Privacy Impact Assessment
for the

Border Surveillance Systems (BSS)

DHS/CBP/PIA-022

August 29, 2014

Contact Point
Douglas Harrison
Associate Chief, Office of Border Patrol
U.S. Customs and Border Protection (CBP)
(202) 344-2050

Reviewing Official
Karen Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), Border Surveillance Systems (BSS) are a combination of surveillance systems deployed to provide comprehensive situational awareness along the United States border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. The BSS include commercially available technologies such as fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, and radio frequency sensors. CBP is conducting this PIA because the BSS collect and process Personally Identifiable Information (PII) including video images, photographs, radio frequency emissions, and location information. In addition, the Secure Border Initiative-net (SBInet) Program PIA, which addresses the SBInet Southern Border and Northern Border Projects will be retired upon publication of this PIA.

Overview

CBP is responsible for securing the borders of the United States while facilitating lawful international trade and travel. CBP employs various technologies to enforce hundreds of U.S. laws and regulations at the border, including immigration and narcotics enforcement laws. BSS are a combination of surveillance technologies designed to assist CBP in detecting, identifying, apprehending, and removing persons illegally entering the United States at and between ports of entry and enforcing U.S. law. BSS may also monitor a particular individual or location as part of a law enforcement investigation, and as evidence if the apprehension of the individual results in criminal proceedings. BSS that are located across urban, rural, and remote areas along the U.S. border include tethered aerial video, radars, mobile and fixed ground video with day and night thermal capabilities, ground sensors, radio frequency sensors, ultra-light aircraft detection, and acoustic sensing devices. Each surveillance system is deployed taking into account the surrounding terrain and population. DHS is conducting this PIA because BSS collect and process PII, including video, images, radio frequency emissions, and location information.

DHS created the SBInet Program in November 2005, to reduce illegal immigration and secure the nation's borders by providing CBP more comprehensive situational awareness along the U.S. border.[1] The "Project 28" (P-28) initiative was a concept demonstration prototype for the SBInet Program followed by a geographical expansion and an operational capabilities enhancement known as the SBInet Southern Border and SBInet Northern Border Projects. On January 14, 2011, DHS Secretary Janet Napolitano directed CBP to end the SBInet Program as originally conceived after assessing the efficiency of the SBInet Program.

CBP replaced the SBInet Program with BSS, a new border security technology plan using

[1] SBInet (CBP's initial border surveillance technology initiative) began as an implementation of the Executive Branch Program, "Border Security and Control Between the Ports of Entry," as authorized under the Secure Fence Act of 2006, Pub. L. #109-367, 8 U.S.C. § 1701 Note; Title 8, C.F.R, Section 287. Initially piloted as Project 28, the program sought to integrate the use of fixed tower cameras, ground sensors, and a Common Operational Picture to enhance border security and combat illegal immigration.

existing and proven technology tailored to distinct terrain and population density. BSS represent a reassessment of the need to provide increased situational awareness for CBP in areas that present capability gaps based on the lessons learned from the P-28 and SBInet Projects. BSS include the Block 1 (part of SBINet) and the Northern Border Remote Video Surveillance as well as the following new projects: Integrated Fixed Tower (IFT), Remote Video Surveillance System (RVSS), Intelligent Computer Assisted Detection (ICAD), Law Enforcement Technical Collection (LETC), Mobile Video Surveillance Systems (MVSS), Mobile Surveillance Capability (MSC), Agent Portable Surveillance System (APSS), Ultra-Light Aircraft Detection (ULAD), and Tethered Aerostat Radar System (TARS). BSS may capture PII in urban, rural, and remote areas along the U.S. border through video cameras, laser range finders, radar, radio frequency sensors and acoustic devices, or some combination thereof. Not all data collected by BSS may be used to identify an individual at the time of collection; however, data captured using the various BSS may later be associated with an individual. Below is a description of the different types of systems BSS uses:

Mobile Border Surveillance Systems

Mobile border surveillance systems are capable of collecting surveillance data from various locations, because the surveillance platform can physically be moved to meet changing mission needs. A description of each of the mobile border surveillance systems follows:

- Mobile Video Surveillance System (MVSS) uses mobile video recording units on platforms that can be moved to provide the best visual range for surveillance of several miles. MVSS provide day and night surveillance images that allow the user or operator to determine if there are items of interest or suspicious criminal activities occurring with the area of coverage and to provide situational awareness to the interdicting Border Patrol Agent.
- Mobile Surveillance Capability (MSC) uses truck-mounted mobile video recording units with cameras and radar mounted to extended masts that allow on-board monitoring of surveillance images by an attending user. MSC covers a range of several miles under optimal conditions. MSC is deployed primarily in rural remote areas or other areas where no fixed surveillance technologies are deployed.
- Agent Portable Surveillance System (APSS) is a surveillance suite that includes cameras with a visual range for surveillance of several miles and ground radar that can be carried and used by Border Patrol Agents in areas where fixed and vehicle-mounted solutions are not feasible or appropriate.
- Ultra-Light Aircraft Detection (ULAD) is a mobile radar system that is being tested to detect and track small, low, or slow flying aircraft with a small radar cross section, known as ultra-light aircraft, in remote areas along U.S. borders. The ULAD system increases and enhances operators' ability to identify suspicious small aircraft[2] so that CBP can monitor possible smuggling routes and make an interdiction. The ULAD system tracks aircraft from entry to either landing or exiting the U.S. when aerial assets are not within response range. ULAD transmits

[2] Small aircraft refers to the ultra-light aircraft, which are essentially hang-gliders with an engine and a prop.

radar sensor data to the Air and Marine Operations Center (AMOC) in Riverside, CA and Border Patrol Sector Dispatch Centers. The AMOC also has remote control capability for the detection units.

Fixed Border Surveillance Systems

Fixed border surveillance systems are capable of collecting surveillance data from a dedicated location. A description of each of the fixed border surveillance systems follows:

- Tethered Aerostat Radar System (TARS) uses the aerostat (a large unmanned blimp or balloon) as a stationary airborne platform for surveillance radar. TARS detects and monitors low-altitude aircraft and vessels along the U.S.-Mexico border, the Straits of Florida, and a portion of the Caribbean in support of the Counter-Narcotics Program with the Department of Defense (DOD). The program's primary mission is to provide persistent, long-range, detection and monitoring of low-level air, maritime, and surface narcotics traffickers using radar detection. There are currently eight operational sites in the continental United States and Puerto Rico.[3] Some TARS are equipped with a video camera capable of assisting CBP users in detecting and tracking pedestrian and vehicular traffic; other sites monitor maritime traffic and relay CBP communications to facilitate interagency operations.
- Integrated Fixed Tower (IFT) sensor suites include towers with mounted day and night cameras and radar that can be monitored from a local CBP Border Patrol sector facility.
- Block 1 and Northern Border Remote Video Surveillance System (RVSS) provide automated day and night wide-area surveillance along the U.S. border using multiple color cameras and thermal infrared detection video cameras. CBP uses RVSS to detect and track illegal entries. The sensor images are transmitted via a dedicated communications system to a CBP facility where the information is processed and displayed.
- The Intelligent Computer Assisted Detection (ICAD) system operates a network of underground sensors and cameras installed along the U.S. border that detects the presence or movement of individuals and relays that information to U.S Border Patrol Sector Headquarters. ICAD records the date, time, and location of the activity, as well as details input by the Border Patrol Agent investigating the incident. Border Patrol Agents input details including name, date of birth, document number, license plate number, and other biographic data about individuals encountered through ICAD detections. The sensor data is stored and can be retrieved by date, time, or the PII that is included in the incident details.
- Law Enforcement Technical Collection (LETC) intercepts radio communications on HF, VHF, and UHF frequencies. LETC operators only collect radio communications in compliance with applicable laws, directives, and policies. CBP officials make notes of suspicious radio chatter including frequency used, location of transmission, code names, and code words to log suspicious

[3] The eight operational sites are: Yuma, AZ; Ft. Huachuca, AZ; Deming, NM; Marfa, TX; Eagle Pass, TX; Rio Grande City, TX; Cudjoe Key, FL; and Lajas, PR.

activity. No log entry is created if the activity is deemed not to be of law enforcement interest.

LETC log entries are retrieved by date, time, frequency, and location of the event. CBP does not retain the transmitted audio unless it is used in support of an ongoing law enforcement activity.

LETC supports the prevention of unauthorized entries by persons; interdiction of smuggled, hazardous material, and contraband; and it assists investigative efforts using a risk-based strategy.

The combination of fixed and mobile surveillance systems supports CBP's persistent and situational surveillance of the U.S. border at and between ports of entry. Sensor information may be relayed to a Border Patrol sector station, Headquarters, port of entry, or users at a fusion center to coordinate a response when available and where necessary to respond. Sensor information is displayed to authorized users at these locations based on their assigned duties and need to know.

CBP is better able to respond to and coordinate its interdictions and law enforcement responses to events at or near the border using the sensor technologies described in this PIA. CBP uses the Land Mobile Radio Network (LMR) to coordinate its response. LMR is a CBP internal radio network responsible for providing tactical communications, operational planning, radio network control services, and investigative information and intelligence services to support CBP operations, port of entry inspections, and other law enforcement activities as required. LMR records radio conversations between Border Patrol Agents in the field and dispatch operators.[4] The CBP Office of Internal Affairs uses audio logs to retrace the activity when investigating incidents involving Border Patrol Agents. The audio logs are kept for a period of seven days and then overwritten by the system unless the information is used in support of ongoing law enforcement investigations by the appropriate federal agency.

Border Patrol Agents may process the apprehension using a mobile processing center or at the sector station when CBP encounters individuals away from a port of entry. BSS users copy the video images and audio recordings from BSS to an archive to be used as law enforcement records and as evidence in any subsequent proceedings during processing. If an incident results in prosecution the authorized BSS users retrieve the BSS recording by the date, time, and device number and provide it to the investigating or prosecuting agency along with the related case file information. All physical transfers of data are recorded on a chain of custody form completed by the user performing the transfer.

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 BSS represent a reassessment of SBInet as authorized under the Secure Fence Act of 2006 and implementing regulations.[5] CBP uses BSS to perform its law enforcement missions under the

[4] Other federal and state agencies leverage this technology including the U.S. Department of Justice, U.S. Department of Interior, and the Massachusetts Criminal Justice Information Service to record and transport their radio conversations. However, the recordings are logically segregated from CBP recordings, and each agency does not have access to another agency's recordings.

[5] Pub. L. 109-367, 8 U.S.C. § 1707 Note and 8 CFR 287.

Immigration and Nationality Act of 1952, as amended, and other pertinent provisions of the immigration laws and regulations,[6] as well as pertinent provisions of the customs laws and regulations.[7] CBP collects information through BSS in conformance with the Electronic Communications Privacy Act of 1986, as amended, and the Communications Act of 1934, as amended.[8]

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

Audio and video recordings in BSS are not retrieved from the device or archive storage using a personal identifier, and therefore, do not constitute a system of records under the Privacy Act of 1974. However, video and audio recordings associated with an individual in a case file and retrieved by a personal identifier are covered under the associated system of records. For example, video associated with a law enforcement activity may 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;[9] DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE);[10] DHS/CBP-017 Analytical Framework for Intelligence System (AFI);[11] or DHS/ALL-020 Department of Homeland Security Internal Affairs.[12]

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

The BSS projects described above are in various stages of the system development life cycle. System Security Plans (SSP) have been completed for Block 1, Northern Border Remote Surveillance System, and Agent Portable Surveillance Systems. All others have system security plans in development.

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

No. CBP is developing a retention schedule for archive storage of BSS data for NARA according to the retention procedures described in 5.1, below.

---

[6] Pub. L. 82-414. *See, e.g.*, 8 U.S.C. §§ 1225 and 1357.
[7] *See, e.g.*, 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, and 1595a(d).
[8] 18 U.S.C. § 2510 *et seq*; 47 U.S.C. § 151 *et seq*.
[9] U.S. Customs and Border Protection TECS SORN, 73 FR 77778 (Dec. 19, 2008), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2008-12-19/html/E8-29807.htm.
[10] DHS/ICE-011 - Immigration and Enforcement Operational Records System (ENFORCE), 75 FR 23274 (May 3, 2010), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2010-05-03/html/2010-10286.htm.
[11] DHS/CBP-017 Analytical Framework for Intelligence System, 77 FR 13813 (June 7, 2011), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm.
[12] DHS/ALL-020 - Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014), *available at*, http://www.gpo.gov/fdsys/pkg/FR-2014-04-28/html/2014-09471.htm.

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.

The BSS does not collect information covered by the Paperwork Reduction Act.

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 as part of the program, system, rule, or technology being developed.

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

BSS collect various types of data that may include PII. Some of the information collected is stored and can be retrieved. Collected information includes:

Video recordings and still images: BSS use mobile and ground fixed cameras to routinely monitor remote border areas for suspicious activity or an unexpected presence. Some video cameras have night vision or thermal imaging capability for monitoring an area at night. The video records and tracks the presence of people illegally crossing the border and entering U.S. territory. Video recordings and still images derived from video recordings may become associated with PII in a case file.

Radio frequency transmissions: BSS intercepts radio communications on HF, VHF, and UHF frequencies used by terrorists and transnational criminal organizations for illicit activities. CBP officials make notes of suspicious radio chatter, including frequency used, location of transmission, code names, and code words to log suspicious activity. Log entries are not created if the activity is deemed not to be of law enforcement interest. LETC log entries are retrieved by date, time, frequency, and location of the event. CBP does not retain the transmitted audio unless it is used in support of ongoing law enforcement operations.

LMR: CBP logs all audio transmissions between Border Patrol Agents and dispatch operators to retrace the activity when investigating incidents involving CBP agents. An audio logging recorder is active at all CBP sector offices and the National Law Enforcement Communication Center (NLECC). The audio logging recording is used by Internal Affairs. Audio logs are kept for a period of seven days and then overwritten by the system unless the information is used in support of ongoing law enforcement investigations by the appropriate federal agency.

Under Ground Sensors: ICAD reads data sent by underground sensors to detect persons or vehicular movement across and along the border and relays the data to a Border Patrol station for a response. ICAD sensor data is stored in ICAD with associated incident details including PII about the persons encountered (name, phone number, address, make and model of vehicle, license plate number, driver's license number, etc.). The data collection, storage, usage, and retention is documented in the forthcoming ICAD SORN.

Radar: CBP collects radar data from MSC, APSS, ULAD, and TARS to detect and interdict aircraft, vehicles, vessels, and other conveyances in the border area and drug trafficking transit zones, such as the adjacent portions of the Caribbean Sea. This radar data does not contain PII, but may be used to locate and apprehend an individual illegally crossing the border. CBP uses MSC and APSS to detect individuals and conveyances moving over ground in remote areas, which may lead to an interdiction. ULAD detects the presence of small aircraft flying along the border. TARS provides persistent, long range, radar for detection and monitoring of low-level air, maritime, and surface contacts along the U.S.-Mexico border, the Straits of Florida, and adjacent portions of the Caribbean sea.

When BSS data is needed as evidence for prosecution, a BSS user retrieves the recorded incident information from the respective border surveillance system or archive based on the case file information (time/date/tower location number) and saves it to a DVD. CBP then controls the BSS data along with the case file information according to its "chain of custody" handling procedures for evidence.

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

CBP collects raw video, photograph, audio, ground sensor, and radar data using BSS in rural and populated areas at or near the U.S. border. Additionally, TARS collects radar data in adjacent portions of the Caribbean Sea.

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. BSS does not use information from public or commercial sources. Also, the BSS have no connections to public or commercial sources, such as the internet.

2.4 Discuss how accuracy of the data is ensured.

CBP captures BSS video, images, audio, ground sensor, and radar data in real-time to maintain a factual record of events. Accuracy is ensured by instructing users to adjust the recording equipment to increase a video image's resolution or sound quality from a microphone. CBP trains BSS operators to properly evaluate and ascertain which data is relevant and necessary to accomplish CBP's border securing mission before copying data off of a device or archiving an incident. This training ensures that the subject of the video or audio collection is within the scope of the defined mission. The alignment of the collection activity within the scope of the mission parameters becomes a critical factor for determining accuracy and relevance because the subject may be determined by an event or circumstance (such as presence at a "drop zone") instead of by identity. 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.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that BSS may capture information about individuals or activities that are beyond the scope of CBP's authorities. Video cameras can capture individuals entering places or engaging in activities as they relate to their daily lives because the border includes populated areas. For example, BSS may collect video of an individual entering a doctor's office, attending public rallies, social events or meetings, or associating with other individuals.

Mitigation: Cameras, radar, and other BSS are oriented toward the border and away from communities and places of worship and commerce frequented by local residents, when operationally feasible. While BSS records lawful activity at or near the border, these recordings are automatically overwritten unless an authorized BSS user determines the recording is needed for an approved purpose. Specifically, CBP copies and retains information from BSS only when it is relevant to an active case file for law enforcement or border security purposes. Additionally, CBP does not associate the recorded video or other data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation.

Privacy Risk: LETC users may listen to or record radio frequency communications between individuals engaged in activities with no law enforcement nexus.

Mitigation: CBP intercepts radio frequency communications near the border that may include communications with no law enforcement nexus; however, CBP is subject to applicable laws, directives, and policies so that log entries are not created and audio is not retained if the activity does not have a law enforcement nexus. CBP officers and agents receive training that addresses awareness of sensitivities arising in conversations, as well as determining associations between the topic of a conversation and a mission purpose. As with any information acquired as part of official responsibilities, CBP officers and agents may not disclose any information collected, unless authorized in accordance with DHS and CBP policy, and remain subject to the CBP Code of Conduct and relevant disciplinary procedures for any violation.

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.

CBP primarily uses information obtained from BSS to enhance border security and interdiction operations at the border. BSS users track the movement of individuals and incidents near the border and dispatch available Border Patrol Agents to provide operational support. CBP uses video surveillance to monitor a particular individual or location as part of a law enforcement investigation and may use the collected images as evidence in criminal proceedings in the event the individual is arrested. CBP uses radar and ground sensor data to detect and interdict persons illegally crossing the border. CBP's Internal Affairs uses LMR audio recordings to retrace events when an incident occurs with a Border Patrol Agent. LETC users note suspicious radio chatter to detect illegal activity at the border. CBP shares BSS 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 (e.g., TECS, Automated Targeting System-Targeting Framework, E3/ENFORCE).

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 Access, Uses, and Disclosure of Information

Mitigation: CBP employees only use BSS 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 is a violation of CBP's Code of Conduct and may subject an employee to disciplinary action, including termination of employment or prosecution.

Risk: There is potential risk of unauthorized access, use, or disclosure of video or audio recordings from BSS.

Mitigation: Access to BSS is limited to those specific CBP employees that must use the systems 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. All equipment and archives are stored in secure facilities with limited access. CBP does not share the information with any other component or agency unless it becomes evidence in a law enforcement investigation. Information sharing is compliant with the routine uses of the respective SORNs.

Section 4.0 Notice and Consent

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.

All persons entering the U.S. at and between the ports of entry are subject to monitoring and data collection for operational and situational awareness. CBP posts signs at ports of entry to notify

individuals of the monitoring and information collection requirements. CBP conducted an environmental assessment process prior to the implementation of the Integrated Fixed Towers that involved public hearings to raise awareness of the program and give the public an opportunity to comment on the location of fixed cameras and their use. This PIA also serves to inform the public generally 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 illegally.

CBP does not provide advanced notice for individuals encountered between ports of entry because entering the U.S without coming through a port of entry is illegal. It is logistically impracticable for CBP to give prior notice to persons seeking to cross the border at other than a port of entry; persons seeking to cross the border illegally are informed that their activities in the border area may be monitored and captured for use to enforce the law through the notice provided in this PIA and the associated SORNs.

4.2 Privacy Impact Analysis: Related to Notice

Risk: There is a risk that collected images 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 or provided consent.

Mitigation: Notice for persons at the ports of entry is provided at the ports. Notice for persons in the border area between the ports of entry is found in this PIA. As described above, CBP conducted public meetings before installing the Integrated Fixed Towers to allow for extended notice and comment from persons living in the immediate vicinity of the tower emplacements.

CBP does not obtain consent to use information pertaining to persons crossing the border as it 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 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. CBP mitigates this risk by strictly controlling the collection, use, and retention of information through BSS. Information that is not collected for a law enforcement purpose is deleted and is not used.

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

CBP does not provide opportunities for consent to monitoring and capturing an individual's image, radio frequency transmissions, or travel in the border areas due to the law enforcement and border security nature of the data captured through BSS surveillance activities at and between the ports of entry. Information collected by CBP that does not pertain to a law enforcement activity is deleted and is not used.

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.

BSS equipment may temporarily retain recordings or directly transmit them to an archive. Both the device and the archive overwrite data after a set period of time, as described below unless the recording is associated with a case file. CBP retains recordings associated with a case file for the retention period of the case file, including proceedings associated with a case file. The retention schedule of the applicable case management system will apply to the associated BSS information once a case has been closed.

Video recordings are stored on the device for varying amounts of time, typically between seven and 30 days before being overwritten. CBP copies the video to an archive and has proposed retention of video recordings for 45 days in an archive before being purged, unless the video is useful for training purposes or is associated with a case file. CBP may keep recordings that are useful for training purposes for up to one year.

LMR audio logs are retained for seven days before being overwritten unless it is needed for and associated with a law enforcement investigation or incident.

Ground sensor data is retained along with incident details according to the ICAD SORN retention period, which is proposed for up to 15 years.

Radar data are not retained unless they are associated with a case file.

Radio frequency transmissions are not retained unless they are used in support of ongoing law enforcement operations and associated with a case file.

5.2 Privacy Impact Analysis: Related to Retention

Risk: There is the risk that surveillance video and recordings may be retained in BSS for a longer period than required by the purpose for which the video and images were collected.

Mitigation: CBP automatically overwrites video that is not needed and identified for an authorized training purpose or for a specific law enforcement investigation or incident to minimize the risk of excessive data retention. Videos used for training are marked and purged after one year. All other recordings that are not associated with a person will be automatically purged within 45 days. CBP identifies and associates recordings with persons to pursue its several law enforcement missions at the border; in these matters the recordings are maintained in association with the respective case management system holding the associated law enforcement matter about the person. CBP maintains recordings in these instances in accordance with the retention period for the respective case management system.

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 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 shares non-PII radar data with the DOD as part of the joint Counter-Narcotics Program. When CBP identifies a possibly illicit radio frequency transmission, CBP provides non-PII notes from the transmission (frequency band, time, date, and location) to the Federal Communications Commission (FCC) and the Drug Enforcement Agency (DEA) for their law enforcement purposes.

CBP does not ordinarily share video or audio outside of CBP. Rather, CBP typically shares information derived from BSS with other law enforcement agencies assisting CBP in an interdiction or law enforcement operation. For example, a BSS user watching a video camera may relay "three suspects are running towards a blue truck near the intersection of X and Y" with local law enforcement on the scene to coordinate the interdiction. CBP provides the video or audio extract as part of the case file shared with federal law enforcement (e.g., Department of Justice) in the event surveillance information results in an arrest and subsequent prosecution.

CBP shares audio or video recordings 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) when an audio or video recording from BSS is associated with a system of records. CBP documents the disclosure on a Form DHS-191 when BSS information is shared in conjunction with PII from a system of records. CBP conditions the disclosure to the receiving agency 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 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 may disclose the information pursuant to the routine uses outlined in the appropriate case file SORN when BSS information is associated with PII in a system of records. For example, video may be shared with local law enforcement to assist with a law enforcement investigation if the video is associated with a case file in:

- TECS pursuant to routine use G, which states, "To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines

that the information would assist in the enforcement of civil or criminal laws."[13]

- Internal Affairs pursuant to routine use G, which states, "To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure."[14]
- ENFORCE pursuant to routine use G, which states, "To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure."[15]
- AFI[16] pursuant to routine use H, which states, "To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, agreement, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws. This routine use applies only to finished intelligence products."[17]

Normally, the requesting agency seeks the information through a Request for Information (RFI), to which CBP responds. The terms of this response discuss the need and authority identified by the requesting agency for use of the information; it then relates those terms to the purpose for which CBP collected and maintains the information under its specific SORN (for example, a DEA request for information pertaining to drug trafficking maintained in a law enforcement case management system). The response notes that CBP requires consultation with respect to further dissemination of the shared information beyond the receiving agency so as to ensure accountability for the collected information.

6.3 Does the project place limitations on re-dissemination?

Yes. CBP only shares video or audio when the requesting agency has an official need to know and agrees to limit re-dissemination by first obtaining approval from CBP, regardless of whether it is associated with a system of records. CBP responds to requests for information or assistance by providing

[13] DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR, 77778 (Dec. 19, 2008).
[14] DHS/ALL-020 Department of Homeland Security Internal Affairs 79FR 23361 (April 28, 2014).
[15] DHS/ICE-011Immigration and Enforcement Operational Records System (ENFORCE) 75 FR 23 274 (May 3, 2010).
[16] DHS/CBP/PIA-010 Analytical Framework for Intelligence (AFI) PIA, *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf.
[17] DHS/CBP-017 Analytical Framework for Intelligence System (AFI) 77 FR 33753 (June 7, 2012).

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.

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. The form requests the date, nature, purpose of each disclosure, and the name and address of the individual agency to which disclosure is made. *Ad hoc* requests not associated with information from a system of records must be approved by the appropriate Program Director and documented locally.

6.5 Privacy Impact Analysis: Related to Information Sharing

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

Mitigation: 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 BSS data 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 BSS data associated with an individual in an automated fashion. CBP will develop a written arrangement (e.g., Memoranda of Understanding (MOU) or Information Sharing Access Agreement (ISAA)) that would 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 conformed to CBP's use, security, and privacy considerations before releasing information.

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?

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

Individuals seeking notification of, and access to any record contained in BSS, in a system of

records containing data from BSS, or seeking to contest its content may gain access by filing a 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
FOIA Division
90 K Street NE, 9th Floor
Washington, D.C., 20229-1181
Fax Number: (202) 325-0230

Most BSS data is not accessible under the Privacy Act of 1974 because BSS data on the device or in an archive is not retrievable by personal identifier. However, CBP provides individuals access to BSS data according to the applicable SORN when CBP associates BSS data with an individual by linking it to a case file in a system of records. There may be occasions when BSS information is covered by a SORN and DHS exempts the information from individual access or amendment provisions of the Privacy Act. This occurs if access to the data could inform the subject of an investigation of the existence of the investigation or reveal investigative interest on the part of DHS or another agency. Access to the CBP-held records could also be denied if such access might permit the individual who is the subject of a record to impede an investigation, tamper with witnesses or evidence, and avoid detection or apprehension. In other cases individuals may be able to gain access to the data pertaining to them.

CBP reviews all such requests on a case-by-case basis, notwithstanding the applicable exemptions. CBP may waive the applicable exemption and provide access to BSS data if it does not interfere with or adversely affect the national security of the United States or activities related to any investigations associated with the BSS data.

Further, individuals may contest information collected through BSS if it is used as evidence in any immigration or criminal proceedings that result from the encounter.

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

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

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 www.cbp.gov.

7.4 Privacy Impact Analysis: Related to Redress

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

Mitigation: 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 BSS data 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 he or she is erroneously associated with BSS data.

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?

Handling the information that is collected by the BSS is governed by standard operating procedures and policies. Only authorized users have the ability to extract materials from the systems. CBP mitigates the risk of misuse of data collected by, and accessed through BSS by maintaining audit trails, including (at a minimum): user name, access date and time, and functions and records addressed. CBP also requires users to conform to appropriate 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 BSS users undergo initial security awareness training and complete the DHS online security awareness-training course and a privacy awareness course on an annual basis.

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 who operate BSS receive training on proper use of the systems and handling of any evidentiary data that may be extracted from the system. All first time users must take a two-day Security Awareness Training provided on the surveillance systems. Users may only request an access account after they have completed the two-day training. The trained user submits account creation forms requiring him or her to provide proof of security awareness training and sign an agreement to abide by the system rules of behavior. The system maintains a log of activities for auditing purposes. CBP program managers and supervisors must authorize each employee to perform certain functions related to BSS. Only authorized personnel are able to delete or add records before or after storage in an archive. For example, while each monitoring user has the ability to operate the surveillance cameras and save eventful surveillance video to the archive server, only the on-duty Video Retention Coordinator may delete video files. Users may not remove or download data from the archive server without authorization and in conjunction with assistance from the aforementioned Video Retention Coordinator. 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 BSS, are created by the operational owner of the system and are 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.

Responsible Officials

Laurence Castelli
CBP Privacy Officer
U. S. Customs and Border Protection
(202) 344-1610

Douglas Harrison
Associate Chief, Office of Border Patrol
U.S. Customs and Border Protection
(202) 344-2050

Sonia Padilla
Executive Director, Program Management Office
U.S. Customs and Border Protection
Office of Technology Innovation and Acquisition
(571) 468-7500

Approval Signature

Original signed and on file with the DHS Privacy Office

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security