Privacy Impact Assessment Update

for the

Aircraft Systems

DHS Reference No. DHS/CBP/PIA-018(b)

May 8, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) employs several types of aircraft, including manned helicopters, fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft may be equipped with video, radar, and sensor technologies to assist CBP in patrolling the border, conducting surveillance for law enforcement investigations or tactical operations, or gathering data to assist in disaster relief and emergency response. In addition, the U.S. Border Patrol (USBP) operates Small Unmanned Aircraft Systems (sUAS) in support of its border security mission. CBP is publishing this Privacy Impact Assessment (PIA) update to provide notice of CBP's use of Tethered Small Unmanned Aircraft Systems (TsUAS) not addressed in the August 2019 Privacy Impact Assessment update, and to assess the privacy impacts of its use of this technology. The distinction between the previously documented sUAS and the new TsUAS is that TsUAS are hard wired via a tether line to the Ground Control System.

Overview

CBP is responsible for securing roughly 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. CBP employs various border surveillance technologies to provide comprehensive situational awareness along the U.S. border 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 enforced or administered by CBP.

CBP has previously described and assessed the privacy risks of Border Surveillance Systems (BSS),[1] including fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, radio frequency sensors, maritime and ground radar, tactical surveillance systems, unmanned ground vehicles (UGV), and the use of commercially available location data to identify activities in designated areas near the United States border. In addition to the technology discussed in the original Border Surveillance Systems Privacy Impact Assessment and subsequent updates, CBP also employs several types of aircraft for border surveillance and law enforcement purposes. These aircraft include manned helicopters, fixed-wing aircraft, UAS, and sUAS. As previously discussed in prior Privacy Impact Assessments, CBP aircraft may be equipped with video, radar, and other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR BORDER SURVEILLANCE SYSTEMS (BSS), DHS/CBP/PIA-022 (August 29, 2014), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

operation, or gathering raw data that may assist during disaster relief or emergency response operations.[2]

Reason for the PIA Update

CBP is conducting a Privacy Impact Assessment update to provide transparency for CBP's use of Tethered Small Unmanned Aircraft Systems (TsUAS). TsUAS is a surveillance system deployed by CBP to provide comprehensive situational awareness along the U.S. border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. laws enforced or administered by CBP. TsUAS include commercially available tethered unmanned aircraft with vertical take-off ability and fixed-wing unmanned aircraft platforms. TsUAS may carry optional payloads such as video surveillance systems, rangefinders, thermal imaging devices, radar, radio frequency sensors, land mobile radios (LMR),[3] or some combination thereof.

CBP will deploy TsUAS to perform the following functions:

- assist CBP in patrolling the border and responding to ground sensor[4] activations;
- enhance situational awareness for U.S. Border Patrol agents entering high risk and unfamiliar areas related to their mission;
- conduct surveillance during tactical operations;
- complement manned aircraft operations; and
- gather raw data that may assist in responses during natural disasters or other emergencies.

TsUAS are comprised of:

- an unmanned aerial vehicle;
- a fiber optic/power tether line;
- a ground power station; and
- a Ground Control System (GCS).

The TsUAS is hard wired via the tether line to the Ground Control System and communication is transferred securely over the power line. In the event of a power loss, TsUAS internal batteries enable the aircraft to continue to fly until the TsUAS can safely auto land. TsUAS are able to

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR INTELLIGENT COMPUTER ASSISTED DETECTION (ICAD), DHS/CBP/PIA-075 (November 4, 2022), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.
[3] A two-way push-to-talk radio system designed for mission critical communications.
[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR AIRCRAFT SYSTEMS), DHS/CBP/PIA-018 (2013 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

remain in the air and record video and sensor data for over 24 hours, though may only be used for CBP mission-related purposes.

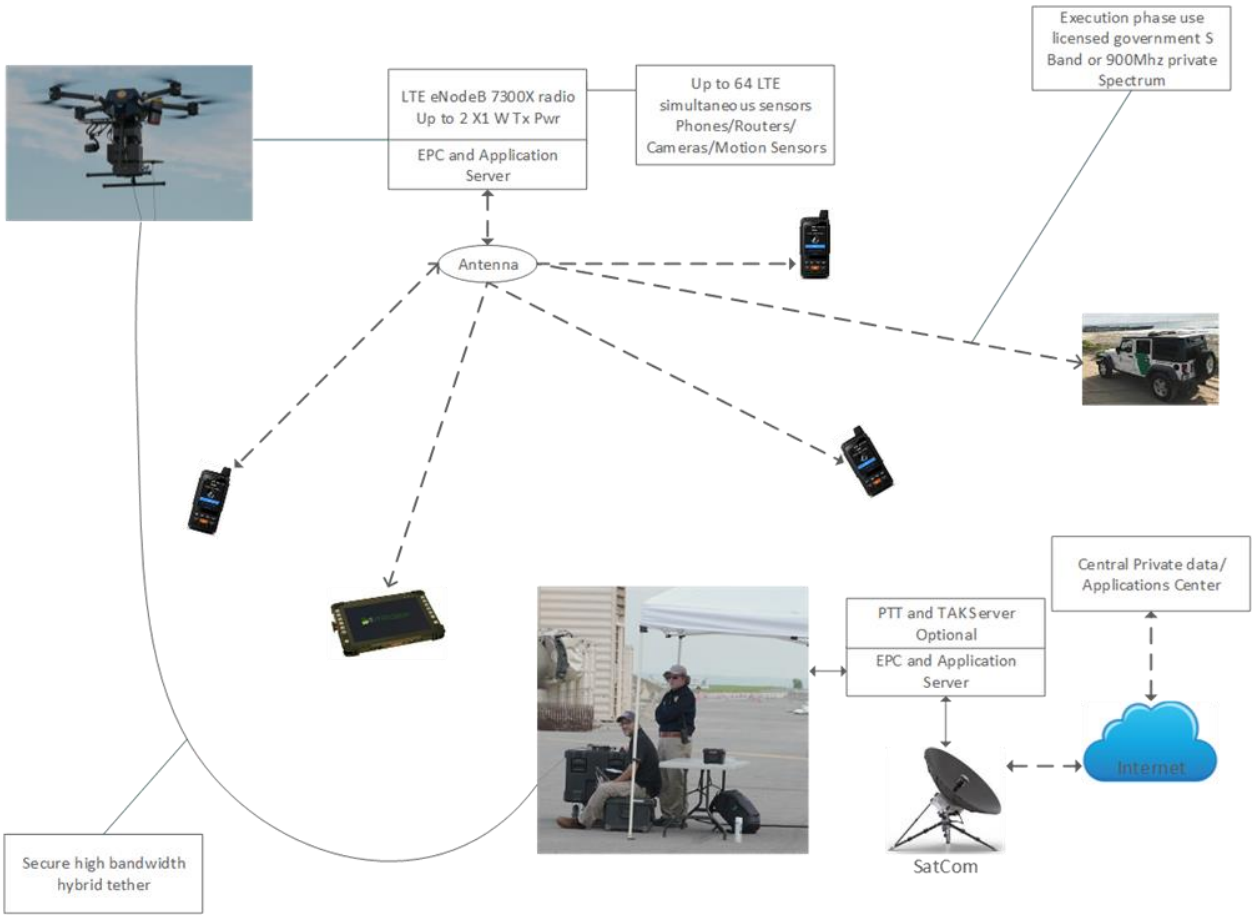
In addition to surveillance activities, CBP will be testing the mobile communication network capabilities of the TsUAS. Using the TsUAS as an antenna, U.S. Border Patrol agents operating in the field will deploy the TsUAS to provide a closed network for radio and cellular communication to other U.S. Border Patrol agents operating within a range of one to five miles of the TsUAS. The antenna on the TsUAS assists in the transmission of radio communications between the TsUAS pilot and U.S. Border Patrol agents operating within the radius of the tethered antenna. This closed network would be accessible to U.S. Border Patrol agents operating within this range and using CBP-issued handheld devices running the Tactical Awareness Kit (TAK) mobile application.[5] This functionality is not used to obtain or listen to other communication capabilities outside of the U.S. Border Patrol network. Communication among and between the U.S. Border Patrol agents will be provided through a push to talk mechanism on the CBP owned and issued handheld devices.

CBP anticipates using the TsUAS established mobile communication networks to provide secure communications between U.S. Border Patrol agents operating in the field and CBP central/regional command personnel during disaster response situations, and when standard communications methods with U.S. Border Patrol agents are inadequate.

Like traditional sUAS, TsUAS surveillance cameras and payload sensors may record border incursion activity such as people and vehicles illegally entering the United States between ports of entry, which allow U.S. Border Patrol agents to track and interdict subjects illegally entering the United States. TsUAS may collect and process Personally Identifiable Information (PII) including video images, photographs, radio frequency emissions, and location information. Not all data collected by TsUAS may be used to identify an individual at the time of collection; however, data captured using the TsUAS may later be associated with an individual, such as in their law enforcement case file. Like sUAS, sensor payloads (e.g., cameras) onboard TsUAS are oriented toward the border and away from communities and places of worship and commerce, when operationally feasible. While TsUAS may record lawful activity during official U.S. Border Patrol operations (e.g., individuals entering a local establishment, in public places, associating with other individuals, or vehicle license plates), these recordings will be overwritten unless an authorized TsUAS user determines the recording is needed for an approved purpose (e.g., associated with an apprehension). TsUAS are highly portable and can be rapidly deployed to high-risk areas, allowing CBP to reduce surveillance and situational awareness gaps related to its mission. Because TsUAS can only hover and have a limited range (400 feet above ground level),

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE TEAM AWARENESS KIT (TAK), DHS/ALL/PIA-072 (July 29, 2021), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

CBP is not required to obtain a Federal Aviation Administration (FAA) Certificate of Authorization (COA) to operate.



Patrolling the Border

TsUAS may enhance U.S. Border Patrol Agent safety by providing the capability of surveilling and detecting threats from afar before agents enter high risk areas and situations related to CBP's mission. Prior to a mission, the TsUAS operator is responsible for coordinating the TsUAS Operations Area (TOA) with local U.S. Border Patrol leadership and in support of an approved operation. For example, in Tucson Sector, U.S. Border Patrol Agents work with the Joint Intelligence Operations Center (JIOC) to de-conflict airspace in a given area. Usually, the TOA will be a 2.5-mile radius from a specific location but could be larger. Use of the airspace is

authorized for a set amount of time - usually not longer than an eight-hour period but able to be authorized for 24 hours or more consistent with the mission need.

Investigative Operations

CBP uses both manned and unmanned aircraft, including sUAS and TsUAS to support investigative operations conducted by other DHS components, such as U.S. Immigration and Customs Enforcement (ICE), and by other federal law enforcement agencies such as the Federal Bureau of Investigation (FBI) or Drug Enforcement Agency (DEA). CBP will deploy TsUAS to provide communications capabilities in areas where cellular or radio communications are limited or non-existent to facilitate government communications. The U.S. Border Patrol may use the TsUAS to create a closed radio and cellular communications network and like other radio communications, these communications are not recorded. These support missions include overhead observation of subjects of investigations, specific locations of interest, and conveyances for enhanced situational awareness and increased officer/agent safety. For example, CBP may deploy TsUAS to conduct surveillance over a building to inform ground units of the general external layout of the building or rugged or inaccessible terrain in order to provide the location of vehicles or individuals along the border and between the ports of entry.

When flying TsUAS in support of another component or government agency for an investigative operation,[6] CBP may provide the other agency with downloaded video images, photographs, radio frequency emissions, and location information of the operation, in whole or in part, based on the request and consistent with law and policy. CBP may also use TsUAS communication capabilities to communicate with other authorized federal, state, and local partners operating in the same Team Awareness Kit user group.

Disaster Support

CBP may use TsUAS during natural disasters in support of other DHS components, other federal agencies, and state and local partners. For example, CBP may use TsUAS to provide images of flooding or other damage to the Federal Emergency Management Agency (FEMA), state emergency operations centers, the United States Geological Survey (USGS), or the U.S. Army Corps of Engineers.

In general, video and other data information from these operations are not used to identify individuals and are not typically associated with Personally Identifiable Information, though may collect video and other images of individuals. As with other requests for support, disaster area

[6] CBP does not "loan out" TsUAS for other agencies to use. At all times CBP personnel will be in control of TsUAS being operated to assist another agency. TsUASs will be used to support investigative operations conducted by other DHS components, such as ICE, and by other federal law enforcement agencies, such as the FBI or DEA. All agencies must have an authorized purpose to utilize CBP TsUAS support.

overflight requests are assigned in accordance with CBP's policy regarding sUAS operations and the tasking of CBP assets.

Officer/Agent Safety and Support to State and Local Law Enforcement

Like sUAS, state and local law enforcement officials may request CBP TsUAS support in emergency situations to enhance officer safety when aerial surveillance is necessary, or the terrain is too difficult for law enforcement personnel to safely navigate in support of authorized law enforcement actions. Requests for TsUAS support are directed to the respective U.S. Border Patrol Sector Chief Patrol Agent responsible for the geographic area in which operations are to be conducted for authorization consistent with applicable law and policy. CBP may provide video images, photographs, radio frequency emissions, and location information taken during emergency situations, to other DHS components consistent with their authorities and pursuant to law and policy. Sharing of this information with state and local partners, including foreign and other authorized entities, is on a case-by-case basis as determined through CBP's Request for Information process and consistent with law and policy.

Information Captured by TsUAS

Due to the altitude at which TsUAS operate and the technical limitations of current sensors, the video images and photographs the TsUAS-deployed surveillance tools generally do not provide enough detail for an operator to determine a person's identity. The only information about individuals that is collected or retained is the indication of a human form, as well as other contextual information (e.g., that an individual is carrying a backpack or a large item, such as a long gun). Video images, photographs, radio frequency emissions, and location information captured by TsUAS, however, may be associated with a person if the person is apprehended, for instance, by inclusion in the person's case file.

Additionally, CBP obtains biographical and biometric data pertaining to the apprehended person following time of apprehension. CBP stores all biographic, biometric, and the associated case information obtained from the apprehended individual in the appropriate law enforcement case management system (in most cases, information is entered in the CBP e3 system[7]). In general, CBP maintains any related video images, photographs, radio frequency emissions, and location information obtained from the TsUAS on removable media in accordance with chain of custody protocols.

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

Video images, photographs, radio frequency emissions, and location information captured by TsUAS are recorded on the Ground Control System.[8] The controller on TsUAS platforms acts as both the Ground Control System and mechanism for controlling the platform. Data can be downloaded from the Ground Control System of an individual TsUAS system as individual video files and maintained on DVD or other CBP-approved digital medium as case file evidence for prosecution cases and for training purposes (removing any personally identifiable information before it is used for training). Data may be copied for storage for training and prosecution purposes and titled by date of incursion, TsUAS registration number, and number of individuals involved. When data is copied to a DVD for prosecution purposes, the prosecution case number will be added to the title. CBP stores DVDs consistent with its chain of custody protocols.

Following a mission, the video images, photographs, radio frequency emissions, and location information captured by TsUAS are generally not downloaded unless required as evidence for prosecution, investigation, or training purposes. Subsequently, and only upon official request, access to a particular image may be provided 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 Personally Identifiable Information. TsUAS video images, photographs, radio frequency emissions, and location information of the crossing or apprehension of persons whose apprehension is the subject of a video recording by a manned or unmanned aircraft, may be associated with a law enforcement case file that contains Personally Identifiable Information.

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. The Homeland Security Act of 2002 Section 222(2) 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. The Fair Information Practice Principles 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

[8] A Ground Control System is a land- or sea-based control center that provides the facilities for human control of the TsUAS.

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 updated Privacy Impact Assessment is conducted to relate the use of these observation and data collection platforms to the DHS construct of the Fair Information Practice Principals. This updated Privacy Impact Assessment examines the privacy impact of tethered Aircraft Systems operations as it relates to the Fair Information Practice Principals.

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.

There are no changes to the privacy risks related to the Transparency principle since issuance of the April 2018 Privacy Impact Assessment which described the privacy risks and mitigations involving sUAS. This Privacy Impact Assessment provides additional notice of CBP's use of TsUAS to monitor activities along the U.S. border.

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.

No change has occurred to the privacy risks related to the Individual Participation principle since the April 2018 Privacy Impact Assessment. The original privacy risks remain, as documented in the previous Privacy Impact Assessment in the DHS/CBP/PIA-018 series.

Like traditional fixed wing aircraft, large UAS, and sUAS, CBP primarily uses TsUAS to maintain situational awareness of the border area and to locate individuals who are crossing the border illegally or engaged in illegal activity in the border area. Allowing an individual to consent to the collection, use, dissemination, and maintenance of TsUAS video images, photographs, radio frequency emissions, and location information would compromise operations and would interfere with the U.S. government's ability to protect its borders.

In the event the TsUAS information is linked to an individual subject of a CBP law enforcement or other investigation, access procedures are described in this Privacy Impact Assessment and in the Border Patrol Enforcement Records System Of Records Notice (SORN).[9] Although the Border Patrol Enforcement Records System Of Records Notice asserts exemptions

[9] *See* DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

from the access provisions of the Privacy Act for the information maintained pursuant to its terms, such exemptions are reviewed in the context of each request. To seek access to information collected via sUAS and linked to a law enforcement case file maintained in e3,[10] individuals may request information about themselves, pursuant to the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)), as applicable, or pursuant to the Freedom of Information Act (FOIA) (5 U.S.C. § 552).

Any individual, regardless of citizenship or immigration status, may seek notification of and access to any CBP record contained in e3 pursuant to procedures provided by the Freedom of Information Act, and can do so by visiting https://www.cbp.gov/site-policy-notices/foia, or by mailing a request to:

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

When seeking records about 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 6 C.F.R. Part 5: Disclosure of Records and Information. The individual must first verify their identity, meaning that the requestor must provide their full name, current address, and date and place of birth. The requestor must sign the 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 Freedom Of Information Act Officer, https://www.dhs.gov/foia, or 1-866-431-0486. In addition, the request should:

- Explain why the requestor believes the Department would have information on them;
- Identify which component(s) of the Department the requestor believes may have requested information about them;
- Specify when the requestor believes the records would have been created; and
- Provide any other information that will help the Freedom Of Information Act staff determine which DHS Component agency may have responsive records.

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

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.

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 Privacy Impact Assessment and the Border Patrol Enforcement Records System of Records Notice describe how individuals may make access requests under the Freedom of Information Act 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 TsUAS 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 System of Records Notice. 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.

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.

There are no changes to the privacy risks associated with the Purpose Specification principle since issuance of the April 2018 Privacy Impact Assessment.

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).

There are no changes to the privacy risks related to the Data Minimization principle since issuance of the April 2018 Privacy Impact Assessment.

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.

There are no changes to privacy risks related to the Use Limitation principle since issuance of the April 2018 Privacy Impact Assessment.

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.

There are no changes to the privacy risks related to the Data Quality and Integrity principle since issuance of the April 2018 Privacy Impact Assessment.

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.

There are no changes to the privacy risks related to the Security principle since issuance of the April 2018 Privacy Impact Assessment.

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.

With the addition of TsUAS, there is no change in CBP's practices related to the Accountability and Auditing principle. 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. All U.S. Border Patrol Agents using TsUAS must be certified in operating the TsUAS. CBP requires 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. CBP employees must follow procedures to maintain an adequate chain of custody in the event that the information is used as evidence.

CBP has a process in place for restricting the dissemination of TsUAS video images, photographs, radio frequency emissions, and location information and keeps a log of the disclosures. CBP redacts law enforcement sensitive information, Personally Identifiable Information, and other sensitive related data unless the requestor has a valid need to know. CBP periodically reviews the logs or disclosure records to ensure compliance with established privacy policies, practices, and procedures for associated systems.

Contact Official

Jason D. Owens
Chief
U.S. Border Patrol
U.S. Customs and Border Protection

Responsible Official

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

Approval Signature

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

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717