Privacy Impact Assessment

for

TSA Unmanned Aircraft Systems

DHS Reference No. DHS/TSA/PIA-053

April 24, 2023

Homeland Security

Abstract

The Transportation Security Administration (TSA) is responsible for security in all modes of transportation and has broad authority to assess threats to transportation and to direct implementation of measures intended to safeguard security at airports and other transportation facilities. Among its programs, TSA conducts vulnerability assessments at airports and other transportation centers and plans to operate unmanned aircraft systems (UAS)[1] to improve these assessments. TSA may also use UAS for law enforcement operations at special events and to assist with the response to transportation incidents such as rail accidents, pipeline spills, or downed aircraft.[2] This Privacy Impact Assessment (PIA) is conducted pursuant to Section 222 of the Homeland Security Act to address privacy risks associated with TSA's use of UAS.

Introduction

Congress granted the TSA Administrator broad statutory responsibility and authority with respect to transportation security in the Aviation and Transportation Security Act of 2001 (ATSA). Under this Act, the Administrator is responsible for security in all modes of transportation, including carrying out Chapter 449 of Title 49 of the United States Code (U.S.C.), relating to civil aviation security, and related research and development activities. The Administrator is given an array of specific authorities with which to carry out that responsibility, including authority to assess threats to transportation (49 U.S.C. §§ 114(f)(2), 40113(a)); protect aircraft and air transportation, authorize arrest, secure airport access perimeters (§ 44903); and assess threats and security (§ 44904). In addition to the above-mentioned authorities, TSA may, pursuant to 49 U.S.C. § 114(p)(2), designate personnel to serve as law enforcement officers, with authority to investigate and take the appropriate law enforcement action, including for violations of 18 U.S.C. § 39B, which makes it a crime for an individual to operate an unmanned aircraft by knowingly or recklessly interfering with, or disrupting the operation of, an aircraft carrying one or more occupants; or knowingly operate an unmanned aircraft within a runway exclusion zone.

Overview

TSA will deploy UAS for specific activities to support the agency's mission to protect all modes of transportation, and, as appropriate, to provide support to other federal agencies. This Privacy Impact Assessment relates to the agency's use of UAS and does not cover use of Counter

[1] This Privacy Impact Assessment uses the term "UAS" to encompass the unmanned aircraft and its associated elements (including audio and visual communication links, cameras, and the components that control the unmanned aircraft) that are required for the safe and efficient operation of the unmanned aircraft.
[2] The use of the term "downed aircraft" in this Privacy Impact Assessment refers to any aircraft (manned or unmanned) that impacts with the ground and that has the potential to negatively affect the security of a transportation system or the safety of individuals within the vicinity of the occurrence.

Unmanned Aircraft Systems (C-UAS).[3] As detailed below, the Privacy Impact Assessment addresses TSA's use of UAS to conduct transportation facility vulnerability assessments by flying, for example, along airport perimeters, observing critical airport infrastructure, and investigating other physical security concerns within and adjacent to the airport perimeter. This Privacy Impact Assessment also provides information about TSA's use of UAS to support other federal agencies' requests for assistance at National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR)[4] events by flying UAS to observe acts that could pose threats to safety and security of those events and performing pre-event inspections for potential security vulnerabilities. Use of UAS for such events is limited to the geographic parameters established for such events. Finally, this Privacy Impact Assessment covers TSA's use of UAS to carry out TSA responsibilities such as investigating transportation incidents around transportation facilities (e.g., rail, pipeline, airports). TSA does not anticipate flying over individuals or collecting personally identifiable information (PII) in its operation of UAS during vulnerability assessments or to investigate transportation incidents. TSA may, however, fly over individuals when operating UAS for National Special Security Events and Special Event Assessment Rating events. Therefore, it may be more likely that TSA could collect personally identifiable information during such activities. TSA will protect any personally identifiable information collected during UAS operations as outlined in this Privacy Impact Assessment, and TSA and DHS policies and procedures.

UAS Functionality and Operational Rules

TSA will operate UAS equipped with cameras, including navigation cameras, color electro-optical cameras, and thermal infrared cameras. The navigation cameras do not record but create an omni-directional view in real-time, permitting the operator to have a 360-degree panoramic view with fewer blind spots than a conventional camera. The color electro-optical cameras can capture photos or record video in color and are able to zoom. Thermal cameras can also capture photos or record video and are able to zoom. The UAS operator will select whether to record video or take a photo based on the mission assignment and operational observations, consistent with applicable policies and procedures. TSA does not expect that the nature and quality of the aerial view imagery will be sufficient to make out facial features or other identifying characteristics. If circumstances warrant, the operator may activate the UAS's electro-optical camera features, for example the zoom capability, to more clearly view a potential threat and to confirm or deny a security concern. In such cases, personally identifiable information may be

[3] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT COUNTER-UNMANNED ACRAFT SYSTEMS (C-UAS), DHS/ALL/PIA-085, *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[4] A National Special Security Event is a designated event that, due to its political, economic, social, or religious significance and high visibility, may be the target of domestic/international criminal activity (e.g., terrorism). Special Event Assessment Rating events are voluntarily submitted special events, which are sent to DHS by state, local, and federal officials for a risk assessment. The two designations can cover a range of events, with Special Event Assessment Rating events generally not of the same magnitude or significance as a National Special Security Event.

observed in addition to other facts and evidence collected about the security concern or threat that could lead to an individual's apprehension by law enforcement.

As noted, UAS will be equipped with cameras that capture images and video necessary to execute TSA's various missions. For example, cameras on the UAS will be used to capture photographs of vulnerabilities around the airport perimeter environment, helping TSA easily to "see" and assess vulnerabilities without the need to have an operator physically on the ground or in a helicopter. All live video feed of the aerial views captured by the cameras is transmitted wirelessly to a ground control station (GCS).[5] The wireless transmission to the ground control station uses a data link that has an encryption key to secure the wireless communication between the UAS and the controller to minimize potential cybersecurity risks. As discussed below, TSA may also take photographs or record videos using technology attached to the UAS and stored on Secure Digital (SD) media cards to support TSA's mission as described above, consistent with TSA and DHS authorities, policies, and procedures.

TSA must adhere to Federal Aviation Administration (FAA) flight requirements for all UAS operations. The FAA has established rules for the safe operation of UAS by government agencies. Generally, there are two options for government agencies and TSA will employ each option as appropriate: (1) fly under 14 CFR part 107, the small UAS rule, which allows operations of UAS under 55 pounds at or below 400 feet above ground level for visual line-of-sight operations; or (2) fly under the statutory requirements for public aircraft (49 U.S.C. §40102(a) and § 40125) and operate with an FAA Certificate of Waiver or Authorization (COA). TSA expects to operate under Part 107 for vulnerability assessments and under Certificates of Waiver or Authorization for other missions, such as National Special Security Events and Special Event Assessment Ratings events. All TSA operators using UAS must be licensed by the FAA to operate the UAS, certified by TSA to operate the UAS by completing manufacturer developed training, and approved to fly by TSA program leadership. TSA will adjust to any new FAA flight requirements as it continues to employ UAS in pursuit of its transportation security mission.

In addition to the FAA requirements, TSA system administrators have established access controls and an approval process requiring clearance to ensure that TSA UAS operators are FAA certified, have the requisite knowledge and skill to safely operate the UAS, and understand their responsibility to protect and appropriately use the data (including personally identifiable information) the UAS may collect, whether through live feed or on Secure Digital (SD) media cards, such as video images and photographs.

TSA's Uses of UAS

[5] A ground control station is land- or sea-based hardware and software that allow UAS operators to control the UAS.

Vulnerability Assessments[6]

Among its programs, TSA conducts vulnerability assessments at many U.S. airports and other transportation centers. TSA uses a risk-based approach to conduct a specialized physical security assessment of the transportation center to identify possible vulnerabilities, provide options for consideration to mitigate those vulnerabilities, and offer best practices encountered throughout the transportation domain. The assessment process also incorporates relevant intelligence pertaining to security, such as recent attack vectors in which unauthorized access is gained to a computer or network to deliver a payload or malicious outcome, and insider threat[7] vulnerabilities. The purpose of the vulnerability assessments is to evaluate the safety and security of the transportation center's infrastructure and to evaluate its current security posture.

To assist the operator with safely flying the UAS, a live aerial visual view feed will be on for navigational purposes and to avoid any obstacles during vulnerability assessments while inspecting airport perimeters, assessing physical security measures, and identifying insider threat pathways. Use of the UAS will vary based on the type of assessment. Some vulnerability assessments will focus on the general threat to airports while others will focus on the threat to airports by individuals who fly UAS into restricted airspace. For example, when an operator assesses an airport perimeter and observes an area where someone could jump a fence and gain unauthorized access to the airport grounds, the operator will direct the UAS take a photograph of this vulnerability. In another scenario, the operator may simulate a bad actor to assess how someone could fly a UAS to exploit vulnerabilities around the airport. The operator may also use the UAS's thermal camera to assess airport critical infrastructure such as heating, ventilation, and air conditioning (HVAC) and other heat admitting systems for damage and susceptibility to tampering.

TSA does not anticipate collecting personally identifiable information from the public during these vulnerability assessments unless the operator suspects an immediate vulnerability such as observing someone jump an airport perimeter fence. In such a case, the operator must confirm and document the airport perimeter breach by taking a photograph or video. However, this aerial image would likely need to be combined with other information collected during an investigation including possible interdiction and apprehension of a suspect to confirm the identity of the individual. Only TSA officials with a need to know may use such an aerial image to initiate

[6] Vulnerability assessments include (1) UAS Threat and Vulnerability Assessments at U.S. airports and other transportation centers; (2) Joint Vulnerability Assessments at U.S. airports and other transportation centers, conducted in collaboration with the Federal Bureau of Investigation (FBI) pursuant to 49 U.S.C. § 44904; and (3) Counter- Man-Portable Air-Defense (MANPAD) Systems Vulnerability Assessments at U.S. airports and other transportation centers.

[7] Insider threats include individuals with access and/or insider knowledge that allows them to exploit vulnerabilities of the Nation's transportation systems with intent to cause harm. Insiders are, or present themselves to be, current or former transportation sector employees, contractors, or partners who have or have had authorized access to transportation sector facilities, operations, systems, and information.

a civil enforcement action against the individual as well as provide the aerial image and any other relevant investigative information to the appropriate law enforcement agencies for possible criminal prosecution. The aerial image and other investigatory information would also become part of the final vulnerability assessment report.

National Special Security Events and Special Event Assessment Rating Events

National Special Security Events are events of national or international significance as deemed by DHS, by virtue of the event's profile or status, represent a significant target, and therefore warrant additional preparation, planning, and mitigation efforts. These events have included summits of world leaders, meetings of international organizations, presidential nominating conventions, and presidential inaugurations. National Special Security Event designation requires federal, state, and local agencies to provide full cooperation and support to ensure the safety and security of those participating in or otherwise attending the event. A National Special Security Event is typically limited to specific event sites for a specified time frame. When an event is designated a National Special Security Event, the U.S. Secret Service becomes the lead federal agency in planning, coordinating, and implementing security operations. The goal of these security operations is to develop and implement a seamless security plan that will create a safe and secure environment for the public, event participants, U.S. Secret Service protectees, and other dignitaries. TSA provides law enforcement support to National Special Security Events as requested.

A Special Event Assessment Rating event is a similar event not of the same magnitude or significance as a National Special Security Event. A Special Event Assessment Rating is an interagency effort led and coordinated by DHS. The level of support provided during a Special Event Assessment Rating event begins with an annual process that relies on the voluntary participation of the states and territories to collect information on events occurring in their jurisdictions and submit them to DHS for a risk assessment. Examples of submitted events include the Super Bowl, Indianapolis 500, and the Kentucky Derby. DHS applies a risk-based methodology that considers the potential threat, vulnerability, and consequences for each event, resulting in a Special Event Assessment Rating. The U.S. Government uses the rating to inform policy decisions on the level and type of support for special events. Examples of Special Event Assessment Rating event assistance that federal agencies have provided include explosive detection canine teams, cyber risk assessments, venue screening and use of field intelligence teams, and air security and tactical operations support. TSA supports certain Special Event Assessment Rating events and may use UAS in support of, and in collaboration with the Special Events Working Group, comprised of representatives from agencies with roles and responsibilities associated with these types of events.

TSA may use UAS to support National Special Security Events or Special Event Assessment Rating events in a number of ways. For instance, TSA may use UAS to assess

appropriate placement of law enforcement personnel. In this instance, the operator would use the UAS to view an area from above to determine the best location to send law enforcement support. TSA may also use UAS to conduct venue vulnerability assessments. Additionally, TSA may use UAS to perform aerial monitoring during the National Special Security Event or Special Event Assessment Rating event. For any of these activities, the operator may activate any of the cameras on the UAS if circumstances warrant, for example, activating the thermal camera on the UAS to assist with detection of threats at night and other situations.

Due to the heightened risk level of these events, TSA may enable the camera features of the UAS in support of National Special Security Events and Special Event Assessment Rating events that permit observation of characteristics that may identify an individual upon further investigation with other facts and evidence collected from the event. For certain missions, such as searching for an individual in support of an active law enforcement investigation related to the National Special Security Event or Special Event Assessment Rating event, TSA may intentionally use the camera features to view and capture photos of suspected individuals. During events where TSA is a supporting agency, TSA may provide recorded data to the lead agency, as appropriate, as well as retain any information relevant for TSA to pursue a possible civil enforcement action related to the event.

Transportation Incident Response

Finally, TSA may use UAS to locate, respond to, and identify any risks associated with a transportation incident response or to assist other agencies who request TSA assistance in responding to a transportation incident. For example, if airport law enforcement notifies TSA of a downed aircraft near or within the airport's perimeter, TSA may deploy UAS to ensure the downed aircraft is not equipped with a hazardous payload or other type of threat to the airport. The same deployment may also take place across transportation modes as incidents arise. The deployment of UAS in support of a transportation incident response reduces potential threats to TSA employees because they do not need to be physically in the location to inspect the vulnerability. The UAS permits the TSA operator to determine potentially hazardous payloads at a safe distance, to assess the incident, and to respond appropriately, to include possible notification to an Explosive Ordnance Disposal unit.[8]

TSA may enable the camera features of the UAS to permit observation of characteristics in a transportation incident response area that may, for example, identify an individual upon further investigation and with other facts and evidence collected from the event. Further, TSA may use the UAS camera features to view, and capture photos of, certain individuals associated with an incident. For example, if in response to a downed aircraft, the TSA UAS camera reveals another

[8] Explosive Ordnance Disposal units provide subject matter expertise to deter, detect, prevent, and respond to chemical, biological, radiological, nuclear, and explosive threats to transportation systems.

UAS operator attempting to retrieve their UAS near the accident scene, TSA may provide or use the imagery to support an enforcement action against the individual. Intentional capture and use of an identifying photo would only occur as part of an investigation into a security violation or violation of criminal law related to the transportation incident. Authorized persons who have a need to know may receive access to an image only when dissemination is needed for a law enforcement activity or to support a criminal case in accordance with relevant chain of custody requirements.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[9] 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.[10]

To implement this requirement, 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.[11] 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[12] and the Homeland Security Act of 2002, Section 222.[13] Because TSA operation of UAS is a program rather than an information technology system, this Privacy Impact Assessment examines the privacy impact of TSA operation of UAS as it relates to the Fair Information Practice Principles.

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.

[9] 5 U.S.C. § 552a.
[10] 6 U.S.C. § 142(a)(2).
[11] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[12] 44 U.S.C. § 3501 note.
[13] 6 U.S.C. § 142.

This Privacy Impact Assessment provides general notice that TSA may operate UAS as part of its vulnerability assessments, in support of other agencies during National Special Security Events and Special Event Assessment Rating events, and in transportation incident response activities. Generally, when conducting vulnerability assessments, TSA will deploy the UAS's camera's navigation view for obstacle avoidance. TSA does not anticipate collecting personally identifiable information during vulnerability assessments. However, if the operator suspects a vulnerability and needs to confirm it by taking a photo/video, personally identifiable information could be collected. Even if an image is collected when the recording feature is turned on, additional information along with the aerial image would likely be necessary to identify an individual. Additionally, the UAS operator may need to zoom in to more clearly view a security concern. Likewise, in such cases, characteristics that may identify an individual may be observed. Capture of an individual's identity during an assessment would only occur as part of an investigation into a security violation or violation of criminal law.[14]

TSA must operate UAS consistent with all applicable requirements, including DHS Policy requirements, FAA Regulations, and Federal Management Regulations.[15] DHS requires that the Office of the Chief Readiness Support Officer provide a Aviation Program Certification, in writing. Additionally, TSA requires\ approval from the TSA Chief Information Security Officer (CISO) for all Aviation Program small UAS[16] assets, which must meet and adhere to the requirements in DHS Policy Memorandum 119-08, OCIO Memorandum "Interim Policy Memorandum: Securing DHS Small Unmanned Aircraft Systems (sUAS), and DHS Small Unmanned Aircraft Systems (sUAS) Cybersecurity Guidance Version 3.0," September 16, 2021.

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.

Because TSA will use UAS to conduct vulnerability assessments, support National Special Security Event and Special Event Assessment Rating events, and respond to transportation

[14] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, TRANSPORTATION SECURITY ADMINISTRATION, PRIVACY IMPACT ASSESSMENT FOR THE PERFORMANCE AND RESULTS INFORMATION SYSTEM (PARIS), DHS/TSA/PIA-038, *available at* https://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

[15] 41 CFR part 102-33.

[16] For this Privacy Impact Assessment, small UAS (sUAS) as indicated in the certification by the Office of the Chief Readiness Support Officer is the same as the term "UAS" used throughout the Privacy Impact Assessment. Small UAS means a small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the national airspace system. Small unmanned aircraft are unmanned aircraft weighing less than 55 pounds on takeoff, including everything that is on board or otherwise attached to the aircraft. 14 CFR part 107.3.

incidents, TSA cannot permit individual consent to collect personally identifiable information (i.e., facial characteristics or other identifying features). Specifically, if personally identifiable information is captured during UAS operations, collection would occur pursuant to or in support of law enforcement operations pursuant to a vulnerability assessment of an airport's perimeter or in support of a special event.

During vulnerability assessments the operator will use the live feed on the UAS for obstacle avoidance. TSA does not anticipate collecting personally identifiable information during vulnerability assessments, unless the operator suspects a vulnerability is being exploited and needs to confirm it by taking a photo/video. Even if personally identifiable information is collected, additional information along with the aerial image would likely be necessary to identify an individual.

TSA expects that it may collect personally identifiable information while operating UAS in support of National Special Security Events and Special Event Assessment Rating events. During such events, TSA may use the UAS to identify an individual, for example, while zooming in for a clearer view to confirm or deny a security concern related to the event.

Any personally identifiable characteristics associated with an individual collected by TSA will become a part of the vulnerability assessment file or a law enforcement file related to the transportation vulnerability assessment, special event, or transportation incident response. It would not be appropriate to permit individual consent for TSA's UAS collection, use, dissemination, and maintenance of personally identifiable information because individual involvement could compromise operations, interfere with the U.S. Government's ability to protect transportation facilities or other assets and enforce the law, and interfere with an investigation or criminal prosecution.

Privacy Risk: There is a risk that individuals may have their image captured without their consent.

Mitigation: This risk is partially mitigated. Notice of potential image capture is provided through publication of this Privacy Impact Assessment. Further, TSA mostly uses UAS cameras for navigational purposes; TSA does not expect imagery used for UAS navigation will be of sufficient quality to discern facial features or other identifying characteristics, unless the operator uses additional zoom features. If circumstances warrant, the operator may choose to zoom in to more clearly view a potential threat to confirm or deny a security concern. In such cases, personally identifiable information may be collected. In these instances, individuals will not be given the opportunity to consent to image collection because requesting consent would require disclosure of TSA's operations, which could compromise TSA operations, investigations, and possible prosecution, as well as interfere with the protection of transportation assets.

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.

TSA will use UAS to augment existing efforts to carry out responsibilities under 49 U.S.C. § 114(f)(2) (assess threats to transportation), § 40113(a) (general authority for transportation security), and § 44903 (protect aircraft and air transportation, authorize arrest, secure airport access perimeters). In particular, 49 U.S.C. § 44904 permits the TSA Administrator to assess current and potential threats and to conduct continuous analysis and monitoring of security threats to include conducting vulnerability assessments, assisting with National Special Security Events and Special Event Assessment Rating events, and responding transportation incidents.[17] Under 49 U.S.C. § 114(p)(2), Federal Air Marshals and other individuals designated by the TSA Administrator have authority to arrest UAS operators for violations of federal law and to seek and execute warrants for seizure of evidence, including evidence related to unlawful operation of a UAS. Under 18 U.S.C. § 39B, it is a crime for an individual to operate an unmanned aircraft by knowingly or recklessly interfering with, or disrupting the operation of, an aircraft carrying one or more occupants; or knowingly operate an unmanned aircraft within a runway exclusion zone. Additionally, TSA regulation prohibits trespassing upon or otherwise accessing secure areas of airports without authorization. Per 49 U.S.C. § 46314, a person who knowingly and willfully enters a secure area in violation of TSA's regulations could be subject to a criminal penalty.

To the extent TSA uses personally identifiable information for civil investigations of security violations or criminal investigations, TSA will use the above-mentioned authorities to investigate and take the appropriate law enforcement action. Any personally identifiable information used for investigations or law enforcement actions will become a part of the vulnerability assessment or law enforcement file.

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).

The UAS's navigation cameras will primarily be used for navigational purposes for safe operation and obstacle avoidance; TSA does not expect that the nature and quality of the aerial view imagery will be sufficient to make out facial features or other identifying characteristics. If circumstances warrant, the operator may activate the UAS's electro-optical camera features, for example the zoom capability, to more clearly view a potential threat and to confirm or deny a

[17] TSA will operate UAS pursuant to FAA statutory and regulatory requirements, as required.

security concern. In such cases, personally identifiable information may be observed in addition to other facts and evidence collected about the security concern or threat that could lead to an individual's apprehension by law enforcement.

Aerial imagery used for navigation during vulnerability assessments is not retained beyond that particular mission unless the operator identifies a vulnerability or sees an individual committing a violation. Because of the potential for a serious threat while providing support to National Special Security Events and Special Event Assessment Rating events, it is possible that TSA may capture imagery that could include individual facial and other characteristics. In this instance, TSA may retain any information relevant to ongoing investigations and/or may provide recorded data to the lead law enforcement agency, as appropriate. During transportation incident response, the UAS operator will activate video to ascertain threats to security, for example, to determine dangerous payloads.[18] If the operator identifies dangerous payloads, the operator will save that recorded data and will transfer it to the investigating agency.

Images recorded during vulnerability assessments that are eligible for retention are retained for 10 years in accordance with a National Archives and Records Administration (NARA) approved schedule (DAA-0560-2019-0011-0001). Images recorded during National Special Security Event/Special Event Assessment Rating event support are retained for 5 years in accordance with a NARA approved schedule (N1-560-06-4, Item 4). Records of images taken during transportation incident response and any images retained relevant to an ongoing investigation are destroyed 25 years after the case is closed.

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.

TSA operates UAS to conduct vulnerability assessments and may operate UAS to support special events or to respond to a transportation incident. It is possible that a subsequent law enforcement investigation related to these uses will associate the UAS imagery with an individual and additional personally identifiable information may be collected as part of the law enforcement investigation. TSA may share personally identifiable information obtained using UAS with appropriate enforcement agencies for investigation or prosecution related to the vulnerability assessment, special event support, or transportation incident response activity. TSA will also provide UAS imagery collected in support of another federal agency's coverage of a special event to that agency, as appropriate, while observing chain of custody procedures. In some instances, TSA will retain copies of the imagery. Any imagery collected by TSA will only be accessible to

[18] Payload is the object or the entity that is being carried by a UAS, exclusive of what is necessary for its flight. It includes anything additional to the UAS such as extra cameras, sensors, or packages for delivery.

those with a need to know. Agencies will retain the UAS imagery in accordance with pertinent retention policies.

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.

TSA uses UAS camera features (navigation, photos, and video) in real time when conducting vulnerability assessments, providing support to law enforcement organizations such as during special events, and responding to transportation incidents. Accordingly, the real time images are accurate, relevant, timely, and complete. Any aerial imagery that is collected is saved and maintained in accordance with the appropriate retention schedule. Outside of these circumstances, navigational imagery is not maintained beyond the deployment mission once the UAS has landed securely.

To help ensure the quality and integrity of the information collected and used as evidence, the information is maintained in its original state and the proper chain of custody is maintained. Also, TSA UAS operators train on the proper operation of the UAS and the associated video equipment. This training includes correct techniques to record evidence during flight and procedures for retaining and/or turning over recorded evidence.

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.

TSA must operate UAS in accordance with FAA UAS requirements. All TSA UAS operators must be licensed by the FAA, certified by TSA to operate the UAS, and approved to fly by program leadership. Additionally, DHS requires documented Office of the Chief Readiness Support Officer Aviation Program Certification and Component Chief Information Security Officer approval for all Aviation Program small UAS assets to ensure that each component has qualified individuals operating UAS to employ the appropriate operational safeguards.

Video, photographs, and other information that a UAS captures are subject to access controls and an approval process requiring clearance by system administrators to ensure that only authorized users with a need to know have access to the video images and photographs. Each UAS has an encryption key that will encrypt all transmissions between the UAS and ground control station. Additionally, aerial imagery will be transmitted securely using the agency's Virtual Private Network for a secure connection. Any media that the operator saves must be retained in accordance with TSA policy and procedures.

Privacy Risk: There is a risk that individual images might be intercepted between the UAS and the ground control station.

Mitigation: This risk is mitigated. TSA does not expect to collect personally identifiable information during vulnerability assessments. Because of the potential for a serious threat during National Special Security Events and Special Event Assessment Rating events, it is possible that TSA may capture imagery that could include individual facial and other characteristics. In this instance, TSA may retain any information relevant to ongoing investigations and/or may provide recorded data to the lead agency responsible for the event, as appropriate. Additionally, the UAS has an encryption key for the safe and secure transmission of images between the UAS and the ground control station to prevent interception.

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.

TSA requires all TSA employees to complete annual privacy awareness training, in addition to training on ethics and the TSA Code of Conduct. Access controls, both physical and technological, are in place to ensure only authorized access to the UAS systems and the collected data/images. All TSA UAS operators must be licensed to operate the UAS by the FAA, certified by TSA to operate the UAS, and approved to fly by program leadership. TSA performs periodic audits to ensure the training status and flight proficiency of its operators.

Contact Official

Gustaf Anderson
Transportation Security Specialist
TSA/LE-FAMS
Gustaf.Anderson@tsa.dhs.gov

Responsible Official

Peter Pietra
Privacy Officer
DHS/TSA

Approval Signature

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

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