Privacy Impact Assessment
for the

Centralized Area Video Surveillance System

DHS/CBP/PIA-014(a)

June 29, 2018

Contact Point
Colleen Manaher
Office of Field Operations
U.S. Customs and Border Protection
(202) 344-3003

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Centralized Area Video Surveillance System (CAVSS) — a system of cameras and separate microphones recording video and audio, respectively — furthers the Department of Homeland Security (DHS) U.S. Customs and Border Protection's (CBP) mission by collecting and maintaining video images and audio recordings of persons involved in any incidents or disturbances related to DHS/CBP law enforcement at the border, including inspection areas, while seeking entry or admission into the United States. CAVSS uses information technology to collect, maintain, and disseminate personally identifiable information (PII) in the form of video and audio recordings. CBP previously published a Privacy Impact Assessment (PIA) discussing the use of CAVSS at land border locations. CBP is updating and reissuing this PIA in full to provide notice of the widespread deployment of CAVSS throughout the CBP enterprise.

Overview

The fundamental mission of CBP is to safeguard America's borders while enabling legitimate trade and travel. In support of this mission and to enhance border security, CBP maintains a series of Closed Circuit Television (CCTV) cameras and microphones in and around various CBP facilities. CAVSS uses these CCTV cameras and microphones to collect video images and audio recordings that may contain PII at these locations. None of the CCTV cameras have audio recording capability; instead, separate microphones are installed near the cameras, or connect into the feed of a camera. The microphones are installed at every place where CBP regularly interacts with the public (e.g., a primary inspection lane); but not every camera necessarily has a microphone installed nearby. For cameras with associated microphones, CAVSS software combines the audio and video recording onto a digital video recorder (DVR). Select analog cameras and DVRs must meet stated hardware design requirements, which requires them to be in close proximity to each other. For cameras with associated microphones, CAVSS software records the audio and video feeds separately on a Network Video Recorder (NVR), which uses mass storage devices and multiple arrays of hard drives. However, live and recorded data from audio and video can be monitored simultaneously. Archives are system files of video and audio recordings exported from CAVSS and stored on external devices particularly for playback purposes in court and other situations.

In addition to enhancing border security, CAVSS imagery and audio recordings are also routinely used to support various CBP missions, administrative functions, and judicial proceedings. Video and audio recordings from CAVSS cameras and microphones are necessary to maintain the security of the physical premises and integrity of personnel employed therein, to provide a record of any incidents or disturbances involving the traveling public related to the inspection processes, to enforce maritime and air travel regulations, to assist with

law enforcement investigations and prosecute persons apprehended for violation of criminal laws, and to assist in adjudicating traveler complaints.

CAVSS cameras in primary inspection lanes and those CAVSS cameras that employ fixed and pan/tilt/zoom capabilities at CBP facilities are primarily focused on traveler identification. In support of that objective, CBP uses audio recording at port locations where the traveling public interacts with CBP personnel. The audio recording from CAVSS microphones can collect a person's verbal statement of his or her name, which is combined with the images collected by the CAVSS cameras for traveler identification. There is no textual PII stored in CAVSS, and PII captured by CAVSS audio/video cannot be electronically searched, queried, or analyzed. For example, at the current time, facial recognition technology is not deployed on the video in CAVSS.Only if there were microphones installed with a camera would audio be available for the respective video recordings. During the surveillance of an individual's presence at a CBP facility and interview of applicants for entry or admission into the United States, an individual's actions and utterances may be collected and stored by CAVSS cameras and microphones. This information may include an individual's name, date of birth, citizenship, port of entry, method of entry, vehicle information, date of entry, time of entry, secondary inspection (including the incident that required a secondary inspection), and a record of items found during inspection when captured by a microphone or in view of a camera.

Some ports are known as "limited hour" or non-24-hour port locations because the hours only correspond to the workday. The CAVSS cameras and CAVSS microphones at these locations focus on threat detection and officer response. CAVSS cameras and CAVSS microphones allow CBP to efficiently monitor non-24-hour CBP facilities without requiring CBP Officers to be physically present, affording the opportunity to view and listen to real-time events at distant CBP facilities. Both 24-hour and non-24-hour ports are networked across the CBP Wide-Area Network (WAN) to a Centralized Area Security Center (CASC), where CBP officers can remotely monitor the networked facilities 24 hours a day. At limited hour or non-24-hour ports, CAVSS cameras on the perimeter incorporate low-light technology coupled with motion detection sensors. At 24-hour ports, CAVSS cameras incorporate a full complement of low-light digital imagery, some of which have motion detection capabilities. CAVSS cameras used at port perimeters are typically day/night cameras due to insufficient lighting, and may be enhanced with infra-red lighting. Additionally, U.S. Border Patrol (USBP) uses CAVSS thermal cameras, which detect images based on heat signatures, and CAVSS perimeter-out cameras at certain locations.

The CAVSS perimeter-out cameras USBP uses may record images up to two miles from a CBP facility, but these longer range CAVSS cameras do not include a CAVSS microphone to record any sound with the images the CAVSS camera captures. USBP requires video information from CAVSS perimeter-out cameras to detect activities away from a CBP

facility that pose a threat to border security. For example, a CAVSS perimeter-out camera could alert USBP to a person leaving a vehicle headed toward a CBP facility, as that person may be trying to avoid detection in case CBP stops the vehicle. These perimeter-out CAVSS cameras are in fixed positions meant to survey a large area far away from a CBP facility, as opposed to the CAVSS cameras capable of following individuals in smaller CBP facilities. There is also no signage in the areas recorded by these longer range cameras informing individuals that CAVSS cameras are recording; the only signage for any CAVSS recording is at facilities where CBP interacts closely with individuals. This allows CBP to efficiently monitor non-24-hour CBP facilities without requiring CBP Officers to be physically present, affording the opportunity to view and listen to real-time events at distant CBP facilities. Both 24-hour and non-24-hour ports are networked across the CBP WAN to a CASC, where CBP officers can remotely monitor the networked facilities 24 hours a day.

In its standard configuration, CAVSS retains video and audio for 90 days on a DVR/NVR with the exception of recordings deemed to have law enforcement significance and retained for longer periods of time. The collection and storage of PII is limited to recorded audio utterances captured by a CAVSS microphone or visible images discernible via a CAVSS camera. There is no textual PII stored with the video or audio data in CAVSS. Stored video and audio data can only be queried by camera location and the data/time stamp on the recording, and PII captured by CAVSS cameras or CAVSS microphones cannot be electronically searched, queried, or analyzed. Audio or video captured by CAVSS cameras or CAVSS microphones will reside on the CAVSS servers and is automatically overwritten after 90 days, unless the PII recorded is part of an incident.

When CAVSS cameras or CAVSS microphones record images or audio of an incident, the relevant recordings will be copied, associated with a case file for the incident, and governed by the system of records notice (SORN) relevant to the incident's case file, (see Section 1.2). Video and audio files in CAVSS archives that have been designated as Significant Event Media,[1] because they depict a significant event, are saved on a disk, which is prominently marked "For Official Use Only" (FOUO). Significant events may include: natural disasters, weather-related incidents, intrusions, fires, tampering with equipment, and unlawful activity. Marked disks are stored in a locked, secure container in a secured area either onsite, or at the local CASC. None of the disks are marked with any PII or other identifiers. Only users with

[1] Significant Event Media are retained for six months, or until the close of the case associated with the event, whichever is later. If the video or audio is needed for a law enforcement case, the video or audio will be linked to the necessary PII and maintained consistent with the relevant enforcement system of records. The video and audio from CAVSS cameras and CAVSS microphones may become associated with an individual such that it is retrieved by a personal identifier and will be covered by a DHS SORN based on the type of incident and the context for the retrieval of information (e.g. physical/personnel security or border security and enforcement). Significant Event Media are retained for six months, or until the close of the case associated with the event, whichever is later. If the video or audio is needed for a law enforcement case, the video or audio will be linked

prior authorization have access to the locked DVRs/NVRs and the marked disks in locked containers.

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?

The data collected by CAVSS is generally authorized by CBP's general statutory authority, which includes the Homeland Security Act of 2002, Public Law 107-296, Section 1512, 116 Stat. 2310 (November 25, 2002); the Immigration and Nationality Act, including 8 U.S.C. §§ 1222-1223, 1225, and 1357, implemented in accordance with the regulations set forth in 8 CFR § 287.5; various customs statutes, including 19 U.S.C. §§ 482, 1433, 1459, 1461, 1499, 1581, 1582, 1644; 6 U.S.C §§ 202, 211, 231; and agriculture laws, including 7 U.S.C. §§ 8303, 8304, 8307.

Further, 40 U.S.C. § 1315 authorizes DHS to protect the buildings, grounds, and property owned, occupied, or secured by the Federal Government and its agencies, as well as the persons on the property. In protecting that property and those persons in and around CBP facilities, CBP is acting in its official capacity to secure the border and has authority to record audio information in CAVSS pursuant to 18 U.S.C. § 2511(2)(d).

In addition, the *Physical Security Criteria for Federal Facilities, An Interagency Security Committee Standard Report* issued on April 12, 2010 (and successor documents) require CCTV monitors for the majority of federal buildings, including those at CBP Facilities, from low security requirements to very high. The DHS Physical Security Construction and Equipment Handbook, May 27, 2010, also requires CCTV for the protection of DHS Headquarters sites.

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

Video and audio in CAVSS are not retrievable by a personal identifier while archived on the DVRs/NVRs or in storage, and therefore do not constitute a system of records under the Privacy Act of 1974. However, video and audio from CAVSS cameras and CAVSS microphones may become associated with an individual such that it is retrieved by a personal identifier and will be covered by a DHS SORN based on the type of incident and the context for the retrieval of the information. For incidents related to the physical access to a CBP facility, those are covered under the DHS/ALL-024 DHS Facility and Perimeter Access Control and Visitor Management SORN[2], or DHS/ALL-025 Law Enforcement Authority in

[2] 75 Fed. Reg. 5609, Feb. 3, 2010.

Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security SORN.[3] In the event that those incidents relate to an internal affairs action, these video and audio recordings may also be maintained pursuant to DHS/ALL-023 Department of Homeland Security Personnel Security Management.[4]

For activities related to border security, video or audio associated with a law enforcement activity will be linked to PII maintained in reports and records residing in the associated case file system of records including, DHS/CBP-011 U.S. Customs and Border Protection TECS[5], DHS/CBP-023 Border Patrol Enforcement Records (BPER)[6], and DHS/CBP-024 Intelligence Records System (CIRS)[7]. These systems provide electronic case management capability to support DHS law enforcement activities and when appropriate, the case status will be updated to reflect the existence of video maintained external to the system to support the narrative remarks contained in the system.

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

A system security plan was completed as part of the process to renew the Authority to Operate (ATO) which is expected to be obtained on August 7, 2018.

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

No. If CAVSS information is incorporated into a particular system of records, the schedule approved for that system of records would govern the retention of the CAVSS data.

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.

CCTV and CAVSS audio/video recordings are exempt from the Paperwork Reduction Act (44 U.S.C. § 3510) because the recordings constitute a passive collection of information on members of the public.

[3] 82 Fed. Reg. 27274, June. 14, 2017.
[4] 75 Fed. Reg. 8088, Feb. 23, 2010.
[5] 73 Fed. Reg. 77778, Dec. 19, 2008.
[6] 81 Fed. Reg. 72601, Oct. 20, 2016.
[7] 82 Fed. Reg. 44198, Sept. 21, 2017.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

CAVSS collects and temporarily stores video images and audio recordings of everyday activity in and around CBP facilities as part of the background data that is collected to observe and to record any incidents and disturbances. If no disturbances or incidents are observed, the images and audio are overwritten after 90 days as subsequent recordings overwrite the past CAVSS audio and video data after the designated timeframe. PII that may be stored on the video (if discernible by the camera) or audio (if captured by the microphone) recordings may include:

- Name;
- Date of birth;
- Citizenship;
- Physical description;
- Verbal statements;
- Port of Entry;
- Method of entry, including vehicle information;
- Date of entry;
- Time of entry; and
- A record of items found during the inspection.

Information stored by CAVSS longer than 90 days includes audio and video images of individuals involved in incidents or disturbances subject to legal holds or executive/judicial orders, including DHS/CBP inspection at a CBP facility, images/audio of the individual escorted into, inside, and out of the inspection areas of the port of entry, video images and audio of activity at the port perimeter at non-24-hour ports, and, in certain instances, video images of activity beyond the port perimeter. For those not involved in such incidents or disturbances (the vast majority of the public at the border), CAVSS will still collect audio and video data that CAVSS will automatically overwrite after 90 days.

Files may be marked with date/time stamps, camera or microphone location, and restriction markings (“FOUO”). Responses to critical incidents, intrusions, or safety-related

incidents captured by CAVSS that necessitate notification of incidents outside DHS to other federal, state, or local law enforcement authorities will be recorded in paper logs that contain the date, time, location, telephone number, and the officer's name and rank. These paper logs are not indexed to be searched by any criteria other than date and time stamps.

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

Video images of the areas surrounding CBP facilities, and the traveling public along with accompanying audio utterances are collected using CAVSS cameras and separate CAVSS microphones at CBP facilities in the United States.

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

No commercial or publicly available data is used.

2.4 Discuss how accuracy of the data is ensured.

Video and audio are recorded in real time to maintain a factual record of events. An authorized user in the CASC can adjust CAVSS cameras and CAVSS microphones to improve the video images and audio recordings (e.g., resolution and microphone volume). Once recorded, the records are kept in a secure CBP facility where multiple forms of authentication are required before entering the facility, including badges, locked doors, and keyed entries. Users of CAVSS are required to log into a CBP workstation using a CBP identification number and valid password, and are then required to log into CAVSS itself. Additionally, authorized users of CAVSS must successfully complete training as described in Sections 3.4 and 8.2.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that information may be collected beyond the scope of CBP's mission of border security.

Mitigation: The nature of CBP's mission requires the collection of information relating to the security of the nation's borders. The video and audio information captured at CBP facilities record current inspection and law enforcement activities that are relevant and necessary to maintain the security of the physical premises, the integrity of the personnel employed therein, and to provide a record of any incidents or disturbances involving the traveling public related to the inspection processes.

Privacy Risk: There is a privacy risk that an individual's image is collected as part of an incident about someone else.

Mitigation: This risk cannot be fully mitigated given that the CAVSS equipment is stationary and focused on designated spaces and the individuals who enter these areas. An individual's image may be captured by CAVSS as part of an incident or as part of a lawful activity, however CBP will not identify or attempt to identify any individuals from CAVSS recordings unless it is relevant and necessary for law enforcement investigations. Any images not associated with incidents will be overwritten after 90 days. There is no textual PII stored in CAVSS, and PII captured by CAVSS audio/video cannot be electronically searched, queried, or analyzed. For example, at the current time, facial recognition technology is not deployed on the video in CAVSS.

Privacy Risk: There is a privacy risk that CAVSS collects more information than needed because a greater population is impacted by the additional deployments throughout CBP.

Mitigation: This risk is minimized because the business (or law enforcement) justification for collection of the data, records retention requirements, use and redress related to video and audio monitoring are unchanged. It is only that a greater volume of recordings will be collected due to wider usage of the equipment. Additionally, while equipment is deployed in detention facilities, there are restrictions on the collection of video and audio in private areas (i.e., showers, bathrooms) of these detention centers.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

The video images and audio recordings captured by CAVSS cameras and CAVSS microphones are used for port surveillance and to enhance border security. Video and audio from CAVSS is necessary to maintain the security of the physical premises and integrity of the public and personnel present therein, to provide a record of any incidents or disturbances involving the traveling public, to assist with law enforcement investigations and the prosecution of persons apprehended for violation of criminal laws, and to assist in the adjudication of complaints. If notification of the incident is necessary to a federal, state, or local law enforcement authority outside of DHS, CBP will record in paper logs the date, time, location, telephone number, and the name and rank of the officer notified. Situations requiring notification include critical incident intrusions or safety related incidents captured by CAVSS cameras and CAVSS microphones. For information release procedures, please see section 3.3.

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. CAVSS captures and stores video and audio on the DVRs/NVRs that record and index the data by date, time, and camera in audio/video files that can be viewed by authorized CBP officials. In cases in which CAVSS imagery and audio recordings are used to address an incident, by, for example, supporting administrative and judicial proceedings, the audio/video files may be saved onto a digital video disk (DVD).

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

Access to the CAVSS system is restricted to CBP personnel. No other DHS component representatives have assigned roles and responsibilities within the system. However, consistent with their enforcement jurisdiction, other DHS components (and other law enforcement entities) may request surveillance video or audio records in support of their enforcement mission. In the event that archived video footage or audio recordings from an event needs to be retrieved for evidence or investigation, the requesting DHS component (e.g., U.S. Immigration and Customs Enforcement (ICE)), must coordinate with authorized CBP personnel, demonstrating an official "need to know" before archived data is released.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: Video and audio recordings will be used in a manner inconsistent with their original purpose of collection.

Mitigation: In furtherance of CBP's mission to secure the border, video and audio surveillance recordings are used to ensure the security of the physical premises at CBP facilities, the integrity of the personnel employed therein, and to provide an evidentiary record of any incident or disturbance at a CBP facility including in areas used for DHS/CBP inspections at a CBP facility, inspection areas of the port of entry, the port perimeter at non-24-hour ports, and, in certain instances, beyond the port perimeter. To ensure that the recordings are accessed and used in a manner consistent with their original purpose of collection, all video and audio recordings are stored on DVRs/NVRs that are located in either locked cabinets/racks or in a secured LAN room. The racks containing the DVRs/NVRs are installed in CBP-controlled access areas that may be entered only by authorized personnel. To gain access to (live or recorded) video or audio, authorized personnel must have prior signed authorization from their supervisors and Port Directors/Chiefs/Directors (via User Access Request Forms). The forms will also identify which camera locations can be accessed and what

actions are permitted with the content. CAVSS user access is reassessed annually. These users must also have a valid "need to know" and have been trained on the proper use of the system, including the two-factor authentication process, before they may directly access the system and specific recordings. CBP Directive No. 5620-003 (dated June 2017) provides guidance on access, recordkeeping, disclosure and response protocols related to CAVSS.

Additionally, all authorized users must take and successfully complete the CBP IT Rules of Behavior Training in addition to the mandatory Privacy Act training annually required for all CBP employees and contractors. As an additional control to ensure use limitation, video and audio recordings that have been designated as Significant Event Media are saved on disks which are prominently marked "For Official Use Only" (FOUO) and do not contain any other markings except date and time stamps. Such marked disks are stored in a locked, secure container in a secured area either onsite, or at the local CASC. Only users with prior authorization have access to the locked DVRs/NVRs and the marked disks in locked containers. Significant events may include: natural disasters, weather-related incidents, intrusions, fires, tampering with equipment, and unlawful activity.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

This PIA provides notice to the general public as to the collection and use of recorded images and audio information. With regard to travelers, signage is posted throughout CBP facilities that notify the public that video and audio recording devices are in use. Per CBP procedural guides regarding video and audio surveillance, twenty-four (24) hour closed circuit television (CCTV) surveillance and recording are required at all locations. The requirements will depend on assessments of the security level for each facility. That is, the quantity and placement of these notices will vary across facilities. Time-lapse video recordings are also highly valuable as a source of evidence and investigative leads. Warning Signs advising of 24 (twenty-four) hour surveillance serves to protect employees and facilities and notifies the public of collection of images and other information on them.

The warning signs typically read as follows:

NOTICE: 24 HOUR VIDEO AND AUDIO MONITORING ARE IN USE AT THIS FACILITY

At CBP facilities along the southern border, the signage is printed in English and Spanish. At other CBP facilities located along the northern border, the signage is printed in English and French. Additionally, notification or signage is prominently displayed at the site where the cameras/microphones are deployed and operational to alert potential subjects of their usage. Please see the Appendix for additional example signage.

Notification signs are not posted outside the CBP facilities with perimeter-out CAVSS cameras used by USBP that can record video of individuals — albeit with significantly less resolution and tracking — up to two miles away. The large areas covered by longer range CAVSS cameras make the placement of signage covering all possible areas capable of being recorded almost impossible. Through publication of this PIA and signage at CBP facilities, the agency provides notice to the public that video and audio recording devices are in use.

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

Generally, the decision whether to travel internationally or to travel in the proximity of another country's borders is a matter within the discretion of the individual. United States law requires individuals seeking to enter the country to identify themselves and demonstrate admissibility to the United States, if applicable, and otherwise comply with other U.S. law. Inasmuch as the cameras and audio recording devices used at CBP facilities are continually in use, there is effectively no mechanism for an individual to decline to provide information, opt out of the project, or decline to consent to the uses of the information. The only way for an individual to avoid the program is to not seek to approach a CBP controlled space that is at or near a CBP facility housing CAVSS equipment.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware that their actions and conversations are being recorded.

Mitigation: In order to provide notice to the traveling public and visitors to CBP facilities, signs are prominently posted throughout CBP facilities that notify the public that video and audio recording devices are in use. As an additional measure of transparency, location-specific, dual-language (Spanish or French) signage is prominently displayed at each site where the video/audio recording devices are deployed to alert potential subjects of their usage with phrasing that indicates the following: "NOTICE: 24 HOUR VIDEO AND AUDIO MONITORING ARE IN USE AT THIS FACILITY". Please see the Appendix for example signage.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

The DVRs/NVRs used by CAVSS are configured to record and maintain data for 90 days. Once this time limit is reached, video and audio surveillance recordings are automatically over-written, unless a significant event has occurred that requires the recording to be extracted from DVR/NVR storage and saved in encrypted devices. A significant event might include the apprehension of an individual attempting to illegally enter the country or one found to be in possession of prohibited merchandise and subsequently arrested by CBP Officers. Some significant events require notification of an incident to a federal, state, or local law enforcement authority outside of DHS. When this occurs, CBP will record in paper logs the date, time, location, telephone number, and the notified officer's name and rank. Situations requiring notification include critical incidents, intrusions, or safety-related incidents captured by CAVSS. CBP will have up to 90 days to retrieve a significant event from earlier recordings. If backup of a specific file or all files from a DVR/NVR are required for evidentiary purposes, an encrypted DVD will be prepared and stored in a secure on-site location.

Significant Event Media are retained for six months, or until the close of the case associated with the event, whichever is later. If the video or audio is needed for a law enforcement case, the video or audio will be linked to the necessary PII and maintained consistent with the relevant enforcement system of records. The video and audio from CAVSS cameras and CAVSS microphones may become associated with an individual such that it is retrieved by a personal identifier and will be covered by a DHS SORN based on the type of incident and the context for the retrieval of information (e.g., physical/personnel security or border security and enforcement).

The video and audio recordings are stored in accordance with a published system of records that permits collection and management of the Agency records for a specific purpose. For activities related to personnel security or internal affairs, or for activities related to the physical security of the port or CBP location, records are maintained pursuant to DHS/ALL-024 DHS Facility and Perimeter Access Control and Visitor Management SORN,[8] DHS/ALL-023 Department of Homeland Security Personnel Security Management,[9] and DHS/ALL-025

[8] 75 Fed. Reg. 5609, Feb. 3, 2010.
[9] 75 Fed. Reg. 8088, Feb. 23, 2010.

Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security.[10]

For activities related to border security, video or audio associated with a law enforcement activity will be linked to PII maintained in reports and records residing in the associated case file system of records including, DHS/CBP-011 U.S. Customs and Border Protection TECS,[11] DHS/CBP-023 Border Patrol Enforcement Records (BPER),[12] and DHS/CBP-024 Intelligence Records System (CIRS).[13] These systems provide electronic case management capability to support DHS law enforcement activities, and when appropriate the case status will be updated to reflect the existence of CAVSS video or CAVSS audio, maintained external to the system, to support the narrative remarks contained in the system.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Data may be retained longer than necessary, which may reduce the relevance and timeliness of the data.

Mitigation: To ensure that data is kept only for the shortest time period necessary, non-significant CAVSS video and CAVSS audio recordings are routinely overwritten after 90 days. Unless a particular incident or event is identified and a backup disk copy made for storage, more recent recordings will overwrite previous data. Disks containing recordings from CAVSS cameras or CAVSS microphones that depict a significant event are designated as Significant Event Media and retained for up to six months or until the close of the case associated with the event. When recordings become associated with law enforcement actions, they will be retained based on the requirements specified in the applicable SORNs for the relevant systems.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS 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.

DHS may use this information in support of its mission responsibilities, including in proceedings against individuals who are apprehended entering the United States illegally, smuggling contraband into the United States, or committing other unlawful activities of which

[10] 82 Fed. Reg. 27274, June. 14, 2017.
[11] 73 Fed. Reg. 77778, Dec. 19, 2008.
[12] 81 Fed. Reg. 72601, Oct. 20, 2016.
[13] 82 Fed. Reg. 44198, Sept. 21, 2017.

CAVSS can provide evidence. As part of the law enforcement mission of CBP, video and audio recorded from CAVSS cameras and CAVSS microphones may be shared with other agencies to assist with their law enforcement investigations or intelligence operations. Responses to critical incidents, intrusions, or safety-related incidents captured by CAVSS cameras or CAVSS microphones that necessitate notification outside DHS to other federal, state, or local law enforcement authorities will be recorded in paper logs that include the date, time, location, telephone number, and the officer's name and rank. These paper logs are not indexed to be searched by any criteria other than date and time stamp. When audio or video recorded from CAVSS cameras or CAVSS microphones is associated with a system of records, those audio or video recordings may be shared along with other case file information covered in that system of records consistent with the Privacy Act of 1974 and the routine uses in the applicable SORN. If audio or video recordings from CAVSS cameras or CAVSS microphones are not associated with a system of records and CBP still wishes to share such audio and video, this PIA provides notice to the public that CBP may share audio or video recorded from CAVSS cameras or CAVSS microphones using criteria in Section 6.5.

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

The video and audio from CAVSS cameras and CAVSS microphones may become associated with an individual such that it is retrieved by a personal identifier and will be covered by a DHS SORN based on the type of incident and the context for the retrieval of information. The various CAVSS record types to be covered by SORNs include:

1. Records relating to the management and operation of the facility and perimeter access control and visitor management system including but not limited to closed circuit television (CCTV) recordings, audio recordings, and digital video recordings: DHS/ALL-024 DHS Facility and Perimeter Access Control and Visitor Management SORN.[14]

2. Information pertaining to incidents and offenses, including internal affairs incidents: DHS/ALL-023 Department of Homeland Security Personnel Security Management,[15] and DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security[16].

3. Data on aliens in custody or detained, including: Transportation information, identification numbers, custodial actions (such as meals, conditions of detainee

[14] 75 Fed. Reg. 5609, Feb. 3, 2010.
[15] 75 Fed. Reg. 8088, Feb. 23, 2010.
[16] 82 Fed. Reg. 27274, June. 14, 2017.

cell, overall detainee care information), custodial property, information related to detainers, book-in/book-out date and time, limited health information, and other alerts: DHS/CBP-011 U.S. Customs and Border Protection TECS,[17] DHS/CBP-023 Border Patrol Enforcement Records (BPER)[18], and DHS/CBP-024 Intelligence Records System (CIRS)[19] System of Records.

The above SORNs set forth routine uses that permit the sharing of recorded video and audio information associated with a system of records with law enforcement and prosecutorial entities or as part of litigation. This sharing is compatible with CBP's law enforcement mission, including ensuring the security of the United States by deterring terrorists from smuggling weapons and explosives across the border, as well as stemming the tide of illegal drugs and ensuring lawful immigration and travel.

6.3 Does the project place limitations on re-dissemination?

The CBP Privacy Officer may approve the sharing of video or audio that is not associated with a system of records only if the CBP Privacy Officer decides the requesting agency has an official need to know, and the requesting agency agrees to limit re-dissemination without first seeking approval from CBP. When video or audio is associated with a system of records, authorization to share information with an external law enforcement agency is subject to approval by the CBP Privacy Officer, insofar as the request and use are consistent with the Privacy Act, the published routine uses for the appropriate SORN, and the receiving agency agrees to be restricted from further unauthorized sharing of the information. The receiving agency's acceptance and use of the shared information is conditioned on (1) the receiving agency's use being consistent with the purpose for collection, (2) the sharing being consistent with a statutory or published routine use, and (3) the 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 around the use and disclosure of the information at the time of the disclosure.

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

Video or audio associated with a system of records that is shared outside of the Department is tracked through the use of the DHS-191, *Accounting of Disclosure Form*. CBP users of CAVSS prepare a DHS-191 form each time they share information covered by a system of records from CAVSS outside of DHS. CBP and DHS share audio or video

[17] 73 Fed. Reg. 77778, Dec. 19, 2008.
[18] 81 Fed. Reg. 72601, Oct. 20, 2016.
[19] 82 Fed. Reg. 44198, Sept. 21, 2017.

information from CAVSS cameras or CAVSS microphones in accordance with the language of a letter of authorization, which facilitates the sharing of a particular record from CAVSS in response to a request for assistance from another law enforcement agency.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Information may be shared under inappropriate circumstances or inconsistent with published SORNs and CBP policies.

Mitigation: When sharing information with third parties, the same limitations on the use of the information that are in place for CBP and DHS also apply to the outside entity. Access to CBP data is governed by "need to know" criteria that require that the entity receiving the information demonstrate a need for the data that is consistent with the use for which it was originally collected before the video or audio from CAVSS cameras or CAVSS microphones is disseminated. The entity receiving this information must demonstrate this "need to know" in writing to CBP before CBP will provide the data. Likewise, with regard to security of the information and accountability of the personnel using the video or audio from CAVSS cameras or CAVSS microphones, the receiving entity is informed in writing that the data must be safeguarded in a manner consistent with CBP/DHS policy and practice and that no disclosure of any shared data may occur without the express prior written permission of CBP (see Section 6.3).

In the event that a recurring sharing arrangement is contemplated between CBP and a federal agency outside DHS, CBP may develop a written arrangement (e.g., Memorandum of Understanding) to specify with particularity the terms and conditions that govern the use of the functionality or data, including limitations on use. Before releasing information, CBP would review the written arrangement and verify that the outside entity conformed to use, security, and privacy considerations.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals may request information about their records contained in CAVSS through procedures provided by the Freedom of Information Act (FOIA)[20] and, whenever those records

[20] 5 U.S.C. § 552.

contained in CAVSS are also associated with a system of records as described in Section 1.2, the access provisions of the Privacy Act of 1974, to the extent applicable.[21]

Generally, information recorded by CAVSS cameras and CAVSS microphones is not retrievable by personal identifiers, so it will be difficult for an individual to find and view a particular video or hear the accompanying audio. Additionally, video and audio recorded by CAVSS cameras and CAVSS microphones are only stored for 90 days unless deemed to be a significant event. The video and audio recorded by CAVSS cameras and CAVSS microphones is then recorded over, which limits the amount of time an individual has to access his or her information. Accordingly, an individual wishing to access his or her information from CAVSS should provide the time, day, specific CBP facility, and specific area within or around the CBP facility to find the information, or other identifying information that will assist CBP in locating the requested record. CBP redacts third-party PII prior to the release of the recording.

Individuals seeking notification of and access to any record contained in CAVSS or seeking to contest its content, may gain access to certain information about them by filing a Freedom of Information Act (FOIA) or Privacy Act request with CBP at https://foia.cbp.gov/palMain.aspx or by mailing a request to:

U.S. Customs and Border Protection
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, D.C. 20229
Fax Number: (202) 325-0230

When CAVSS records become associated with a SORN and subject to the Privacy Act, information may be exempt from individual access or amendment provisions of the Privacy Act because access to the data in CAVSS could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the existence of the investigation, or reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, tamper with witnesses or evidence, and avoid detection or apprehension. In other cases, however, individuals may be able to gain access to the data pertaining to them under the FOIA process. Determinations regarding the granting or denial of access are made once the request is received by the CBP Privacy Officer who will forward it, if necessary, to the data-owning agency. CBP reviews all such requests on a case-by-case basis and may withhold the records if an exemption under FOIA applies.

For the cases when CAVSS records become associated with a SORN subject to the Privacy Act, to the extent the CAVSS information is part of a SORN, the Secretary of the

[21] 5 U.S.C. § 552a(d).

Department of Homeland Security has exempted the systems of records associated with CAVSS from the notification, access, and amendment requirements of the Privacy Act due to the law enforcement nature of CAVSS.[22] Because of the law enforcement purposes for which information is collected, individuals do not have direct access to CAVSS or the data contained therein.

CAVSS overwrites video images and audio recordings, generally after 90 days of the recording. In cases of incidents involving legal holds or executive/judicial orders, the information may be retained longer as described in Section 5.1. Any information not on litigation hold or subject to executive or court order prior to the 90 days would be overwritten or destroyed thereafter. CAVSS also destroys the information pursuant to the retention policies discussed in 5.1.

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

The CAVSS system records live action video images and audio utterances. No procedures exist to edit, correct, or amend the recorded information, aside from copying Significant Event Media clips from the DVR/NVR to secure storage. However, video or audio recordings associated with a case file will follow the access and amendment procedures associated with that system of records. If a traveler believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
OPA—Rosslyn
U.S. Customs and Border Protection
1300 Pennsylvania Avenue, NW
Washington, DC 20229

Travelers may also contact DHS TRIP, 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip. Individuals making inquiries should provide as much identifying information as possible regarding themselves to identify the record(s) at issue.

[22] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, Final Rule for Privacy Act Exemptions (Aug. 24, 2009), 74 F.R. 42578; DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records, Notice of Proposed Rulemaking for Privacy Act Exemptions (June 14, 2017), 82 FR 27218; DHS/CBP-11 U.S. Customs and Border Protection TECS, Final Rule for Privacy Act Exemptions (Aug. 31, 2009), 74 F.R. 45072; and DHS/CBP-23 Border Patrol Enforcement Records (BPER), Final Rule for Privacy Act Exemptions (Dec. 20, 2016), 81 F.R. 92549.

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

Through the publication of this PIA, individuals seeking notification of and access to CAVSS audio and video recordings are informed that they may submit a request through the procedures in 7.1 and 7.2, above. Individuals seeking records that are linked to an individual such that the records are retrievable by a personal identifier, and individuals seeking records that are linked to a case file must conform with the Privacy Act regulations set forth in 6 C.F.R. Part 5, in accordance with the DHS/ALL-024 DHS Facility and Perimeter Access Control and Visitor Management SORN,[23] DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security SORN,[24] DHS/CBP-011 U.S. Customs and Border Protection TECS,[25] DHS/CBP-023 Border Patrol Enforcement Records (BPER)[26] and DHS/CBP-024 Intelligence Records System (CIRS).[27]

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: Due to the law enforcement nature of this system, and the fact that recordings cannot be altered, individuals may not correct or amend the recordings.

Mitigation: The system operates as a passive observer, creating recordings of live activity at CBP facilities. As such, individual participation by the traveling public is not elective; the only way to decline participation is to not seek to approach a CBP controlled space that is at or near the port of entry. CBP provides awareness of the system and the creation of video or audio recordings from CAVSS cameras or CAVSS microphones through onsite signage and the publication of this PIA. Because the records in CAVSS are a memorialization of events as they occur, they cannot be amended or corrected through CAVSS. However, limited redress, in the form of access, is available through requests as described in Sections 7.1 and 7.3. When video or audio is associated with a case file in another system of records, individuals may seek redress through the procedures for that system of records.

[23] 75 Fed. Reg. 5609, Feb. 3, 2010.
[24] 82 Fed. Reg. 27274, June. 14, 2017.
[25] 73 Fed. Reg. 77778, Dec. 19, 2008.
[26] 81 Fed. Reg. 72601, Oct. 20, 2016.
[27] 82 Fed. Reg. 44198, Sept. 21, 2017.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

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

CAVSS recordings are proprietary, meaning that the audio/video can only be viewed on a CAVSS workstation, which may be accessed only from within a secure CBP facility where multiple forms of authentication are required before entering the facility, to include badges, locked doors, and keyed entries. Users of CAVSS are required to log into a CBP workstation using a CBP hash ID and valid password, and are then required to log into CAVSS itself. Additionally, authorized users of CAVSS must successfully complete training as described in Sections 3.4 and 8.2.

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

All CBP officers and Border Patrol agents receive training at federal facilities for their specific role and all CBP employees are required to take annual "CBP IT Security Awareness and Rules of Behavior Training" through the online DHS Virtual Learning Center to gain access to the CBP network, systems, or data. All CBP employees and contractors must also complete mandatory Privacy Act training annually. Additionally, written guidance to CAVSS users includes privacy compliant procedures to follow for disclosure of audio or video information recorded by CAVSS cameras or CAVSS microphones.

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

CAVSS user access is restricted to certain designated CBP Officers and other similarly authorized CBP personnel with a need to know. Access to particular video and audio feeds to CAVSS cameras or CAVSS microphones is based upon the user's role and further limited by geography.

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?

No routine sharing of recorded images or audio files recorded by CAVSS cameras or CAVSS microphones exist. However, in the event that a recurring sharing arrangement between CBP and an agency outside DHS is contemplated, CBP may develop a written

arrangement (e.g., Memorandum of Understanding) to establish the terms of use and security for the exchanged data. The written arrangement would specify the terms and conditions that govern the use of the functionality or data, including limitations on use. Before releasing information, CBP would periodically review the written arrangement and would verify that the outside entity conformed to use, security, and privacy considerations.

Responsible Officials

Colleen Manaher
Office of Field Operations
U.S. Customs and Border Protection
Department of Homeland Security

Debra Danisek
CBP Privacy Officer
Office of the Commissioner
U.S. Customs and Border Protection
Department of Homeland Security

Approval Signature Page

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

APPENDIX

Northern Border Signage for CAVSS

Southern Border Signage for CAVSS