Privacy Impact Assessment
for the

United States Secret Service
Counter Surveillance Division
Unmanned Aircraft Systems Program Test

DHS/USSS/PIA-020

August 2, 2017

Point of Contact
SA Rich Ricciardi
Counter Surveillance Division
United States Secret Service
(202) 841-3837

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

Abstract

The Department of Homeland Security (DHS) United States Secret Service's (USSS or Secret Service) Counter Surveillance Division (CSD) is conducting a Proof of Concept to test and evaluate a tethered small Unmanned Aircraft System (sUAS) during a Presidential visit to the Trump National Golf Club, Bedminster, New Jersey, in August 2017. The Proof of Concept will help determine the potential future use of tethered sUAS in supporting the Agency's protective mission. The tethered sUAS used in the Proof of Concept is operated using a microfilament tether that provides power to the aircraft and the secure video from the aircraft to the Operator Control Unit (OCU). The sUAS is equipped with electro-optical (EO) and infrared (IR) camera. USSS is conducting this privacy impact assessment (PIA) to evaluate the privacy risks associated with tethered sUAS's surveillance and image capturing capabilities. This PIA is limited to covering the use of EO/IR sensors on a single tethered sUAS during one event. Any other use of these types of sensors by USSS on USSS aircraft—including sUAS—will be addressed in a future PIA.

Introduction

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. To accomplish this mission, the USSS currently relies on other federal, state, and local government agencies to provide manned aircraft for aerial surveillance purposes. Typically, these manned aircraft have some type of imaging capability such as video, still images 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). Unfortunately, the manned aircraft usually used are limited in scope, unable to provide a persistent and dedicated overhead coverage for USSS fixed sites secured over a longer period of time, and too loud for certain USSS protected outdoor sites or venues.

In recent years, companies developed tethered small Unmanned Aircraft System (sUAS) technology as a potential viable tool for law enforcement to increase overall situational awareness during large outdoor public events. In 2017, the Massachusetts State Police used tethered sUAS technology to support the Boston Marathon, Fourth of July, and the Boston Operation Sail (OPSAIL) events. Tethered sUAS technology has also benefited the military as a tool to increase situational awareness for decision makers, planners, and security personnel.

To assist in the analysis and potential acquisition of such tethered sUAS technology for use in its mission objectives, the USSS Counter Surveillance Division (CSD) is conducting a Proof of Concept at the Trump National Golf Club, Bedminster, New Jersey in August 2017. The Proof of

Concept will test and evaluate a tethered sUAS's capabilities and effectiveness in increasing overall situational awareness to the Office of Protective Operations (OPO), the Presidential Protective Division (PPD), and other supporting elements during a Presidential visit to his Bedminster, New Jersey residence. This Proof of Concept will assist future decisions on acquisition and deployment of similar systems. This privacy impact assessment (PIA) is necessary because the aircraft is equipped with technology that captures information that may be associated with persons who USSS encounters.

The tethered sUAS used for the Proof of Concept is controlled from the Operator Control Unit (OCU), which is a laptop that provides user interface software to operate the system. The tethered sUAS is programmed to autonomously fly 300-400 feet Above Ground Level (AGL), allowing the operator to control and operate the Electro Optical/Infrared (EO/IR) camera from the OCU. The camera transmits video images through the tether back to the OCU using an encrypted feed; images are not stored onboard the sUAS. The images are then uplinked from the OCU 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 OCU will be stored remotely on the FSS servers located at a USSS-controlled facility. Any images or video obtained during the Proof of Concept in Bedminster, New Jersey will either be overwritten within 30 days or become part of a law enforcement investigation case file, if appropriate. The tethered sUAS camera operator will primarily focus on the outer perimeter of the USSS-established secure zones of protection in and around the Trump National Golf Club. This perimeter restriction and notification will serve to decrease the risk of unintentional privacy violations. Images recorded from the tethered sUAS camera may only be accessed by authorized personnel with an authorized need to know, controlled through chains of custody, and stored in secure locations until it is destroyed.

There is a risk that persons in range of the sUAS sensors may not be aware that the sUAS can provide long-range surveillance for a long time since 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 surveillance 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.[2] USSS has strict mission priorities for this pilot.

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, nor is that its purpose. The primary purpose of using a tethered sUAS is to provide sustained situational awareness. The sUAS operates at an altitude of 300-400 feet. The

[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 surveillance.

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 the Trump National Golf Course.

Further, the EO camera that will be used during the Proof of Concept is limited to a 30x optical zoom and the IR camera is limited to an 8x infrared zoom. The sUAS does not have audio or signals intercept capabilities and does not 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 camera on an individual, the focus will be on obtaining a physical description of the person to promote his 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 CSD 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.

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 PII. 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.[3] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure the Homeland.

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 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 this observation tools to the DHS construct of the FIPPs. This PIA examines the privacy impact of tethered sUAS operations as it relates to the FIPPs.

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

1. Principle of Transparency

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

This PIA provides transparency to the public about the USSS Proof of Concept at The Trump National Golf Club in Bedminster, New Jersey, to be conducted in August 2017 in support of the Presidential visit to the facility. 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 may be clear enough to help investigators identify an individual when used in conjunction with other data (e.g., 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, unless those images or video need to be retained for investigative reasons, otherwise they will be overwritten within 30 days. Video images that are retained for investigative reasons will be associated with an investigative case file, and retained in accordance with the NARA-approved retention schedules for the case file. Depending on the type of case file, USSS may retain records according to NARA-approved retention schedules for a period of time between 3 years and 30 years; or in limited cases, on a permanent basis by NARA.[4]

Members of the Trump National Golf Club and accompanying guests who enter the premises will also receive notice prior to entering the club that aerial surveillance is in progress. This PIA provides additional notice of the following:

Generally, records associated with this test are not covered by the Privacy Act because they are not retrieved by an individual identifier. 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 that individual's case file are covered by the either the Protection Information System SORN[5] or the Criminal Investigative Information System SORN.[6]

---

[4] *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 N1-87-88-1, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0087/n1-087-88-001_sf115.pdf.

[5] *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.

[6] *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.

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 the tethered sUAS will be used primarily to enhance overall situational awareness around the perimeter of the USSS secure zone of protection in and around the Trump National Golf Club. The USSS will provide notice to the public, club members, and employees before accessing the zone of protection that aerial surveillance is in progress.

Any images or video obtained during the Proof of Concept in Bedminster, New Jersey will either be overwritten within 30 days or become part of a law enforcement investigation case file. Providing individuals of interest access to information about them in the context of a pending law enforcement investigation may alert them to or otherwise compromise the investigation. Consequently, there is no mechanism for correction or redress for the video collected by the tethered sUAS. Once that video is associated with an individual's case file, the individual must follow the procedure outlined in the corresponding privacy documents for the respective criminal investigation system. While individuals cannot participate in the initial collection of this information, they may contest or seek redress through any resulting proceedings brought against them.

Privacy Risk: There is a risk that images of individuals outside the zone of protection will not receive notice of the test and may have their image captured without their consent. Individuals who see the notice and chose not to enter the club during the testing may still have their images captured despite declining to consent due to their proximity to the club's 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. However, USSS will be operating at a high altitude and the images will not be associated with the individual 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.*

CSD performs surveillance for indicators and operations that include planning, directing, and executing surveillance 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.[7] Further, USSS is authorized to enforce zones of protection.[8]

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, officer safety, and to assist in 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 this Proof of Concept, all video, data, and still images obtained via the tethered sUAS that does not pertain to an incident or investigation will be stored on the secure USSS FSS servers until it is overwritten within 30 days, consistent with NARA approved Records Control Schedule number 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 3 years after the date the specific event or occurrence was first recorded; or when no longer needed; or with corresponding case file materials, whichever is later. Recordings associated with

[7] 18 U.S.C. § 3056.
[8] 18 U.S.C. § 1752.

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.

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 Proof of Concept testing and evaluation of a tethered sUAS's capabilities and effectiveness is for the limited purpose of increasing overall situational awareness to the Office of Protective Operations (OPO), the Presidential Protective Division (PPD), and other supporting elements during a Presidential visit to his Bedminster, New Jersey residence. This Proof of Concept will assist future decisions on acquisition and deployment of similar systems. Should data and images captured by the tethered sUAS need to be retained due to an incident or other investigative reason, the video and images may be shared with the military, or other federal, state, or local law enforcement agencies that support the USSS during the Presidential visit to the Trump National Golf Club. Any sharing would be covered under the Protection Information System SORN[9] or the Criminal Investigative Information System SORN.[10]

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 the Proof of Concept, PII captured by the tethered sUAS has no continuing value in the law enforcement context; rather, the goal is to test and evaluate how the overhead perspective afforded by the tethered sUAS enhances overall situational awareness around the perimeter of the USSS secure zone of protection at the Trump National Golf Club. The focus of the Proof of Concept is on how the EO/IR camera captures physical characteristics of an individual and not on determining the individual's actual physical identity. The EO/IR camera used during the testing does not produce images of sufficient quality to support their use by a facial recognition system.

---

[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.

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.*

The tethered sUAS system will pass encrypted live video feeds and control information through a micro-filament wire running from the aircraft to the OCU. The image data is then decrypted and brought inside the firewall and secured network from the OCU where the FSS's servers can then provide a video feed to the designated decision makers and 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 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 is being used appropriately and that data is properly disposed of within the 30 day period.

Conclusion

This Proof of Concept will assist the USSS to determine 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 PII.

Responsible Officials

SA Rich Ricciardi
USSS Counter Surveillance Division
(202) 841-3837

Latita Payne
USSS Privacy Officer
(202) 406-5838

Approval Signature

Original, signed copy on file with DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security