Privacy Impact Assessment
for the

Aircraft Systems

DHS/CBP/PIA-018

September 9, 2013

Contact Point
Lothar Eckardt
Executive Director, National Air Security Operations
Office of Air & Marine
U.S. Customs and Border Protection
(202) 344-3950

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) employs several types of aircraft including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or responses to other emergencies. Video, images, and sensor data collected through these Aircraft Systems alone cannot be used to identify a person, but they may later be associated with a person as part of a law enforcement investigation or encounter with CBP officers or agents. DHS/CBP is conducting this Privacy Impact Assessment to evaluate the privacy impact of these technologies on persons.

Introduction

The Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP) is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard. To achieve these missions, CBP employs several types of aircraft, including manned helicopters and fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or other emergencies. This Privacy Impact Assessment (PIA) is necessary because the aircraft are equipped with technology that captures information that may be associated with persons whom CBP encounters.

Overview

CBP employs several types of aircraft to achieve its mission objectives. All aircraft, manned or unmanned, have some type of imaging capability such as video, still images collection, and/or radar. The UAS differ from CBP's manned aircraft only in that the pilot controls the aircraft from the ground and the aircraft are capable of flying farther distances and longer hours continuously. All aircraft are owned and operated by the Office of Air and Marine (OAM); the Office of Intelligence and Investigative Liaison (OIIL) is responsible for processing, exploitation, and dissemination (PED) of imagery transmitted from aircraft.

CBP aircraft, both manned and unmanned, are used in the following scenarios: (1) to patrol the border; (2) to conduct surveillance for investigative operations; (3) to conduct damage assessment in disaster situations; and (4) in response to officer safety scenarios. While CBP also

allocates its air assets in a manner that reflects this prioritization, CBP reviews and considers all requests for assistance. Lastly, CBP does not equip its aircraft with weapons. While the crew in all manned aircraft and the officers and agents onboard the aircraft during tactical missions do carry weapons, the various aircraft are not equipped with armaments.

Helicopters

CBP operates several types of manned rotary-wing aircraft (helicopters) in support of its mission, notably, the American Eurocopter AS-350, Augusta Westland AW-139, Bell Huey UH-1, and Sikorsky UH-60. CBP uses helicopters for observation, for tracking suspects and supporting ground units, aerial reconnaissance of moving objects and persons, external lift capability for seizures and equipment delivery, and tactical support and transportation for law enforcement activities. Areas of operation include the border environment, both land and sea, to observe and interdict unlawful crossings of persons and goods, the airspace surrounding defined DHS National Special Security Events or critical venues, and populated or unpopulated areas that are the subject of defined law enforcement activity or investigation. CBP's helicopter fleet operates out of 30 locations maintained by OAM across the United States.

Fixed-wing Aircraft

CBP has manned fixed-wing P-3 AEW/LRT Orion aircraft operating out of specific operations centers in Corpus Christi, TX and Jacksonville, FL. CBP practices a defense in depth strategy of the borders of the United States and in active prosecution of attempts to smuggle persons or contraband by extending surveillance over international and coastal waters. As part of this strategy and as a means of integrating with the overall U.S. Government strategy to interdict the flow of narcotics and controlled substances across the U.S. southern borders, this defense in depth includes expanding the area of patrol to include the Caribbean and Eastern Pacific waters that border Source and Transit Zone countries.[1] Together the operations centers operate the P-3 aircraft primarily in Central and South America. Certain P-3s are used to intercept and track both aircraft and vessels for hours at a time while maintaining a covert standoff. CBP also operates several smaller, manned, fixed-wing aircraft out of OAM operational locations. These fixed-wing aircraft include piston-engine propeller-powered aircraft (Cessna models), larger turbo-prop powered aircraft (Bombardier Dash Eight, Pilatus, and Beechcraft Super King Air), and jet aircraft (Cessna Citation). These aircraft variously perform surveillance, tracking, interdiction, intercept, and information gathering roles. Fixed-Wing Aircraft employ various types of sensor technology including video, still, and radar images, and Law Enforcement Technical Collection (LETC) (electronic signals information across the electromagnetic spectrum).

[1] Source and Transit Zone countries are those nations working in partnership with the United States to interdict the flow of narcotics and controlled substances to the United States through the Caribbean Basin and along the coastal waters of the eastern Pacific Ocean. http://www.whitehouse.gov/ondcp/transit-zone-operations.

UAS

A UAS encompasses an unmanned aircraft, digital network, and personnel on the ground who operate the aircraft. CBP currently owns and operates ten such aircraft. The UAS aircraft include the Predator B[2] and the maritime variant of the Predator B, the Guardian, which allows CBP to conduct missions in areas that are remote, too rugged for ground access, or otherwise considered too high-risk for manned aircraft or personnel on the ground. The aircraft are stationed and principally controlled at four locations: Sierra Vista, AZ (4 aircraft); Grand Forks, ND (2 aircraft); Corpus Christi, TX (2 aircraft); and Cape Canaveral, FL (2 aircraft). CBP's UAS operate in accordance within the Federal Aviation Administration (FAA) Certificate of Authorization (COA) process. CBP works with the FAA to develop the COAs to define airspace for UAS operation. Consistent with the primary mission for the UAS, these COAs, which are in effect for a period of two years, define airspace (altitude, latitude, and longitude (geography)) along the border and outside of urban areas to support CBP UAS flight operations. As the FAA develops its roadmap to integrate UAS into the National Airspace System (NAS)[3], CBP will adjust to these new requirements and continue to employ UAS in pursuit of its primary border security mission.

Uses of Aircraft

Patrol

CBP uses all of its aircraft to patrol different parts of the border based on the specific strengths of the different aircraft. CBP P-3s patrol in a 42-million square mile area of the Western Caribbean and Eastern Pacific, known as the Source and Transit Zone, in search of drugs that are in transit towards U.S. shores. The P-3's distinctive detection capabilities allow highly-trained crews to identify emerging threats well beyond U.S. land borders. By providing surveillance of known air, land, and maritime smuggling routes in an area that is twice the size of the continental U.S., the P-3s detect, monitor, and disrupt smuggling activities before they reach shore.[4] As part of this patrol responsibility, images and radar information obtained in detecting, monitoring, or supporting activities is collected and maintained either for direct case support or to permit historical trend analysis regarding smuggling routes.

Along both the northern and southern borders CBP also employs UAS and smaller manned aircraft to help agents detect, identify, apprehend, and remove individuals and

[2] The General Atomics Aeronautical Systems MQ-9 Predator B is a mid-size Unmanned Aerial Vehicle (UAV) approximately thirty-six feet in length, with a maximum gross weight of 10,500 pounds and a wing span of sixty-six feet.
[3] See, *FAA Modernization and Reform Act of 2012*, Pub. L. No.112-95, sec. 331, 126 Stat. 11, 72, which mandates that the FAA prepare a roadmap to integrate UAS into the NAS by 2015.
[4] The Anti-Drug Abuse Act of 1988 established the Office of National Drug Control Policy (ONDCP) to set priorities, implement a national strategy, and certify Federal drug-control budgets. Interdiction of the flow of illicit drugs through the Source and Transit Zone is a critical component of the National Drug Control Strategy prepared annually by ONDCP.

contraband illegally entering the United States at and between Ports of Entry (POE). The COA defined airspace establishes operational corridors for UAS activity both along and within 100 miles of the border for the northern border, and along and within 25 to 60 miles of the border for the southern border, exclusive of urban areas. CBP helicopters and manned fixed-wing aircraft may operate in and around urban areas; however, the principal mission remains focused on those areas between the POE. Images, LETC, and radar information, specifically with respect to border areas between the POEs, are collected in support of case development or to permit trend analysis.

Following a flight, the images are provided to OIIL for processing, exploitation, and dissemination. Subsequently, and only upon request, OIIL provides access to the forensic analysis of a particular image and area to authorized persons who have a "need to know;" when the dissemination is in response to a particular law enforcement activity or case, that analysis may include PII.

Persons who are apprehended and who were video recorded from a UAS or a manned aircraft may have the video of their crossing and/or apprehension associated with a case file that contains their PII.

Separately, CBP also deploys manned fixed-wing aircraft with LETC sensors over the border area in support of its counter-terrorism and interdiction of smuggling operations. The LETC sensors permit surveillance of the electromagnetic spectrum for the purpose of identifying organized border crossing activity between the ports of entry.

Investigative Operations

CBP uses both UAS and manned aircraft in support of other DHS components, such as U.S. Immigration and Enforcement (ICE), or other federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI) or Drug Enforcement Agency (DEA). Requests for aircraft support that are related to the border surveillance must be directed to the Assistant Commissioner, OIIL, for authorization. Each request for information follows a standard process and is reviewed and considered in terms of the requesting agencies' authorities to receive the sought after information, CBP's own authority to lend assistance, and CBP's ability to integrate the information collection into its mission. Separately, OAM must determine the availability of aircraft type and the integration of the requested activity into its flight operations.

Typical support missions include overhead observation of previously identified persons, specified locations, and particular conveyances for enhanced situational awareness and increased officer safety. For example, the UAS could conduct surveillance over a building to inform ground units of the general external layout of the building or provide the location of vehicles or individuals outside the building. When flying a UAS in support of another component or government agency for an investigative operation, CBP may provide the other agency with a direct video feed through access controls or with a downloaded video recording of the operation,

in whole or in part, based on the request. Similarly, CBP may deploy a helicopter or manned fixed-wing aircraft to provide over top visibility into a developing incident. Video images from the Electrical Optical/Infrared ball (EO/IR) ball are fed through the DHS firewall to "Big Pipe," a video and image distribution network operating within the CBP/DHS firewall, to identified users, analysts, and decision makers for real-time mission support and border protection.

Disasters

The P-3 may be used to conduct reconnaissance missions during natural disasters in support of FEMA. During these missions, P-3s can provide near real-time, high quality video of affected areas to first responders and FEMA. P-3s are equipped with similarly capable EO/IR Ball cameras; the images are also fed through a transmission to a ground station where the video is decrypted and fed to Big Pipe to disseminate inside the DHS firewall to authorized users within DHS and any other requesting agency.

UAS may also be used outside existing COAs during natural disasters once the government has issued a disaster declaration. For example, the UAS may fly missions in support of other government agencies such as the National Oceanic and Atmospheric Administration (NOAA) or FEMA to provide video or radar images of flooding. In disaster situations, CBP works with the FAA to construct a COA defining the airspace where a CBP UAS may operate. The UAS may provide a real-time feed during flight through Big Pipe or, subsequently, an analyzed image comparing the raw feed to an image with identified details, noting changes, to FEMA, state emergency operations centers, United States Geological Survey (USGS), and/or the Army Corps of Engineers. Video from these operations are not used to identify individuals. As with other requests for support, disaster area overflight requests are assigned in accordance with the national policy regarding the tasking of CBP air assets.

Officer Safety and Support to State and Local Law Enforcement

State and local law enforcement officials may request aircraft support (e.g., UH-60, P-3, UAS) in emergency situations; often this involves circumstances when officer safety is implicated, and in which aerial surveillance is necessary or the terrain would be too difficult for law enforcement personnel to navigate. OIIL reviews each request to determine whether to respond and OAM reviews how and in what context it may respond. Based on both organizations within CBP, a decision is made whether to provide assistance. Access to video taken during emergency situations may be provided, either at a DHS/CBP facility or by temporarily granting direct access through the DHS firewall. Sharing of this information with state, local, or other government agencies is on a case by case basis as determined through CBP's Request for Information process.

As in the mission uses discussed above, UAS and manned aircraft offer several options for deploying information gathering equipment. The UAS can serve as force multiplier insofar as the UAS enables the monitoring of large areas of land more efficiently and with fewer

personnel than other aviation assets. UAS can enhance situational awareness and increase officer safety by providing aerial support to officers on the ground by monitoring a fixed location while flying at a high altitude to reduce the likelihood of detection. Manned aircraft offer the ability to fly in more congested airspace and to transport officers, agents, equipment, and seized assets.

Technology on Board the Aircraft

The various aircraft have different types of surveillance technology. Most aircraft, manned and unmanned have an EO/IR ball attached to provide a means of collecting information. The EO/IR ball installed on the UAS also assists the pilot during take-off and landing. While the cameras on each aircraft are not identical, they have almost identical performance specifications. The EO/IR ball is a camera, which employs a fixed-focus lens, that is capable of providing video at any altitude and allows operators, using digital zooming (software based image enhancement), to take small-scale aerial video images of buildings, vehicles, and people. Aircraft altitude directly affects a fixed-focus camera's performance; the higher the aircraft's altitude, the less detail an operator is able to see.

A lower altitude permits the EO/IR ball to provide greater detail in an image, which may permit identification; this observation activity, however, does not occur unnoticed or subject to attempts at evasion, and therefore is more often part of a defined law enforcement operation. Persons are often successful at hiding their identity from known surveillance aircraft by simply looking away.

At present, the flight and mission parameters for the UAS place their operation within an altitude block of 19,000 to 28,000 feet, thereby effectively limiting the altitude for the EO/IR ball on a UAS to a minimum of 19,000 feet. At this minimum altitude, the camera does not provide enough detail for an operator to identify a person (that is to discern physical characteristics such as height, weight, eye color, hair style, or a facial image). The camera operator may have enough detail to identify whether an individual is carrying a long gun or wearing a back pack. At an altitude of 19,000 feet the camera operator cannot read a license plate, nor are license plate readers effective.

Conversely, the flight parameters for helicopters and fixed-wing aircraft are broader in terms of altitude and geography; their flight operations are integrated into the NAS and do not require a COA. The mission parameters and physical capabilities for helicopters and manned fixed-wing aircraft, however, place different operational restrictions upon the aircraft.

The EO/IR ball can provide daytime or nighttime visual video observation of movement or objects on the ground. The images, depending upon the aircraft deploying the camera, tend to be small in scale, to provide environmental context. A principal purpose for tracking a person or vehicle from an aircraft with an EO/IR ball is to assist CBP or law enforcement personnel on the ground with information to permit a safe encounter—this requires environmental context more

than a best possible close-up of a face. When viewing vehicles, an operator can distinguish a car from a truck, and depending on the altitude at which the aircraft is flying, may be able to identify the model of the vehicle. During daytime flights, an operator may also be able to determine the color of the vehicle. The images of vehicles and/or individuals recorded by the EO/IR ball are not associated with any biographical information unless the individual is apprehended, at which point the video may be associated with the Personally Identifiable Information (PII) contained within the individual's case file.

In addition to EO/IR CBP deploys a UAS stationed along the Southwestern border in Sierra Vista, AZ, with the Wide Area Surveillance System (WASS). WASS uses a sensor mounted to the wing of a UAS to sweep large areas of border territory (approximately six kilometers in width) as the aircraft moves along its flight path. WASS alerts CBP to the existence of persons and/or vehicles along the border and provides coordinates to determine their location. The UAS pilot and sensor operator can then inform ground units of the location so that Border Patrol may coordinate an interdiction of the persons or vehicles. WASS provides a radar sensor image, which CBP may share through Big Pipe during operation.

Some manned and unmanned aircraft are also equipped with synthetic aperture radar that can provide black and white images in all weather. This radar can provide silhouettes of people and vehicles, but provides no identifying details. Using this technology, an operator is not able to pick up identifying characteristics of a person or a vehicle. The synthetic aperture radar is primarily used for change detection. For example, the operator can identify tire tracks on the ground that were not present in prior images provided by the radar. Similarly, an operator can use the synthetic aperture radar to determine the extent of flooding in a particular region by noting the changes to the topography.

Certain manned fixed-wing aircraft deploy LETC sensors used to detect electronic signals in the electromagnetic spectrum. These specifically designed aircraft operate in support of counter-terrorism efforts and to interdict organized smuggling (people, contraband, and controlled substances) operations within the border area. Like with the EO/IR ball, information from LETC sensors may be employed to support officers and agents on the ground as they move to a position where they can safely encounter observed persons. LETC aircraft sensors are solely deployed on manned fixed-wing aircraft.

Data on the digital video recorders on CBP aircraft are maintained for a maximum of 30 days and then overwritten by new data. The images and related data from CBP aircraft, both manned and unmanned, are provided through Big Pipe to identified users, analysts, and decision makers for real-time mission support and border protection. Images from the EO/IR ball mounted on the UAS are sent by an encrypted transmission, first to the satellite providing the control signals, and then, again by encrypted transmission, to the ground control station where the pilot and sensor operator are located. The image data is decrypted and brought inside the

DHS firewall at the ground control station, where Big Pipe can ingest the data and provide a feed to assigned users and analysts.

Big Pipe is a fully distributed network hosted by CBP and supports not only event-based law enforcement missions, but also FEMA's National Response Framework.[5] Big Pipe employs role-based access controls to provide users possessing a need to know access to distinct video feeds at command centers, other CBP/DHS locations, and for authorized persons with technical access through the DHS firewall. OAM retains control over defining users for Big Pipe and assigning access. After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data. Stored data is retrieved based on the date and time of the mission and only by authorized users on a need to know basis. If data is used for investigative purposes, and associated with a particular individual it goes into a case management system, which is covered by the corresponding Privacy Act System of Records Notice (SORN) for the case management system. Big Pipe, separately, provides a feed of video and radar images from UAS to the Air and Marine Operations Center (AMOC), where OIIL operates one of several PED cells to review this data over time to perform trend analysis and change detection. Video and radar images maintained by a PED cell, such as at the AMOC, are stored on a separate server dedicated to the PED cell mission for up to five years. The analyzed images may be shared by OIIL in response to law enforcement needs.

Summary of Privacy Risks

The use of these aircraft and accompanying surveillance technologies presents several privacy concerns. The first concern is ensuring that CBP's collection and use of data from aerial surveillance remains within the scope of its authorities to protect the border and provide support for law enforcement activities, while continuing to preserve a person's right to privacy. CBP's border security mission has a broad mandate to determine the admissibility of persons and ensure that goods are not introduced into the United States contrary to law.[6] Similarly, the statutory language in CBP's annual appropriations directs CBP Air and Marine to provide integrated and coordinated border interdiction and law enforcement support for homeland security missions, including assistance to federal, state, and local agencies and emergency humanitarian efforts; to provide airspace security for high-risk areas or National Special Security Events[7]; and to combat

[5] The National Response Framework is a DHS/FEMA led effort, which provides the guiding principles that establish a comprehensive, national, all-hazards approach to domestic incident response—from the smallest incident to the largest catastrophe. http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.
[6] Title 8, United States Code (U.S.C.), sections 1225, 1357, other pertinent provisions of the immigration laws and regulations; 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, 1595a(d), and other pertinent provisions of customs laws and regulations.
[7] See Title 18 U.S.C. Section 3056, which authorizes the designation of National Special Security Events.

efforts to smuggle narcotics and other contraband into the United States[8]. Deploying OAM's various air assets to support these missions improves DHS/CBP's capability to obtain streaming video, and to assess critical infrastructure before and after events.

CBP's use of manned and unmanned aircraft to conduct aerial observations is consistent with CBP's authorities and obligations. To the extent that aircraft flying in support of tactical operations overfly private residences, there is a minimal risk that a person's privacy might be unintentionally violated. The images captured are not personally identifiable without further investigative information. Neither manned nor unmanned aircraft physically intrude upon or disturb the use of private property. Further, the cameras deployed on UAS or manned aircraft do not have the capability to see through walls or otherwise collect information regarding what occurs in the interior of a building, nor is that their purpose. UAS operate primarily at an altitude between 19,000 and 28,000 feet pursuant to their COA approved by the FAA, and are focused as previously described.

A second privacy concern, specific to UAS, is that they present a perceived risk to privacy because they are able to fly for longer hours than manned aircraft and conduct surveillance undetected. Like other aircraft, UAS are useful for monitoring remote land border areas where patrols cannot easily travel and infrastructure is difficult or impossible to build. Unlike manned aircraft, UAS are operated by personnel on the ground, allowing the crew to be relieved while the UAS is still in the air. This capability allows UAS to provide long-range surveillance for greater lengths of time than manned aircraft. Because of their small size compared to manned aircraft, and the altitude at which UAS can operate, these physical attributes may serve to conceal the presence of a UAS and reduce detection of their operating noise while still being able to maneuver over a small area and provide surveillance. Other OAM operated long range fixed-wing aircraft cannot steadily monitor a set location because of their size and turning radius. Helicopters are more easily detected because of their noise and lower operational altitudes. This means that, unlike fixed-wing aircraft and helicopters, UAS can monitor either a moving target or a fixed location for relatively longer periods of time without the likelihood of detection.

While UAS can fly for longer periods of time, they are equipped with the same technology to conduct surveillance that is presently deployed on CBP manned aircraft. The only sensor available on UAS that is not used by CBP manned aircraft currently is the WASS sensor. The WASS sensor can only detect the presence of a person and track his or her movements (much the same way other radar technology can detect an object and track its movement); it cannot be used to identify a person. The WASS sensor is designed to sweep large areas of land and is only used to patrol along the southwest border and to assist with interdictions. Other technologies on the UAS are shared by CBP's manned aircraft. Putting these technologies on a

[8] See National Drug Control Strategy, http://www.whitehouse.gov/ondcp/2013-national-drug-control-strategy.

UAS only enhances CBP's ability to perform its existing functions. For instance, CBP's surveillance video of a location used to smuggle persons or contraband using a UAS instead of a P-3 may be longer in duration with less interruption and less likelihood of detection.

To mitigate the risk presented by longer sustained surveillance of an individual or residence without the individual's knowledge, CBP has strict mission priorities for UAS and all aircraft operations. For instance, CBP aircraft may only be used in support of an authorized mission or investigation, the video or other data collected from CBP aircraft may only be accessed by authorized personnel with an authorized need to know, and the CBP-held video or other data is controlled through chains of custody and stored in secure locations until it is destroyed. In addition, the FAA requires CBP to construct a COA, in the instance of deploying a UAS, for a duration determined by the investigative activity or emergency circumstance, before conducting an operation away from the border and already established COAs.

The third privacy concern, unique to UAS, pertains to the security of the system itself and the potential for hijacking of the unmanned aircraft. CBP has taken several steps to protect UAS against potential hackers. All UAS are controlled and monitored at all times by operators in ground control stations using satellite communication that is relayed through an encrypted data feed. The ability to interfere with such an encrypted data feed requires disrupting the signal from satellite to UAS, for the purpose of acquiring the data feed or controlling the UAS. In the event that the ground control station loses its ability to control the UAS, another ground control station can pick up control of that UAS. The UAS use redundant navigation systems and GPS receivers so that if a signal is lost or someone attempts to override the signal, the UAS relies on these other systems and the GPS receivers for flight operations. In order to protect the airspace, the FAA is notified immediately if a UAS loses its signal. Furthermore, if communication between ground control and the UAS is ever interrupted or lost, the UAS are pre-programmed to fly to a pre-coordinated point in a remote location to orbit while waiting for the signal to be reestablished, or to continue to orbit this Flight Termination Point until the aircraft runs out of fuel and crashes.

Because of the unique privacy concerns raised by CBP's use of Aircraft Systems, CBP has conducted this PIA to evaluate the privacy risks associated with the use of Aircraft Systems and to enhance public understanding of the authorities, policies, procedures, and privacy controls related to that use.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[9] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. Given that Aircraft Systems and their associated devices are mechanical and operational systems rather than a distinct information technology system or collection of records pertaining to an individual that would be subject to the parameters of the Privacy Act, this PIA is conducted to relate the use of these observation and data collection platforms to the DHS construct of the FIPPs. This PIA examines the privacy impact of Aircraft Systems operations as it relates to the DHS FIPPs.

1. Principle of Transparency

Principle: *DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.*

This PIA provides a level of transparency to the public about the current surveillance programs undertaken by CBP. The video, still images, signals information, and/or radar images do not clearly identify individuals. The only information about individuals that is collected and/or retained is the indication of a human form. These images, however, may be associated with a person if the person is apprehended. For example, video collected by an EO/IR ball may show several individuals traversing the land border and being intercepted by officers or agents of CBP. While the video resolution or radar mapping images are not sufficiently precise to permit actual identification, the circumstances of CBP interdiction and apprehension of a suspect in conjunction with the aerial surveillance are sufficient to link the indistinct images of persons traversing the ground to the case file. Individuals who are apprehended by CBP as a result of observation by aircraft at or near the border may have video of their crossing and apprehension associated with their enforcement case file. CBP obtains biographical data pertaining to the apprehended person at the moment of apprehension. CBP stores all biographical information

[9] DHS Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, December 29, 2008.

obtained from apprehended individuals and any video or radar images of their movement obtained from the aircraft in the appropriate law enforcement case management system.

When CBP associates video, still images, signals information, and/or radar images with an individual after apprehension, that information becomes subject to the requirements of the Privacy Act in the same manner and to the same extent that the apprehension of the individual becomes a record in a Privacy Act system. The Privacy Act requires that agencies publish a SORN in the Federal Register describing the nature, purpose, maintenance, use, and sharing of the information. This PIA serves as notice to the public that information captured by Aircraft Systems may become subject to the Privacy Act once it is associated with an individual.[10] Additionally, the video images associated with an individual's case file are covered by the appropriate law enforcement case management SORN, which maintains the case file. CBP will periodically re-assess the means by which the images from the aircraft are retrieved to determine whether the requirement for a SORN is triggered.

2. Principle of Individual Participation

Principle: *DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

Individual participation provides complementary benefits for the public and the government. The government is able to maintain the most accurate information about the public, and the public is given greater access to the amount and uses of the information maintained by the government. A traditional approach to individual participation is not always practical or possible for CBP, which has law enforcement and national security missions. Aircraft are primarily used to sweep the border area to locate individuals who are crossing the border illegally. Allowing an individual to consent to the collection, use, dissemination, and maintenance of video, still images, and/or radar images would compromise operations and would interfere with the U.S. government's ability to protect its borders, thereby lessening overall homeland security.

Individuals do not have the opportunity to restrict CBP's ability to collect information in the public sphere. Any information associated with an individual is part of a case file that is created as part of a law enforcement investigation or encounter.[11] Providing individuals of interest access to information about them in the context of a pending law enforcement

[10] For example, video information from an aircraft of an apprehension of a person at the border that is identified to that person would be referenced in the case notes pertaining to that person's apprehension in TECS (DHS/CBP – 011 TECS System of Records Notice December 19, 2008 73 FR 77778)

[11] CBP also incorporates images from surveillance or encounters into reports and analyses maintained in the Analytical Framework for Intelligence (AFI) (DHS/CBP – 017 System of Records June 7, 2012 77 FR 13813).

investigation may alert them to or otherwise compromise the investigation. Consequently, there is no mechanism for correction or redress for the video collected by the aircraft. Once that video is associated with an individual's case file, the individual must follow the procedure outlined in the corresponding privacy documents for that system. While individuals cannot participate in the initial collection of this information, they may contest or seek redress through any resulting proceedings brought against them. More information on redress is provided below.

3. Principle of Purpose Specification

Principle: *DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

The purpose specification principle requires DHS to 1) articulate the authority to retain the PII in question; and 2) articulate the purpose(s) for which DHS uses the PII.

CBP is authorized to collect video, other images, signals information, and data using aircraft in support of its border security mission and pursuant to the appropriations language mandating support for law enforcement as part of the mission of CBP Air and Marine.[12] Together, these authorities allow CBP to obtain information in support of border interdiction of narcotics and other contraband, the prevention of the illegal entry of aliens into the United States, the security of airspace for high-risk areas or National Special Security Events, and in support of federal, state, and local law enforcement, counterterrorism, and emergency humanitarian efforts.

CBP may use video, still images, signals information, and/or radar images, obtained from aircraft, to apprehend individuals and to provide evidence of an illegal border crossing or other violation of law. Consistent with applicable laws and SORNs, the information may be shared with other state, local, federal, tribal, and foreign law enforcement agencies in furtherance of enforcement of their laws. [13]

Video, still images, and/or radar images collected during investigative operations as part of a law enforcement investigation are used for enhanced situational awareness and increased officer safety, and may be used to provide evidence of a violation of law. These images are maintained in association with the investigative or case file that they support; their retention is managed by the same SORN and follows the handling of the investigative or case file.

---

[12] *See, e.g.*, H.R. REP. No. 112-91, at 46 (2011) stating "CBP Air and marine provides integrated and coordinated border interdiction and law enforcement support for homeland security missions; provides airspace security for high risk areas or National Special Security Events upon request; and combats efforts to smuggle narcotics and other contraband into the United States. CBP Air and Marine also support counterterrorism efforts of many other law enforcement agencies."

[13] *See* Consolidated Appropriations Act of 2012, Pub. L. No. 112-74 (2011), providing for "the interdiction of narcotics and other goods; the provision of support to Federal, State, and local agencies in the enforcement or administration of laws enforced by the Department of Homeland Security; and at the discretion of the Secretary of Homeland Security, the provision of assistance to Federal, State, and local agencies in other law enforcement and emergency humanitarian efforts…."

Video, still images, and/or images collected in natural disaster and/or emergency situations are used for relief work and disaster reconnaissance. CBP typically provides a direct feed of the video captured by aircraft in these scenarios to provide support to FEMA or state emergency operating centers. Video, still images, and/or radar images are not associated with an individual and are only used to indicate where an individual or group of individuals may be for emergency response purposes.

4. Principle of Data Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

CBP seeks to minimize the collection and retention of video, signals information, and radar to that which is necessary and relevant to carry out CBP's mission. Accordingly, when aircraft are flown to patrol the border, they are authorized to fly the designated border surveillance mission area to ensure they are only capturing images and information necessary to detect, identify, apprehend, and remove persons and their possessions illegally entering the United States at and between POE. When aircraft are flown for investigative operations, officer safety incidents, or natural disaster reconnaissance, CBP approves and defines the specific mission that is authorized, and in the case of UAS, works with the FAA to construct a COA to establish airspace for that specific UAS operation. The video (that has not been associated with a case) remains on the digital video recorder originally used for recording until it over-written through re-use, which is after approximately 30 days.

After the creation of live mission data, Big Pipe manages the transmission, processing, distribution, consumption, and storage of the live mission data. Big Pipe archives selective mission data on a Big Pipe server hard drive for a maximum of 7 days, after which the data is deleted. Big Pipe does not use PII to retrieve stored mission data.

The information collected by the aircraft is not subject to the Privacy Act unless it is retrieved by using an individual's name or other unique identifier. If an individual is apprehended by CBP as a result of observation by aircraft or subsequent association from the presence of CBP assets, CBP may have video of that individual's apprehension associated with his or her enforcement case file. That video is retained according to the retention schedule of the SORN of the corresponding case management system. Video and Radar images obtained from UAS patrols of the border are also provided to PED cells operated by OIIL for use in analyses and intelligence products concerning historical, change detection (e.g., natural and man-made alterations to geography) along the border, and patterns of movement of persons across the border. This unassociated data, in conjunction with meta-data (such as latitude, longitude, date and time of the imagery) is retained for a maximum of five years.

5. Principle of Use Limitation

Principle: *DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

CBP only collects video and/or radar images, and signals information via aircraft pursuant to its law enforcement authority, as part of its border security mission, or when flying a mission in support of another agency, and when that other agency's authority covers the mission either through delegation of authority or direct control of the information collected. For example, CBP has provided support to the U.S. Forest Service in response to large scale wild fires to permit an overview of the extent and scale of the fire and identification of hot spots; this activity is pursuant to a request from the Forest Service, is performed pursuant to their authority, and the images are conveyed through designated access to the Big Pipe video distribution service. While the video resolution, radar mapping images, and signals information are not sufficiently precise to permit actual identification of a person, the images or information may be associated with an individual from context within the image, circumstances surrounding the activity occurring in the image, or additional information obtained directly from the person by an officer or agent. The images or information are only associated with an individual if the individual is apprehended or if the images are taken as part of an ongoing law enforcement investigation. Accordingly the data can only be used for the purposes specified in section 3 of this PIA.

CBP has procedures and processes in place for sharing any data collected by aircraft, including when that information becomes associated with a case and is used as evidence against an apprehended individual. In addition, all requests for aerial surveillance for intelligence gathering purposes must receive prior approval by the Assistant Commissioner, OIIL, before the air asset can conduct the flight. Similarly, requests for analytical products incorporating historical analysis of the border topography must be approved by the Assistant Commissioner, OIIL.

6. Principle of Data Quality and Integrity

Principle: *DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.*

As explained in section 4 (above), to ensure that the PII captured by aircraft is relevant and timely, any video, still images, signals information, and/or radar images must be associated within 30 days with the individual CBP apprehends, or the video/digital image is overwritten by OAM. Video and/or radar images are of no continuing value in a law enforcement support context unless they are associated with an individual during an apprehension because the video resolution or radar mapping images are not sufficiently precise to permit actual identification of

individuals. Video and/or radar images that are not associated with a person provide value in an intelligence context for helping to demonstrate the state of change occurring over time along the border. These unassociated images are separately maintained by OIIL for a maximum of five years.

To preserve the quality and integrity of the information collected that is used as evidence, CBP requires its officer/agents to successfully complete training on the proper operation of the recording equipment on its aircraft. The training includes correct techniques to copy recorded evidence from a non-portable hard drive to portable digital media and procedures to ensure that such evidence is not co-mingled with data from other investigations. The training also includes procedures to maintain an adequate chain of custody for all recorded evidence. Each officer/agent making a recording must ensure that the time and date shown in the original recording is accurate. After a mission is completed, the officer/agent must ensure that the original record is transferred entirely, in its original format, to portable media. The transferred data must not be edited or altered in any way. The officer/agent making the recording must label all copies of portable media with the corresponding case number (if available), the date and place of the original recording, and the names of the officer/agent and aircraft commander. The officer/agent making the recording must also label, initial, and maintain possession of the evidence until custody is properly transferred to the appropriate designated evidence custodian, case agent, Assistant United States Attorney, or other appropriate government official. As with any information associated with a case file, once the images are cross referenced to an investigation or case, they become covered by the system of records for that case file system and subject to the access and amendment provision of that system.

7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

CBP has taken steps to protect live video feeds, signals information, and recorded video, radar, and/or still pictures captured by its aircraft. Live video and flight information, which are sent from the UAS, are passed along an encrypted feed from the UAS through the satellite relay to the ground control station. Similarly, control information from the ground control station to the UAS also passes along an encrypted feed. Video and data transmitted in real time via Big Pipe, a closed system with restricted access, is subject to access controls and an approval process requiring clearance by one of two CBP/OAM system administrators to ensure that only authorized users with a need to know have access to the video feeds. The real time video feeds are not recorded and archived. Any recorded images that are saved to be used as evidence or for intelligence gathering must be handled in accordance with CBP policy. Images that are used as evidence must be handled according to the procedures detailed in section 6 of this PIA. All

recorded evidence must be kept in a locked container, segregated from other property and/or equipment. Video that is collected during an investigative operation that contains sensitive analytical surveillance, or reconnaissance related data may not be disclosed unless a request for disclosure has been submitted to the OIIL Collections Division Director. The request must include a copy of the information that is to be disclosed, must clearly specify the name of the intended recipient, how the information will be used, and the reasons justifying the disclosure. In the event that the information is disclosed, the OIIL Collections Division Director or his/her designee is required to redact law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a need-to-know.

8. Principle of Accountability and Auditing

Principle: *DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

All CBP employees are required to complete annual privacy awareness training, in addition to training on ethics and the CBP Code of Conduct. Access controls, both physical and technological, are in place to ensure only authorized access to the aircraft systems and the collected data/images.

Moreover, CBP requires its employees to successfully complete training on techniques to copy recorded evidence to portable digital media and requires them to follow procedures to ensure that such evidence is not co-mingled with data from other investigations. Employees must follow procedures to maintain an adequate chain of custody in the event that the information is used as evidence.

OIIL has a process in place for restricting the dissemination of video, still images, and radar images and keeps a log of the disclosures. Also, OIIL redacts law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a valid need-to-know. Separately, CBP periodically reviews the logs or disclosure records to ensure compliance with established privacy policies, practices, and procedures for associated systems.

Conclusion

CBP operates aircraft systems in support of its border protection and law enforcement support missions. These systems provide a variety of mobile platforms from which to obtain signals information, video, still, and radar images of persons and vehicles in the border area or that are the subject of an investigation or law enforcement activity. The collection of these images and signals information complies with the same internal procedures and practices required of any surveillance using any means by CBP officers and agents. The distinct capabilities of the different aircraft operated by OAM enhance CBP's ability to conduct certain missions pertaining to information collection, surveillance, or reconnaissance; however, the processes and procedures for authorizing and accounting for how, when, and where information is obtained remain consistent with CBP's traditional border security and law enforcement practices and policy. As technology improves, operating environments change, and policies adapt, this PIA will be updated and amended to refresh the analysis of these changes on the privacy of persons, who directly or indirectly come into contact with the information and data collection activities associated with CBP Air operations.

Responsible Officials

Lothar Eckardt
Executive Director, National Air Security Operations
Office of Air & Marine
U.S. Customs and Border Protection
202-344-3950

Laurence Castelli
CBP Privacy Officer
Office of Privacy and Diversity
Office of the Commissioner
U.S. Customs and Border Protection
202-325-0280

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Page 20

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

From: (b)(6)
Sent: 7 Apr 2017 15:50:54 -0400
To: (b)(6)
Subject: FW: Criteria for Reviewing UAS Grant Applicants
Attachments: Criteria for Reviewing Grant Applicants.docx

(b)(6)
Security, Intelligence and Information Policy Section
DHS Office for Civil Rights & Civil Liberties
(b)(6)

From: (b)(6)
Sent: Wednesday, October 26, 2016 2:27 PM
To: (b)(6)
Subject: Criteria for Reviewing UAS Grant Applicants

(b)(6)
Senior Policy Advisor
Office for Civil Rights & Civil Liberties
U.S. Department of Homeland Security
(b)(6)

Criteria for Reviewing UAS Grant Applicants'

Privacy, Civil Rights, and Civil Liberties Policies

1. Is there a Designated Individual Responsible for Privacy, Civil Rights, and Civil Liberties Compliance?

This should be a senior level individual within the organization, preferably in the office(s) responsible for privacy, civil rights and civil liberties (if one exists), with working knowledge of the relevant privacy, civil rights, and civil liberties laws and regulations. The senior level individual should have a "direct line" to the person who has overall responsibility for the unmanned aircraft program.

2. Does the Policy Limit Collection, Use, Dissemination, and Retention of UAS Recorded Data?

Considerations:

- Recorded images of individuals should not be retained beyond a reasonable period as defined by existing agency/departmental policy unless there is authorization based on a legal, policy or operational purpose.
- Collection, use, dissemination, or retention of unmanned aircraft system-recorded data should not be based solely on individual characteristics (e.g., race, ethnicity, national origin, sexual orientation, gender identity, religion, age, or gender), which is a violation of the law.
- The users of unmanned aircraft system-recorded data are responsible for ensuring dissemination of data is authorized and consistent with the recipients' legitimate need to know and authority to receive such data; any further dissemination by a data recipient should require the data owner's prior consent, which should only be provided upon the advice of the entity's legal counsel.
- Federal agencies need to establish whether their systems collect and store PII, and if so, whether there is an applicable System of Records Notice. Additionally, if their system does collect and store PII, agencies should consider whether they should limit the collection of personally identifiable information in accordance with OMB M 7-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- Requests for unmanned aircraft system data by commercial entities, civil litigants, or Freedom of Information Act requesters should be reviewed by legal counsel to determine if such sharing is appropriate and permissible under applicable laws or regulations.
- Unmanned aircraft program managers should employ reasonable technological or administrative safeguards to ensure that images of people incidentally recorded who are not relevant to an operation are not disseminated or viewed unnecessarily to protect individual rights. This is especially important for recordings that include images of minors not relevant to an operation.

- Follow and clarify (if necessary) existing procedures for identifying, disseminating, retaining, indexing, and storing relevant and necessary unmanned aircraft system- recorded data in a retrievable manner.

3. Does the Policy address Constitutional Protections?

Considerations:

- Incidental images of identifiable individuals that are recorded, but not needed for legal compliance or law enforcement purposes, should be deleted according to established procedures and within 180 days.
- Be attuned to the potential privacy risks or legal ramifications arising from inadvertently capturing images of individuals engaging in constitutionally protected activities, and establish appropriate guidelines and administrative controls to anonymize, destroy, safeguard or prevent the misuse of such data, consistent with applicable law.
- Unmanned aircraft system-recorded data should not be collected, disseminated or retained solely for the purpose of monitoring activities protected by the U.S. Constitution, such as the First Amendment's protections of religion, speech, press, assembly, and redress of grievances (e.g., protests, demonstrations).

4. Is there a Redress Program for Individuals that Covers UAS Activities

Considerations:

- Where an administrative process is used, the process for resolving complaints should promote resolution within a reasonable amount of time.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security, individuals should be provided information regarding the factual basis for redress determinations.
- Information on how an individual requests redress should be succinct, straightforward, and readily available to the public.

5. Is there Accountability in Management of Unmanned Aircraft Program

Considerations:

- Establish or confirm that existing oversight procedures (including audits or assessments) ensure compliance with policies and regulations; this may also serve as another layer of security and improve the overall integrity of the program.
- Provide adequate supervision of personnel and a process for personnel to report suspected cases of misuse or abuse.
- Impose penalties for misuse and non-compliance with policies and procedures.
- Establish policies and procedures for documenting individuals accessing or requesting access to unmanned aircraft system-recorded data.

- Institute a schedule of regularly submitted reports to agency legal, privacy, civil rights, and civil liberties experts documenting all unmanned aircraft system activities and complaints received during the prior reporting period. Reports should be submitted at least annually.
- Determine whether there is a need for new data sharing agreements, and establish appropriate record management policies before sharing data with other agencies.

6. Does the Policy Address Properly Securing and Storing UAS Recorded Data?

Considerations:

- Ensure access to unmanned aircraft system-recorded data is controlled by using appropriate physical, personnel or technical security measures as appropriate (e.g., digital watermarks, encryption, or other security and authentication techniques) to protect the data.
- Apply appropriate handling and safeguarding procedures to unmanned aircraft system-recorded data that may be linked to individuals, or to sensitive information that is not otherwise personally identifiable (e.g., sensitive government or business proprietary information).
- Ensure the unmanned aircraft program authenticates and establishes a chain-of- custody that preserves the integrity of all data stored in the event that the data are produced in litigation.
- Develop procedures to ensure the system and its stored data are used only as authorized.
- Security measures should be layered to avoid reliance on any single security measure; employ several measures that functionally overlap to create redundancy in the security of data and the overall program.
- Protect the physical security of the communication links, and operational and data storage centers.
- Individuals with access to unmanned aircraft systems should receive background checks in accordance with an agency's regulations.

7. Does the Policy Promote Transparency and Outreach?

Considerations:

- When organizing initial outreach efforts, consider using the best practices listed in this guide that are operationally and legally feasible for your agency as a starting point, and periodically engage the public to keep them informed about the program and proposed significant changes.
- Outreach efforts should consider how to include persons with limited English proficiency and persons with disabilities.
- When circumstances permit, and while not revealing information that could reasonably be expected to compromise law enforcement or national security,, provide notice to the public as to where unmanned aircraft routinely operate (e.g., a description of the general operating area on websites, public documents, or through use of public signs).

8. Does the Policy Require Privacy and Civil Liberties Training?

Considerations:

- Individuals with access to stored data should receive training designed for the specific software and hardware employed by the agency's unmanned aircraft program.
- Those personnel responsible for handling unmanned aircraft systems support requests from other agencies should receive additional training on the agency's standard operating procedures for handling such requests.
- Staff should be instructed not to use any unmanned aircraft systems-acquired data for personal use.