Privacy Impact Assessment
for the

United States Secret Service
Unmanned Aircraft Systems Program

DHS/USSS/PIA-028

May 22, 2020

Point of Contact
ATSAIC Scott Windish
Office of Strategic Intelligence and Information
United States Secret Service
(202) 406-6744

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) United States Secret Service (USSS or Secret Service) is responsible for identifying threats, mitigating vulnerabilities, and creating secure environments for statutorily protected peoples, places, and events. The USSS Office of Strategic Intelligence and Information's (SII) Counter-Surveillance Division (CSD) performs observation and counter-surveillance for indicators of operations that include planning, directing, and executing observation Counter-surveillance operations are also used to detect suspicious activity or pre-incident behaviors in support of the USSS protective mission. SII is in the process of requesting funding to establish an Unmanned Aircraft Systems (UAS) Program in Fiscal Year 2022. In the interim, SII is working to secure immediate funding to evaluate readily available small UAS (sUAS). The sUAS covered by this privacy impact assessment (PIA) will be tethered and will only use optical sensors. The sUAS proof of concept pilot testing will be conducted at various test sites around the U.S. with the goal of enhancing the current CSD aerial platforms. The USSS is conducting this PIA to evaluate the privacy risks associated with sUAS observation and image capturing capabilities. This PIA is limited to the use of sUAS during protective missions. Any use of other types of sensors by USSS on USSS aircraft—including sUAS—will be addressed in a future PIA.

Introduction

The USSS is responsible for identifying threats, mitigating vulnerabilities, and creating secure environments for statutorily protected peoples, places, and events. To accomplish this mission, the USSS currently relies on other federal, state, and local government agencies to provide manned aircraft for aerial observation purposes. The USSS UAS Program is being initiated such that USSS does not have to solely rely on these external entities. The USSS UAS Program is being scaled into several progressively complex phases, in alignment with DHS acquisition policies. Initially, the program will take measured steps towards the identification of Commercial-Off-The-Shelf (COTS)/Non-Developmental Item (NDI) solutions in an effort to maximize the return on investment and minimize risks. Solutions will likely be developed in spirals, with each spiral incorporating additional capabilities. For example, the first spiral could address the protective mission first, while subsequent spirals could add the investigative mission, sensors, countermeasures, etc. If funded, a comprehensive study will identify existing COTS/NDI solutions and serve as basis of market research; provide an opportunity to develop Concept of Operations (CONOPS) for protective and investigative missions; and assist in the development of design, functional, and operational requirements.

To assist in the program development, analysis and future acquisition of such tethered sUAS technology, the USSS SII is conducting a pilot proof of concept, operational test, and

evaluation at several protected venues nationwide. The operational test and evaluation will demonstrate tethered sUAS capabilities and effectiveness in increasing overall situational awareness to the Office of Protective Operations (OPO), the Presidential Protective Division (PPD), the Vice Presidential Protective Division (VPD), and other supporting elements during Presidential and Vice Presidential visits. Various tethered sUAS and technologies will be tested against factors such as weather, payload capability, and ability to satisfy mission requirements (e.g., duration, environment, operation). The operational test and evaluation will assist future decisions on acquisition and deployment of similar systems as well as address the methods in which they are used.

Typically, the manned aircraft provided to USSS have some type of imaging capability such as video, still image collection, or forward looking infrared radiometer or radar (FLIR). These manned aircraft are used to fly over hard-to-reach or hard-to-observe areas of concern, protectee motorcade routes, protected sites, and designated National Special Security Events (NSSE). Manned aircraft typically are limited in scope, unable to provide the persistent and dedicated overhead coverage needed for USSS fixed sites secured over a longer period of time, and too loud for certain USSS protected outdoor sites or venues. Thus, USSS is considering tethered sUAS technology to meet its mission objectives.

The tethered sUAS that are expected to be a part of spiral 1 will be controlled from a Ground Control Station (GCS). This GCS laptop provides user interface software to operate the system. The tethered sUAS are programmed to autonomously fly 200-400 feet Above Ground Level (AGL), allowing the operator to control and operate the Electro Optical/Infrared (EO/IR) camera from the GCS. The camera transmits video images through the tether back to the GCS using an encrypted feed; images are not stored onboard the sUAS. The images are then uploaded from the GCS through secure USSS Field Support System (FSS)[1] servers to authorized users and decision makers for real-time operational support. All video transmitted from the GCS will be stored remotely on the FSS servers located at a USSS-controlled facility. Any images or video obtained during the pilot proof of concept and operational testing and evaluation will either be overwritten within 30 days or become part of a law enforcement investigation if appropriate. The tethered sUAS camera operator will primarily focus on the outer perimeter of the USSS-established secure zones of protection. This perimeter restriction will serve to decrease the risk of unintentional access to private locations. Images recorded from the tethered sUAS camera may be accessed only by authorized personnel with an authorized need to know, controlled through chains of custody, and stored in secure locations until it is destroyed. Further, USSS will provide notice to individuals accessing the secure area that the premises are being monitored by sUAS. [2]

[1] *See* DHS/USSS/PIA-014 Field Support System (FSS), *available at* www.dhs.gov/privacy.
[2] NOTICE: These premises are under 24-hour aerial video observation.

There is a risk that persons in range of the sUAS sensors may not be aware of the length of time that the sUAS can sustain long-range observation. The sUAS is powered through the tether and operated by personnel on the ground—allowing the team to be relieved while the sUAS is still in the air. To mitigate the risk presented by persistent observation of an area without the foreknowledge of individuals entering the area, USSS will notify all individuals residing at—or entering—the property that the premises are being monitored by sUAS.

To the extent that the tethered sUAS may be within range of private residences, there is a risk that a person's privacy might be unintentionally violated. The aircraft does not have the capability to see through walls, or otherwise collect information regarding what occurs in the interior of a building. The primary purpose of using a tethered sUAS is to provide sustained situational awareness outside and around a building or particular location. The sUAS operates at an altitude of 200-400 feet. The tether makes the system stationary, with only minor horizontal movement occurring in response to weather conditions. The sUAS will not physically intrude upon or disturb the use of private property outside of protected venues.

Further, the EO/IR cameras that will be used during the operational test and evaluation are limited in optical zoom, and the IR cameras have a limited infrared zoom. The sUAS do not have audio recording/transmission or signals intercept capabilities and are unlikely to provide images of sufficient quality to permit subjecting them to a facial recognition system. To the extent that it proves necessary to focus the EO/IR cameras on an individual, the focus will be on obtaining a physical description of the person to promote his or her expeditious interception.

Data and images captured by the tethered sUAS that need to be retained due to an incident or other investigative reason will be secured by SII and transferred to the appropriate USSS Field Office for any necessary processing, use, and dissemination. These images may contain personally identifiable information (PII) and will be controlled in accordance with USSS policies pertaining to the storage and handling of PII. Though unlikely due to the altitude at which the tethered sUAS will operate and the quality of the video obtained, the data and images collected or retained help investigators identify an individual when used in conjunction with other data such as clothing, hair color, previously taken photographs, license plates numbers, vehicle descriptions.

The USSS is expected to test sUAS if funding is secured during Fiscal Year (FY) 20 and FY 21. Following successful pilot integration tests, the USSS will continue the pilot phase through test and evaluation at protected venues to further refine tactics, techniques, and procedures for future deployments. The USSS will operate sUAS in accordance with the Federal Aviation Administration (FAA) Certificate of Authorization (COA) requirements in accordance with 14 C.F.R. Part 107 rules and guidelines. As the FAA develops its roadmap to integrate sUAS into the National Airspace System (NAS), the USSS will adjust to any new requirements and continue to employ sUAS in pursuit of its protective mission.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[3] 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.[4]

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.[5] 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[6] and the Homeland Security Act of 2002 Section 222.[7] Given that tethered sUAS and their associated devices are mechanical and operational systems rather than a particular information technology system or collections 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 tools to the DHS construct of the 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.*

This PIA provides transparency to the public about the USSS pilot proof of concept and operational testing and evaluation, to be conducted in 2020-2021 in support of the Presidential and Vice-Presidential visits to protected venues. Though unlikely due to the low altitude at which the tethered sUAS will operate and the quality of the video obtained, the data and images collected or

[3] 6 U.S.C. § 142.
[4] 6 U.S.C. § 142(a)(2).
[5] *See* 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," *available at* www.dhs.gov/privacy.
[6] 44 U.S.C. § 3501 note.
[7] 6 U.S.C. § 142.

retained help investigators identify an individual when used in conjunction with other data such as clothing, hair color, previously taken photographs, license plates numbers, vehicle descriptions.

USSS will store video and images on the USSS secure network for no more than 30 days before they are overwritten, unless those images or video need to be retained for investigative reasons. Video images that are retained for investigative reasons will be retained in accordance with the National Archives and Records Administration (NARA) approved retention schedules for the case file. Depending on the type of criminal investigative file, USSS may retain records according to NARA-approved retention schedules for a period of time between three years and 30 years, or, in limited cases, on a permanent basis.[8]

Members of the public who enter the protected venue will receive notice prior to entering that aerial observation is in progress. This PIA provides additional notice of the following:

Generally, the Privacy Act does not cover records associated with this test because they are not retrieved by an "identifying particular." Information captured by the EO/IR cameras on the tethered sUAS may become subject to the Privacy Act once it is associated with an incident or an individual under investigation. Any video images associated with criminal investigative files are covered by the either the Protection Information System SORN[9] or the Criminal Investigative Information System SORN.[10]

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.*

A traditional approach to individual participation is not always practical or possible for USSS, which has dual investigative and protective missions. The video and images obtained from tethered sUAS will be used primarily to enhance overall situational awareness around the perimeter of the USSS secure zone of protection in and around protected venues. The USSS will

[8] *See* NARA retention schedules N1-87-92-2, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-92-002_sf115.pdf and N1-8788-1, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-ofhomeland-security/rg-0087/n1-087-88-001_sf115.pdf.
[9] *See* DHS/USSS-004 Protection Information Systems SORN, 76 FR 66940 (October 28, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.
[10] *See* DHS/USSS-001 Criminal Investigation Information System SORN, 76 FR 49497 (August 10, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.

provide notice to the public before accessing the zone of protection that aerial observation is in progress.

Any images or video obtained during the operational test and evaluation flights will either be overwritten within 30 days or become part of a law enforcement investigation. DHS/USSS-001 Criminal Investigative Information System permits information gathered by sUAS to be excluded from the access and certain redress provisions of the Privacy Act. For those who are eligible for redress, access requests should be directed to Communications Center, FOIA/PA Officer, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223, and will be considered on a case-by-case basis. Consequently, there is no mechanism for correction or redress for the video collected by the tethered sUAS. the individual must follow the procedure outlined in the corresponding privacy documents for the respective criminal investigation system. While individuals cannot alter in the initial collection of this information, they may contest or seek redress through any resulting proceedings brought against them.

Privacy Risk: There is a risk that images of individuals outside the zone of protection will not receive notice of the video collection and may have their image captured without their consent. Individuals who see the notice and choose not to enter the secure zone during the testing may still have their images captured despite declining to consent due to their proximity to the secure perimeter.

Mitigation: This risk is partially mitigated. Individuals outside the secure zone of protection may not always be given the opportunity to consent to image collection, as it may compromise protective operations and interfere with the USSS's ability to carry out its mission. Additionally, USSS will use the Office of Media Relations to provide notice to the public and media if it is determined there would be an increased risk to the public due to the location of the protected venue. However, USSS will be operating at a high altitude, the images will not be associated with the individual unless integrated into an incident or criminal investigative reason, and will be overwritten after 30 days, unless the image becomes associated with an investigative or incident record.

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.*

USSS SII's CSD performs observation for indicators and participates in operations that include planning, directing, and executing observation and counter-surveillance operations to better detect suspicious activity or pre-incident behaviors in support of the USSS protective mission. USSS has the statutory authority and responsibility to conduct criminal investigations and provide protection for the President, Vice President, their families, visiting heads of state, National

Special Security Events (NSSE), and other designated individuals.[11] Furthermore, USSS is authorized to enforce zones of protection.[12]

These authorities allow the USSS to use the camera on the tethered sUAS to capture video and still images for the purpose of increasing situational awareness, promoting officer safety, and detecting suspicious activity in support of the USSS protective mission. The USSS may use information captured from and stored on the camera systems to apprehend individuals in violation of the law or provide evidence supporting suspicious activity.

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).*

USSS seeks to minimize the collection and retention of video, data, and still images to that which is necessary and relevant to carry out its dual missions. Accordingly, during the pilot proof of concept and operational test and evaluation, all video, data, and still images obtained via the tethered sUAS that do not pertain to an incident or investigation will be stored on the secure USSS FSS servers until they are overwritten within 30 days, consistent with NARA-approved records schedule: DAA-0087-2014-0001, "Security Camera Recordings and Associated Data." USSS will not associate the images with an individual unless it becomes part of an incident or investigative file; in such cases the relevant footage associated with a specific event, occurrence, or time period, needed for prescribed law enforcement purposes (e.g., required for court; subpoena; after action analysis, and/or training), and/or in support of any authorized investigation, will be destroyed three years after the date the specific event or occurrence was first recorded; or when no longer needed; or with corresponding criminal investigative materials, whichever is later. Recordings associated with a highly unusual incident, occurrence, or significant event such as an assassination attempt or successful assassination will be transferred to NARA as permanent records after the corresponding investigation has been completed.[13]

[11] 18 U.S.C. § 3056.
[12] 18 U.S.C. § 1752.
[13] Criminal investigation records: N1-087-89-02 for Field Offices and N1-087-92-002 for Headquarters.

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.*

This pilot proof of concept and operational test and evaluation of tethered sUAS capabilities and effectiveness are for the limited purpose of increasing overall situational awareness to OPO, PPD, and other supporting elements during Presidential and Vice-Presidential visits. These operational tests and evaluations will assist future decisions on acquisition and deployment of similar systems. Should data and images captured by the tethered sUAS need to be retained for a criminal investigative reason, the video and images may be shared with federal and/or state agencies or with law enforcement entities that support the USSS protected sites and persons. Any sharing would be covered under the Protection Information System SORN[14] or the Criminal Investigative Information System SORN.[15]

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.*

For the purposes of spiral 1 operational tests and evaluations, the goal is to test and evaluate how the overhead perspective afforded by the tethered sUAS enhance overall situational awareness around the perimeter of the USSS secure zones of protection. The focus of the operational test and evaluation is on how the EO/IR camera captures physical characteristics of an individual and not the individual's actual physical facial identity. The EO/IR cameras envisioned for use during the testing do not produce images of sufficient quality to support their use by a facial recognition system. During the proof of concept pilot testing, there is no intent to collect PII, though some may be inadvertently captured by the cameras.

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.*

---

[14] *See* DHS/USSS-004 Protection Information Systems, 76 FR 66940 (October 28, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27883.htm.
[15] *See* DHS/USSS-001 Criminal Investigation Information System, 76 FR 49497 (August 10, 2011), *available at* https://www.gpo.gov/fdsys/pkg/FR-2011-08-10/html/2011-20226.htm.

The tethered sUAS system will pass encrypted live video feeds and control information through a microfilament wire running from the aircraft to the GCS. The image data is then decrypted and brought inside the USSS network firewall from the GCS where the USSS FSS's servers can then provide a video feed to the designated decision makers and other authorized receivers of that data. These video images will be maintained on the secured server for a maximum of 30 days and then will be overwritten. The FSS servers are located at a USSS controlled facility.

Strict access controls and system administrators ensure that only authorized users with an operational need to know will have access to the video feeds. Any recorded data, video, or still images that are saved to be used as evidence will be handled in accordance with USSS policy[16] and as outlined in Section 6 of this PIA.

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 USSS employees and contractors receive annual privacy and security training to ensure they understand how to handle and secure PII. Additionally, all agency employees receive training on ethics and the USSS Code of Conduct. Furthermore, there are technological and physical controls in place to ensure that there is only authorized access to the sUAS and the collected data/images.

Periodic audits will be conducted to ensure that the tethered sUAS are being used appropriately and that data is properly disposed of within the 30-day period. When the UAS moves past the spiral 1 funding and product test phases covered by this PIA, the USSS UAS Program will finalize its policies and procedures currently in development for audit policy definition and implementation. The USSS UAS Program Manager will be minimally expected to:

- Audit the flight logs biannually;
- Document the results of the audits; and
- Prepare an annual report for review by the Director, which includes the total number of flights, total time of operation of the sUAS, the total cost of sUAS operations (includes personnel, training, safety issues and resolutions, equipment and maintenance), community feedback and concerns, and any such other information as deemed relevant by the Director.

[16] *See* Professionalism with the Workforce, Fiscal Year 2015 Report to Congress (July 17, 2015), *available at* http://www.dhs.gov/sites/default/files/publications/United%20States%20Secret%20Service%20%28USSS%29%20-%20Professionalism%20within%20the%20Workforce.pdf.

Conclusion

This pilot proof of concept and operational test and evaluation will assist the USSS in determining the effectiveness and utility of the tethered sUAS to increase situational awareness and improve the USSS's ability to detect suspicious persons, activities, and pre-incident behaviors around protected sites and persons. The USSS has implemented proper access controls, procedures, and protocols to ensure that stored video and images are properly handled and that proper protections and safeguards are in place to protect any PII/SPII.

Responsible Officials

ATSAIC Scott Windish
Office of Strategic Intelligence and Information
United States Secret Service

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security