed, exported, or printed in report form. Dispatch data is not shared with systems outside of ICAD, however dispatched data is shared between ICAD applications.

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.

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

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that CBP may incidentally collect information about individuals who are complying with the law and are not subjects of interest.

Mitigation: This risk is not mitigated. CBP may deploy sensors, cameras, and surveillance technology in areas that are trafficked by members of the public who are not the target of CBP's investigative efforts. For example, ICAD sensors may be used to detect and track members of the public engaged in recreational hiking. Due to the covert nature of the placement of this equipment, CBP cannot provide appropriate markings or signage that would allow individuals to avoid the area to prevent CBP's collection of their information. CBP partially mitigates this collection risk by strictly controlling the collection, use, and retention of information it collects through Border Surveillance Systems (BSS).

Privacy Risk: There is potential risk of unauthorized access, use, or disclosure of ICAD information.

Mitigation: This risk is mitigated. CBP employees only use ICAD in compliance with applicable laws, policies, and directives. CBP trains users about appropriate collection and use procedures before providing access to a particular system. Failure to comply with these guidelines

[16] *See* Supra 7.

is a violation of CBP's Code of Conduct and may subject an employee to disciplinary action, including termination of employment or prosecution. Access to ICAD is limited to those specific CBP employees who require access as part of their assigned duties. Equipment use is tracked and monitored for accountability and authorized users and system administrators are the only persons with access to the systems and surveillance data.

Privacy Risk: There is a risk that ICAD may capture information about individuals or activities that are beyond the scope of CBP's authorities. For example, ICAD sensors may capture individuals entering places or engaging in lawful activities as they relate to their daily lives because the border includes populated areas. Although unlikely during busier time periods, there is a possibility that ICAD sensors may collect video images, photographs, and location information of an individual hiking or biking along paths that parallel the border.

Mitigation: This risk is mitigated by the fact that ICAD sensors are generally located in remote areas along the northern and southwest border and away from urban areas, communities, and places of worship. While ICAD sensors may record lawful activity at or near the border, these recordings are automatically overwritten unless a USBP agent investigating a sensor alert determines the recording is needed for an approved purpose. Specifically, CBP copies and retains ICAD sensor alert information only when the images captured are relevant to an active case file for law enforcement or border security purposes. CBP does not associate the ICAD alert or other data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation.

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.

All persons entering the United States at and between ports of entry are subject to inspection. CBP uses ICAD to monitor the border at and between ports of entry to provide for operational and situational awareness. This PIA provides general notice to the public of the presence of surveillance devices at the border and the use of these devices to detect and support the apprehension of persons crossing the border without inspection. CBP cannot reasonably provide timely notice of monitoring to individuals entering the United States between ports of entry. This PIA and the BPER[17] SORN serve as general notice of CBP's use of border surveillance activities along the U.S. border.

[17] *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.

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

CBP is obliged by statute to ensure the security of the border and to determine the identity and citizenship of all persons crossing the border; CBP does not provide individuals an opportunity to consent. CBP signage at the ports of entry informs persons of the video capture and its intended use. CBP recognizes that residents and visitors in areas proximate to the ports of entry and the border may have their images captured incidentally while hiking or biking along paths that parallel the border. CBP mitigates this risk by strictly controlling the collection, use, and retention of information in ICAD.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that a member of the public will not know that ICAD sensors deployed at and between ports of entry may be collecting photo, video, or other information obtained through surveillance technology.

Mitigation: This risk is partially mitigated through the publication of this PIA, which provides notice of CBP's use of ICAD sensors at and between ports of entry. In addition, CBP may avoid providing notice of an ICAD sensor in a particular area because doing so would compromise the integrity of a law enforcement operation or investigation. All individuals entering the United States at and between ports of entry are subject to inspection and data collection for operational and situational awareness. CBP posts signs at ports of entry to notify individuals of the inspection and information collection requirements, and general signage stating that the areas around the ports of entry are under camera surveillance. However, CBP cannot reasonably provide timely notice for individuals encountered between the ports of entry. This PIA and the BPER SORN serve as general notice of CBP's use of border surveillance technology to monitor activities along the U.S. border.

Privacy Risk: There is a risk that collected images of individuals or activities at the border either at or between the ports of entry may include innocent persons or persons who are complying with the law and who have not received notice.

Mitigation: This risk is partially mitigated. While CBP signage at the ports of entry provides notice of the presence of border surveillance systems, providing notice between the ports of entry is not operationally or logistically feasible. CBP sensors and surveillance technologies may capture lawful activity near the border, and individuals in the vicinity may not be aware of this information collection. Further, providing specific information on the location of specific technologies may pose operational security risks. Though it cannot always provide specific notice at the point of collection, CBP publishes PIAs and provides general notice to the public on its

website of its information collection activities near the border.

Privacy Risk: There is a risk that individuals cannot choose the degree to which they wish to participate since individuals subject to CBP surveillance activities are not provided an opportunity to opt out.

Mitigation: This risk is not mitigated. Individuals near the U.S. border may be subject to CBP surveillance and do not have the opportunity to opt out. CBP attempts to mitigate the impact of this risk by: (1) minimizing its collection and retention of surveillance information that is not linked to suspicious activity or an enforcement event; (2) employing auditing and accountability measures that ensure surveillance tools are used appropriately and judiciously; and (3) using surveillance tools in combination with other law enforcement tools to ensure that activities are based on accurate and relevant information. The lack of an opportunity to opt out increases the significance of public notice of these activities, which CBP provides on its website, through signs posted where feasible, and through the relevant PIAs and SORNs.

Section 5.0 Data Retention by the project

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

USBP is working with the CBP Records Information Management office to identify an approved records retention schedule for ICAD records. All records will be retained until an approved records retention schedule has been approved. Data associated to a prosecution case will be retained for 75 years as per the BPER SORN. Information used for prosecution is stored in the Prosecutions Module in e3.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that sensor alerts and reported suspicious activity may be retained in ICAD for a period longer than required by the purpose for which the information was collected.

Mitigation: This risk is partially mitigated. If an ICAD event is associated with a law enforcement action, the recordings are maintained in association with the respective case management system holding the associated law enforcement matter. CBP maintains recordings in these instances in accordance with the retention period for the respective case management system. The NARA retention period for data not associated with law enforcement matters will not be finalized until NARA approves the retention schedule for ICAD. CBP will publish an update to this PIA once the retention schedule is finalized. ICAD sensors may record lawful activity at or near the border and these recordings are automatically overwritten within a one to seven day timeframe unless a USBP agent investigating a sensor alert determines the recording is needed for an approved purpose.

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 does not routinely disseminate ICAD information outside of CBP. Rather, CBP typically shares information derived from ICAD with other law enforcement agencies, who share their sensor alerts and may assist CBP in an interdiction or law enforcement operation. CBP may share ICAD information with coordinating agencies to assist in an interdiction or operation, as appropriate and described by the routine uses of the respective SORNs that govern the case file or investigative report.

For example, a suspicious activity report may include "several suspects who were observed crossing the U.S. border near the intersections of X and Y." CBP may share this information with local law enforcement on the scene to coordinate the interdiction. CBP may also provide ICAD information, such as the sensor alert or event tracking information results, as part of the case file shared with federal law enforcement (e.g., Department of Justice) at the time of an arrest and subsequent prosecution.

CBP shares ICAD information along with other case file information from a system of records consistent with the Privacy Act of 1974 and the routine uses in the applicable SORN(s). CBP documents the disclosure on the DHS-191 Accounting of Disclosure Form when ICAD information is shared in conjunction with PII from a system of records (*e.g.*, e3). CBP conditions the disclosure to the receiving agency on:

- Receiving agency's use being consistent with the purpose for collection;
- Sharing being consistent with a statutory or published routine use; and
- Receiving agency's acceptance of the restriction barring unauthorized dissemination outside the receiving agency.

These conditions are stated in the written authorization provided to the receiving agency and represent the constraints on the use and disclosure of the information at the time of the disclosure.

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

CBP's disclosure of ICAD information to law enforcement partners is consistent with the original purpose of collection articulated in the BPER SORN to allow CBP to investigate and interdict individuals entering the United States between the ports of entry), or otherwise violating

laws CBP enforces and administers at the border.

6.3 Does the project place limitations on re-dissemination?

Yes. CBP only shares ICAD information when the requesting agency has an official need to know and that agency agrees to limit re-dissemination to only after first obtaining approval from CBP. CBP responds to requests for information or assistance by providing a written response to document the terms and conditions of use.

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

ICAD information associated with a law enforcement action may be shared pursuant to the case management system of records and is tracked through the use of the DHS-191, Accounting of Disclosure Form. The form requests the date, nature, purpose of each disclosure, and the name and address of the individual agency to which disclosure is made.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is the risk that PII from ICAD information may be shared inappropriately with external organizations.

Mitigation: This risk is mitigated. The same limitations on the use of the information that are in place for CBP and DHS also apply to the outside entity when sharing information with third parties. CBP restricts sharing or access to ICAD information based on "need to know" criteria, which requires the receiving entity to demonstrate a need for the data that is compatible with the use for which it was originally collected before the video or audio is disseminated. Likewise, the receiving entity must provide assurances that the data will be safeguarded in a manner consistent with CBP/DHS policy and practice and that the receiving agency will not disclose any shared data without the express prior written permission of CBP.

CBP does not currently have any arrangements to share ICAD information associated with an individual in an automated fashion. For any future routine sharing, CBP will develop a written arrangement (e.g., Memorandum of Understanding (MOU) or Information Sharing Access Agreement (ISAA)) to specify with particularity all terms and conditions that govern the use of the data in the event that such a recurring sharing arrangement is contemplated between CBP and an agency outside DHS. CBP would review the written arrangement and verify that the outside entity conforms to CBP's use, security, and privacy considerations before releasing information.

Section 7.0 Redress

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

Much of the data in ICAD is law enforcement sensitive and generally unavailable for access by the public. However, individuals may request information contained in ICAD through procedures provided by the Freedom of Information Act (FOIA) (5 U.S.C. § 552), the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)), when applicable, and the Judicial Redress Act.

Any individual, regardless of citizenship or immigration status, may seek notification of and access to any CBP record pursuant to procedures provided by FOIA, and can do so by visiting https://www.cbp.gov/site-policy-notices/foia 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 about oneself from any applicable system of records or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information. The individual must first verify their identity, meaning that the requestor must provide their full name, current address, and date and place of birth. The requestor must sign their request, and the signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While an inquiry requires no specific form, forms may be obtained for this purpose from the DHS Chief Privacy Officer and DHS Chief FOIA Officer at https://www.dhs.gov/foia or 1-866-431-0486.

In addition, the request should explain why the requestor believes the Department would have information on them; identify which component(s) of the Department the requestor believes may have requested information about them; specify when the requestor believes the records would have been created; and provide any other information that will help the FOIA staff determine which DHS Component agency may have responsive records.

If individuals are uncertain what agency or database manages the information, they may seek redress, regardless of citizenship, through the DHS Traveler Redress Program ("TRIP"), 601 South 12th Street, TSA-901, Arlington, VA, 22202-4220 or online at www.dhs.gov/trip.

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

Individuals may contest information collected through ICAD through any immigration or criminal proceedings that result from the encounter. The individual may file a Privacy Act amendment request if the ICAD information is associated with a system of records.

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for CBP records.

Mitigation: This risk is partially mitigated. This updated PIA and the applicable SORNs describe how individuals may make access requests under FOIA or the Privacy Act, as applicable. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law and policy.

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

CBP is providing notice to the public through this PIA, the applicable SORNs, and through the FOIA section on https://www.cbp.gov/site-policy-notices/foia.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is the risk innocent individuals may suffer negative effects if their information and images are erroneously associated with a crime without the ability to correct it.

Mitigation: This risk is mitigated. CBP does not use surveillance images to identify an individual, but instead to detect and interdict suspected criminal activity. An individual can only be linked to an image if the ICAD information leads to an apprehension, subsequent identification, and association with the case file. The individual may contest the association through the subsequent immigration or criminal proceeding if they are erroneously associated with ICAD information.

Privacy Risk: Due to the law enforcement nature of the information collected by ICAD and maintained in e3 or other law enforcement case management systems, there is a risk that individuals will not be able to access, correct, or amend their records if the records are exempted from access, correction, and amendment under the Privacy Act.

Mitigation: This risk is not mitigated. Providing individuals access or correction of records may be limited for law enforcement reasons, including as expressly permitted by the Privacy Act.

Permitting access to the records could inform the subject of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies. Information from certain CBP source systems, however, may be amended as indicated in the applicable SORN.

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?

Handling the information that is collected by ICAD applications is governed by standard operating procedures and policies. Only authorized users can extract materials from the systems. CBP mitigates the risk of misuse of data collected by, and accessed through ICAD by maintaining audit trails, including (at a minimum): username, access date and time, and functions and records addressed. CBP also requires users to follow security and privacy policies, follow established rules of behavior, and receive adequate training regarding the security of the system.

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

All ICAD users undergo initial security awareness training and complete the DHS online security awareness-training course and privacy awareness course on an annual basis. Training and interviewing techniques employed by USBP agents and Communication Assistants reduce the risk of inaccurate information being entered in the system.

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

All CBP employees with access to ICAD applications receive training on proper use of the systems and handling of any evidentiary data that may be extracted from the system. The system maintains a log of activities for auditing purposes. USBP Supervisors must authorize each employee to perform certain functions related to ICAD. Only authorized personnel are able to delete or add records before or after storage in an archive. Users may not remove or download data from the archive server without authorization. These precautions not only safeguard the data but also ensure the integrity of the information for when it is necessary to be used as evidence.

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 information sharing and MOUs concerning the sharing of PII, including those related to ICAD, are created by the operational owner of the system and sent to the CBP Privacy Officer and Office of Chief Counsel for review and to the DHS Privacy Office for final concurrence before being approved and signed.

Contact Official

C. Taylor Ray
Director, Systems Division
U.S. Border Patrol
U.S. Customs and Border Protection

Responsible Official

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

Approval Signature

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

_____

Lynn Parker Dupree
Chief Privacy Officer
Department of Homeland Security