Privacy Impact Assessment Update
for the

Border Surveillance Systems (BSS)

DHS/CBP/PIA-022(a)

August 21, 2018

Contact Point
Scott Luck
Deputy Chief, U.S. Border Patrol
U.S. Customs and Border Protection (CBP)
(202) 344-2050

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

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) deploys Border Surveillance Systems (BSS) to provide comprehensive situational awareness along the United States border for border security and national security purposes, and to assist in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. BSS includes 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 updating this PIA to assess the privacy risks associated with new border surveillance technologies not addressed in the original PIA, including maritime and ground radar, enhanced video capabilities, seismic and imaging sensors, and the use of commercially available location data to identify activity in designated areas within near the United States border.

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, customs, counterterrorism, and narcotics enforcement laws. Border Surveillance Systems (BSS) are a combination of surveillance technologies designed to assist CBP in enforcing U.S. laws and detecting, identifying, apprehending, and removing persons and contraband illegally entering the United States at and between ports of entry. BSS may also monitor individuals in a particular border location as part of a law enforcement investigation, and may be used as evidence if the apprehension of the individual results in criminal or administrative proceedings. BSS are located across urban, rural, and remote areas along the U.S. border and include tethered aerial video, ground radar, commercially available maritime radar, mobile and fixed ground video with day and night thermal capabilities, unmanned ground sensors, radio frequency sensors, seismic sensors, imaging sensors, low-flying aircraft detection, and acoustic sensing devices. CBP deploys various types of surveillance technologies depending on the surrounding terrain and population.

Reason for the PIA Update

As threats and enforcement challenges continue to evolve, CBP has updated its border surveillance capabilities since the previously issued 2014 BSS PIA[1] and has deployed new technologies such as the mobile, fixed, and other technologies listed below. Since the previously issued 2014 BSS PIA, CBP has made the following updates to its surveillance systems:

[1] DHS/CBP/PIA-022 Border Surveillance Systems (BSS), *available at* www.dhs.gov/privacy.

New Surveillance Technologies:

1. Mobile Surveillance Technologies:
    - Tactical Aerostats (TAS);
    - Lightweight Counter-Mortar Radar / Lightweight Surveillance and Target Acquisition Radar (LCMR/LSTAR); and
    - Man-Portable Aerial Radar System-Kit (MARS-K).
2. Updated Fixed Surveillance Technologies:
    - Integrated Fixed Towers (IFT) integration with the Tracking Signcutting Modeling (TSM).
3. Other new surveillance technologies:
    - Cross Border Tunnel Threat (CBTT) Program;
    - Border Tunnel Activity Detection System-Point (BTADS-P);
    - Linear Ground Detection System (LGDS);
    - National Intrusion Sensor Infrastructure (NiSI)/Unattended Ground Sensors (UGS);
    - Maritime Surveillance Technology; and
    - Commercially available location data.

Dispositioned surveillance technologies

In addition to these new projects, CBP is no longer using the following systems that were outlined in the original BSS PIA:

- Low Flying Aircraft Detection (LFAD);
- Mobile Surveillance System (MSS); and
- Ultra-Light Aircraft Detection (ULAD).

New Mobile Border Surveillance Systems

Mobile border surveillance systems can be moved and relocated to collect data from various locations to meet changing mission needs. In addition to the mobile systems described in the original BSS PIA, CBP has deployed the following new mobile technologies:

Tactical Aerostats (TAS)

CBP deploys aerostats[2] (airships or hot-air balloons, usually tethered, that can be moved to different locations) that are equipped with persistent radar, motion imagery, and day/night video surveillance technologies. Aerostats are tethered but re-locatable and look similar but differ in size, operate at different altitudes, and provide varying surveillance coverage. The U.S. Border Patrol (USBP) uses TAS to surveil the ground border to assist CBP in detecting, identifying, apprehending, and removing narcotics traffickers and individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law within a reasonable distance of the border.[3]

Information generated and processed by the TAS includes recorded surveillance or still images of a specified area along the U.S. border that may include suspected illegal activities that require USBP intervention.

Lightweight Counter-Mortar Radar / Lightweight Surveillance and Target Acquisition Radar (LCMR/LSTAR)

LCMR/LSTAR is a self-contained, easily transportable, network-enabled radar technology. CBP developed the LCMR/LSTAR system to fill critical air surveillance gaps. Its 3-D and 360 degree electronic scanning capability enables detection and tracking of difficult targets, including low altitude and slow flying small aircraft, such as ultralights, para-gliders, hang-gliders, and unmanned aerial vehicles (UAV) flying illegally from Mexico into the southwestern United States. LCMR/LSTAR's Doppler processor and electronically-scanned antenna allows it to detect slow speed aircraft in the presence of clutter. Radar captured via LCMR/LSTAR is transmitted to the Air and Marine Operations Center (AMOC)[4] in Riverside, California via OneNet. Radar activity along the U.S. border may capture illegal activity requiring CBP intervention.

Man-Portable Aerial Radar System-Kit (MARS-K)

MARS-K is a two-man portable system that uses an X-band Doppler air and ground radar system to provide up to 360 degrees scan rate (one scan every 4 seconds). The MARS-K comes in

[2] Aerostat is defined as an airship or hot-air balloon, especially one that is tethered.
[3] Pursuant to 8 U.S.C. § 1225(d)(1), CBP agents "are authorized to board and search any vessel, aircraft, railway car, or other conveyance or vehicle in which they believe aliens are being brought into the United States." Under 8 U.S.C. § 1357(a)(3), CBP agents are also authorized "within a reasonable distance from any external boundary of the United States, to board and search for aliens any vessel within the territorial waters of the United States and any railway car, aircraft, conveyance, or vehicle…" By regulation, "a reasonable distance" is currently defined as 100 air miles (8 C.F.R. § 287.1(a)(2)).
[4] The Air and Marine Operations Center (AMOC) is an international, multi-domain, federal law enforcement operations center that strengthens the execution of CBP's global mission. The AMOC targets all threats, primarily in the non-commercial aviation and maritime domains with an emphasis on the aircraft and vessel approaches to the U.S. border, Mexico, Canada, the Bahamas, Puerto Rico, and the Virgin Islands, as well as criminal activity internal to the United States.

two backpacks/rucksacks, each weighing approximately 60 pounds. The system has the capability to detect and track small unmanned air targets and ultra-light aircraft as well as provide detection and tracking of ground targets. MARS-K track data is displayed locally on a portable laptop. MARS-K does not have a camera. MARS-K data is not transmitted or ingested into another CBP system. Radar recordings are retrievable by date of occurrence, time, and asset used.

Updated Fixed Border Surveillance Systems

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

Integrated Fixed Towers (IFT)

CBP deploys IFTs, or fixed tower sensor suites with mounted day and night cameras, radar, and laser illuminators sensors that can be monitored from a local USBP sector facility. IFTs, which resemble radio towers, provide camera surveillance from fixed locations with remote pan and tilt, zoom and focus capabilities, and common operating picture (COP)[5] that facilitate situational awareness to USBP Agents in the field. The IFT systems have been deployed in Arizona along remote sections of the Southern border to fill in the gaps of uncovered areas. IFT surveillance cameras record border incursion activity (from a distance between 0.5 to 7 miles range, without facial recognition capability) allowing USBP to track and interdict illegal border entrants. Since the publication of the 2014 BSS, IFT has been enhanced to share information with CBP's Tracking, Sign-cutting, and Modeling (TSM) tool. The IFT system surveillance video is handled in the same manner as other BSS and may share geospatial data and still images with the TSM tool.

Other New Border Surveillance Systems

In addition to mobile and fixed border surveillance systems, CBP has deployed a number of other border surveillance projects, described below:

Maritime Surveillance Technologies

While the majority of technologies described in this PIA are in use along the land border, CBP has also deployed both mobile and fixed surveillance in the maritime environment. Several maritime surveillance capabilities are currently located off the coast of California and at the international border on the eastern end of Lake Erie and the western part of Lake Ontario. CBP's maritime projects rely on commercially available maritime radar, video cameras, communications, and remote command and control systems to automatically detect and track watercraft of various sizes crossing between international waters and U.S. waters and shorelines. Sensor images and radar are transmitted via a dedicated communications system to a CBP facility where the

[5] Common Operating Picture (COP) is a central hub that receives data from one or multiple tower units. The tower systems automatically detect and track items of interest, and provide the COP operator(s) with the data, video and geospatial location of selected items of interest to identify and classify them.

information is processed and displayed. The objective of these maritime surveillance projects is to assess the effective range, detection performance, camera performance and multimodal communication technologies currently available. If successful, CBP may deploy additional mobile and fixed maritime technology in other areas to help CBP to detect and track suspicious activity and targets of interest, enabling CBP and its partners to identify, classify and interdict threats in the maritime environment.

Cross Border Tunnel Threat (CBTT) Program

The purpose of the CBTT program is to strengthen border security between the ports of entry by diminishing the ability of Transnational Organized Crime (TOC) networks and other actors to gain access into the United States through cross-border tunnels and the illicit use of underground municipal infrastructure (UMI) (e.g., sewer system). The CBTT program is made up of a network of subterranean ground sensors that collect seismic information that may detect people walking near the border, climbing over the border fence, or digging near the CBTT program sensing devices, as well as vehicles and animals near the U.S. border, and low-flying aircraft crossing the U.S. border. CBTT program sensors are able to detect, classify, and localize activity providing enhanced surveillance in areas where other technologies are hindered by terrain, foliage, or sustainability, by combining existing point and linear seismic monitoring, electromagnetic/gravity imaging, and automatic signal detection and classification capabilities. CBP uses CBTT to predict potential tunnel locations, detect the presence of suspected tunnels and tunneling activity, and confirm the existence and location of a tunnel through mapping and measurements. CBTT sends alarms and sensor data to USBP Agents working at the local CBP Station Command and Control Center. CBTT program alarms and sensor data will appear on an Intelligent Computer Aided Detection (ICAD)[6] system display, allowing the operators to identify where the alarm occurred and perform quality analysis before notifying USBP Agents in the field to respond.

National Intrusion Sensor Infrastructure (NiSI)/Unattended Ground Sensors (UGS)

The National Intrusion Sensor Infrastructure (NiSI) is CBP's ground-intrusion alarm system. NiSI is a national-scale, long-term, physical intrusion detection system that includes detection monitoring, logging, and management components. The NiSI system employs a network of UGS (which include environmental sensors, equipment health sensors, communication equipment, and related equipment) to detect suspicious activity and allow rapid response to changes in risk along the U.S. border. UGS is an overarching term used to describe unattended ground sensors that include seismic, acoustic, magnetic, and day/night cameras that are used to automatically detect persons or vehicles and transmit activity reports or images via radio-frequency or satellite communications to the CBP ICAD system. In addition, NiSI UGS trigger or

[6] *See* the original BSS PIA provides a description of the ICAD system; *available at* www.dhs.gov/privacy.

queue large platform surveillance and provide notification of areas requiring USBP agents to respond and resolve. NiSI UGS also confirm inactivity in areas believed to have effective impedance and denial[7] measures by providing CBP with situational awareness and persistent surveillance.

As part of the NiSI, the USBP UGS program includes a broad range of remotely monitored surveillance systems emplaced in areas where there is generally no persistent presence of CBP personnel in the immediate vicinity of the device. USBP agents nearby receive notification of a NiSI UGS alarm and prioritize their response. Under typical circumstances, NiSI UGS are covertly placed along the U.S. border, and are generally concealed above, or immediately below the ground. NiSI UGS are ground-based surveillance as opposed to aerial, cyber, or marine surveillance, but NiSI UGS may include some capabilities to detect activity in close proximity to the ground or in areas immediately off shore. While the majority of CBP's NISI UGS are deployed outdoors, some devices may also be located in other public spaces or locations to which CBP has access, such as on or inside buildings and structures; inside culverts, sally ports, alleys, passages, and underpasses; inside caves, crevices, or other natural enclosed spaces; and inside tunnels or UMI and similar environments. Specifically, NISI UGS are used to monitor the border environment for increased risk and changes in the threat environment, to detect illicit vehicle, pedestrian, underground, and in some cases, vessel and aircraft traffic, and to track activity across related detections so that CBP may record the event and respond appropriately.

Sensor activations are transmitted from the NiSI UGS to USBP sector dispatch centers monitored by USBP Sector Enforcement Specialists (SES), who view the signals via the ICAD system. NiSI UGS systems may capture point clouds,[8] photos, and video clips of the immediate vicinity, which may include recognizable faces of individuals and other data such as vehicle license plate information. USBP SES personnel monitor ICAD and contact USBP agents in the field to alert them to sensor activations in their area of responsibility (AOR). USBP responds to the location of the sensor activations as appropriate to investigate the source of the activation and determine if an incursion has taken place. Once it has been determined that an incursion has taken place, USBP will take action to resolve the situation in an expedient manner by attempting to interdict and apprehend the source of the incursion.

Commercial Location Data - Data as a Sensor

CBP may use commercially available location data acquired from a data provider in order to detect the presence of individuals in areas between Ports of Entry where such a presence is

[7] Impedance and Denial refers to the ability to impede border incursions and deny the use of terrain (i.e., land, air, water) for advantage in conducting illegal activity and acts of terrorism, primarily through the use of man-made walls/barriers/fencing and the deployment of fixed and mobile surveillance systems and USBP personnel.
[8] A point cloud is a collection of data points defined by a given coordinates system. In a 3D coordinates system, for example, a point cloud may define the shape of some object.

indicative of potential illicit or illegal activity. The goal is to utilize this data to detect the presence of – but not identify – individuals in an area which CBP has identified as an area of interest, consistent with CBP statutory authorities, federal law, and DHS policy. Data from such datasets is compiled by a third-party provider from multiple commercial sources and anonymized, offered for purchase, and can then be acquired by public or private entities, including CBP. The information purchased by CBP may include location, time, date, a randomly generated unique ID for a given entity, and resolution of the number of entities (i.e., whether the signal indicates 1 person traveling in a line, or 100 people at singular points in a row). CBP will retain this data for periods of time, consistent with existing privacy policies, in order to identify patterns that are relevant to mission operations, such as a track that is indicative of a new illegal border crossing trail, or for identification of trends of certain seasonally utilized illegal transit routes.

The data CBP receives will be fully anonymized by the data provider and will not be attributable to an individual. If this location data leads to an enforcement action based upon violations of U.S. law, CBP may retain the applicable originating location data derived through this process. In addition, the randomly generated unique ID associated with a given entity will not persist indefinitely. Rather, the unique ID will be regenerated at intervals dictated by established CBP privacy policies to enable tracking of a data source long enough to determine that the information was emanating from one source/person over a period of time rather than several individuals in the same vicinity. CBP will analyze this data to identify areas where CBP may limit acquisition of the data to avoid any unnecessary collection (for example, along interstates or other areas used for primarily legitimate purposes).

Small Unmanned Aerial System (SUAS)

In addition to the aforementioned border surveillance systems, CBP recently provided public notice of its use of small unmanned aerial systems (SUAS), which may be equipped with border surveillance technologies including video surveillance systems, rangefinders, thermal imaging devices, radar, and radio frequency sensors. SUAS is a rapidly deployed air surveillance capability that provides CBP with ground detection capabilities, especially in remote areas along the U.S. border where challenging terrain and limited air-surveillance support exist. SUAS and the tools they support assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between the ports of entry or otherwise violating U.S. laws enforced or administered by CBP, such as narcotics and human smuggling. CBP provides a thorough description of its use of SUAS and the associated privacy risks in the Aircraft Systems PIA.[9]

[9] *See* DHS/CBP/PIA-018(a) Aircraft Systems, *available at* www.dhs.gov/privacy.

Dispositioned Surveillance Systems

CBP is no longer using the following systems that were outlined in the original BSS PIA publish in 2014:

- Low Flying Aircraft Detection (LFAD): CBP used LFAD to detect, track, and classify low flying aircraft along the northwest border. It used multi-modality sensors (radar, acoustic, and electro-optical/infrared, or EO/IR) and provided autonomous, all weather, 24/7 operations, delivering live air picture, data manipulation, and visualization capabilities to multiple users. Live LFAD sensor data (radar, acoustic, and EO/IR) was collected and transmitted to CBP. The LFAD radar detection units did not collect or retain information on individuals. CBP decided to cease its operation of LFAD in 2017 and destroyed all data collected by the LFAD system data with the decommissioning and repurposing of the system components.
- Mobile Surveillance System (MSS): The MSS platform consisted of a combination of electronic surveillance sensors and cameras that enhanced CBP's ability to detect, assess and ultimately apprehend individuals who were attempting to enter the United States illegally. Each recording or still photo capture was stored locally on each MSS system component as a file. Recordings and images were retrievable by date of occurrence, asset used, and number of individuals apprehended. Recorded surveillance images and sensor activity were not associated with any individual unless the images and sensor activity became linked to an investigation as a result of a law enforcement event. CBP dispositioned MSS in 2017 and purged all data from the platform.
- Ultra-Light Aircraft Detection (ULAD): Like LFAD, the purpose of ULAD was to provide CBP with the persistent detection and tracking of small, slow, and low flying aircraft with a small radar cross section, such as ultra-light aircraft, along U.S. borders. CBP decommissioned ULAD and destroyed the ULAD data in 2015.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

CBP's use of these new surveillance technology in accordance with the authorities specified in 2014 BSS PIA. Specifically, CBP uses BSS to perform its statutory duties[10] and law enforcement missions under the Immigration and Nationality Act, as amended, and other pertinent provisions of the immigration laws and regulations,[11] as well as pertinent provisions of the customs

[10] *See, e.g.*, 6 U.S.C. § 211.
[11] Pub. L. 82-414. *See, e.g.*, 8 U.S.C. §§ 1225 and 1357.

laws and regulations.[12] 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.[13]

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 recordings associated with an individual in a case file and retrieved by a personal identifier are covered under the associated system of records. Since the last PIA, CBP has issued a new System of Records Notice (SORN) for Border Patrol Enforcement Records (BPER),[14] which provides coverage for any information associated with enforcement events occurring between the Ports of Entry. In addition, 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.[15]

Characterization of the Information

BSS collect various types of data that generally do not contain PII, but may still relate to an individual. If an apprehension occurs, CBP may record personally identifiable information related to these individuals is recorded in the E3[16] system. CBP's newest border surveillance technologies collect, process, and maintain the information outlined below:

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 capture images of individuals and may become associated with PII in a case file.

Unattended Ground Sensors: This update to the BSS PIA covers in detail the different categories and sub-categories of NiSI UGS deployed by CBP. NiSI UGS are ground-based surveillance as opposed to aerial, cyber, or marine surveillance, but some NiSI UGS are capable of detecting activity in close proximity to the ground or in areas immediately off shore. While the majority of CBP's NiSI UGS are outdoors, the devices may also be deployed in other public spaces or locations to which CBP has access, such as on or inside buildings and structures; inside culverts, sally ports, alleys, passages, and underpasses; inside caves, crevices, or other natural enclosed spaces; and inside tunnels or underground municipal infrastructure (UMI) and similar environments. ICAD reads data sent by UGS to detect persons, vehicular or vessel movements,

[12] *See*, *e.g.*, 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, and 1595a(d).
[13] 18 U.S.C. § 2510 *et seq*; 47 U.S.C. §151 *et seq*.
[14] DHS/CBP-023 Border Patrol Enforcement Records (BPER), October 20, 2016, 81 FR 72601.
[15] DHS/CBP-011 U.S. Customs and Border Protection (TECS), December 19, 2008 73 FR 77778.
[16] *See* DHS/CBP/PIA-012(a) CBP Portal (E3) to EID/IDENT, *available at* www.dhs.gov/privacy.

and even low flying aircraft that across along the U.S. border and based on the type of UGS, may relay the data to a USBP facility for a response. UGS 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 of this data is documented in the BPER SORN.

Radar: CBP collects radar data from fixed and mobile surveillance systems to detect and interdict aircraft, vehicles, vessels, and other conveyances in the border area, including the maritime environment. CBP uses this technology to detect individuals and conveyances moving over ground in remote areas, which may lead to an interdiction. In addition, BSS may detect the presence of small aircraft flying and provide persistent, long range radar for the detection and monitoring of low-level air, maritime, and surface contacts along the U.S. border. In the case of its maritime surveillance systems, CBP uses commercially available maritime radar to monitor vessels along the shoreline and in the Great Lakes area.

Location Data: CBP receives commercially sourced location data when an individual enters the designated area of interest; however, CBP does not retain any personally identifiable information from this transmission, and only retains the original location information in the event of an interdiction.

CBP may use commercially available location data under the following conditions:

- A commercial dataset is available for purchase by private and/or public entities;
- The commercial dataset is anonymized, or can be anonymized before being provided to CBP so as to not contain PII;
- The terms of service under which the data was collected discloses that the data may be sold to a customer base that includes public sector customers, and the user must accept the terms of service prior to using / accessing a service or product; and
- The data will be used in support of the CBP mission pursuant to CBP's statutory authorities and applicable regulations.

These types of data sources would be used to identify the presence, but not the identity, of individuals within the border area.

Since the publication of the 2014 BSS PIA, there has been no change to how CBP ensures the accuracy of the BSS data. CBP captures BSS video, images, unattended ground sensors, 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 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.

Privacy Risk: There is a risk that BSS may capture information about individuals or activities that are beyond the scope of CBP's authorities. For example, BSS may inadvertently capture information outside of a reasonable distance from the border, or from individuals engaged in First Amendment protected activities.

Mitigation: This risk is mitigated in that CBP's deployment of surveillance technologies strictly within a reasonable distance of the border is consistent with its authorities to monitor and secure U.S. borders. 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: There is a risk that CBP may incidentally collect information from individuals who are complying with the law and are not subjects of interest.

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

Privacy Risk: There is a risk that CBP will receive and retain personally identifiable information from commercial sources related to individuals who have entered an area which CBP has identified as an area of interest.

Mitigation: This risk is fully mitigated. CBP receives only anonymized data from commercial sources. Similar to other border surveillance methods, this information allows CBP to take action solely based on information indicating the presence of an unidentified individual or group of individuals, with no associated PII. CBP only uses the location indicator to identify anomalous activity and as a lead to inform the deployment of resources, and obtains PII from the individual only pursuant to a subsequent encounter or enforcement activity.

Privacy Risk: There is an over-collection risk associated with CBP's deployment of UGS on government owned buildings and installations.

Mitigation: This risk cannot be fully mitigated. CBP policy requires the monitoring of all Government owned buildings and installations (e.g., LAN rooms, repeater sites and sensitive equipment storage facilities). CBP deploys UGS and other surveillance technology to monitor CBP facilities, thus providing CBP with persistent surveillance and situational awareness at and around the facility. Over-collection is minimized by the fact that CBP does not always deploy UGS which are capable of capturing video and still images. Instead, CBP may deploy seismic or infrared capable UGS to notify CBP personnel that individuals are in the vicinity of the facility. This risk is further minimized by the use of signage that gives notice that the facility is under surveillance.

Uses of the Information

Since the publication of the 2014 BSS PIA, there has been no change to how and why CBP uses the information collected by BSS. CBP 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 CBP personnel 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. When BSS data is needed as evidence for investigation or 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 portable media (e.g., a DVD). CBP then controls the BSS data along with the case file information according to its "chain of custody" handling procedures for evidence.

Notice

This PIA provides notice of CBP's use of new surveillance technologies, including commercially available location data. Such data is originally obtained from users who consent to the collection of their location data to a third party provider, per the provider's terms of service The third party requires that the terms of service discloses that the dataset may be sold to a customer base that includes public sector customer. While the third party privacy policy outlines how their customers may use the information, and this policy specifically mentions law enforcement purposes, it is possible that users are unaware of this use case, since they may not know to whom specifically the application provides their data.

For all other border surveillance technologies, the same issues outlined in the original BSS PIA related to notice continue to apply. All persons entering the United States 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 (IFT) 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. While it is logistically impractical for CBP to provide notice to individuals seeking to cross the border between the ports of entry, this PIA and the associated SORNs serve 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.

Privacy Risk: There is a risk that individuals will not know that a third party may provide their location to CBP.

Mitigation: This risk cannot be fully mitigated because it cannot fully control the point of collection. While CBP is publishing this PIA to provide generic notice of this program, and while users consent to the terms of service that include the provision of location data to third parties, these terms do not specifically make mention of CBP or any other customer. As with other border surveillance technologies, CBP cannot reasonably provide notice to individuals attempting to cross the border between ports of entry. Further, because crossing between the ports of entry is itself a violation of law, and activity in these areas are often indicative of other crimes, efforts on CBP's part to provide notice at the time of collection might impede investigative and interdiction efforts. However, CBP mitigates the impact of these risks by ensuring that it only receives anonymized data, and only in areas that are suspected of being associated with criminal activity and where the likelihood of encountering other lawful activity is minimal.

Privacy Risk: There is a risk to individual participation, since individuals subject to CBP surveillance activities are not able to opt out.

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

Data Retention by the project

There has been no change to CBP's retention of BSS data. As reported in the 2014 PIA, 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.

Information Sharing

Since the publication of the 2014 BSS PIA, there has been no change to the internal and external sharing and disclosure of BSS data. CBP continues to share 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.

Redress

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)), and the Judicial Redress Act, if applicable.

Any individual, regardless of citizenship or immigration status, may seek notification of and access to any CBP record pursuant to procedures provided by FOIA, and can do so by visiting https://www.cbp.gov/site-policy-notices/foia , or by mailing a request to:

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

When seeking records about one's self from any of the system of records applicable or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information. The individual must first verify his or her identity, meaning that the requestor must provide his or her full name, current address, and date and place of birth. The requestor must sign his or her request, and the signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While an inquiry requires no specific form, forms may be obtained for this purpose from the DHS Chief Privacy Officer and DHS Chief FOIA Officer, https://www.dhs.gov/freedom-infomration-act-foia, or 1-866-431-0486. In addition, the request should:

- Explain why the requestor believes the Department would have information on him or her;

- Identify which component(s) of the Department the requestor believes may have requested information about him or her;
- Specify when the requestor believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS Component agency may have responsive records.

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

There have been no changes to individual participation since the 2014 PIA. A traditional approach to individual participation is not always practical for CBP due to its law enforcement and national security missions. Providing notice and consent of border surveillance systems would interfere with the U.S. government's ability to protect its borders and diminish the effectiveness of CBP's law enforcement efforts, thereby lessening our overall national security.

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

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

Privacy Risk: Due to the law enforcement nature of the information collected by BSS and maintained in E3 or another case management system, there is a risk that individuals will not be able to access, correct, or amend their records since the records are exempted from access, correction, and amendment under the Privacy Act.

Mitigation: This risk is partially mitigated. Information from certain CBP source systems may be amended as indicated in the applicable SORN. However, providing individual access or correction of records may be limited for law enforcement reasons, including as expressly permitted by the Privacy Act. Permitting access to the records could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations

and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Privacy Risk: With the cancellation of the DHS "Mixed Systems" policy[17] through DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, there is a risk that persons other than U.S. Citizens and Lawful Permanent Residents are now unable to access, correct, and amend their information as they were previously able to do.

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

If an individual believes that CBP actions are the result of incorrect or inaccurate information, then inquiries may be directed to:

CBP INFO Center
U.S. Customs and Border Protection
1300 Pennsylvania Avenue N.W.
Washington, D.C. 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 may be asked to provide additional identifying information to enable DHS to identify the record(s) at issue.

CBP provides general notice on its public-facing website about the procedures for submitting FOIA and Privacy Act requests and via the Federal Register. In addition, this PIA and the Applicable SORNs provide further information about access and redress procedures.

[17] For more information, please *see* Privacy Policy Guidance Memorandum 2007-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, available at* https://www.dhs.gov/privacy.

Auditing and Accountability

The Unattended Ground Sensor Program is managed at the station, sector and headquarters level. The oversight of UGS deployment is outlined in the Intelligent Computer Assisted Detection (ICAD) Policy, dated September, 2006. Section 5.1 of the policy states that the Sector Assistant Chief Patrol Agent is responsible for: reviewing and evaluating reports for data accuracy and consistency; monitoring and directing compliance with policies and procedures; delegating authority for data quality control, as appropriate; and recommending disciplinary action for noncompliance.

Deployment of UGS must be conducted within a Border Patrol Agent's scope of authority. Pursuant to 8 U.S.C. § 1357(a)(3), USBP may access private land within 25 miles of the border, and, absent exigent circumstances, may enter private dwellings only with a warrant or consent. Monitoring of Government owned buildings and installations is required by policy, but deployment of UGS on privately owned land is only executed with consent of the property owner, pursuant to a warrant, or in exigent circumstances.

Only authorized users have the ability to extract materials from CBP 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. 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.

All information sharing and memoranda of understandings (MOU) 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 Official

Scott Luck
Deputy Chief
U.S. Border Patrol
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security