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

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	Testing of Department of Defense Counter Unmanned Aerial Systems Technology		
Component:	U.S. Secret Service (USSS)	**Office or Program:**	Special Operations Division (SOD), Airspace Security Branch (ASB)
Xacta FISMA Name (if applicable):		**Xacta FISMA Number (if applicable):**	Click here to enter text.
Type of Project or Program:	**Program**	**Project or program status:**	**Development**
Date first developed:	**October 16, 2014**	**Pilot launch date:**	**February 23, 2015**
Date of last PTA update	**N/A**	**Pilot end date:**	**February 27, 2015**
ATO Status (if applicable)	**Not started**	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	(b) (6), (b) (7)(C)		
Office:	Special Operations Division, Airspace Branch	**Title:**	Electronics Engineer
Phone:	(b) (6), (b) (7)(C)	**Email:**	(b) (6), (b) (7)(C) @usss.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Click here to enter text.		
Phone:	Click here to enter text.	**Email:**	Click here to enter text.

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Choose an item.

Please provide a general description of the project and its purpose in a way a non-technical person could understand. If this is an updated PTA, please describe what changes and/or upgrades that are triggering the update to this PTA. If this is a renewal please state whether or not there were any changes to the project, program, or system since the last version.

This PTA is being submitted at the request of the DHS Privacy Office.

On October 16, 2914, the United States Secret Service (USSS) entered into a Memorandum of Agreement (MOA) with the Aviation and Missile Research, Development and Engineering Center (AMRDEC) of the U.S. Army. Pursuant to that MOA, the AMRDEC and USSS SOD-ASB conducted testing over the course of five days, from February 23 through February 27, 2015, to determine the capabilities of a (b) (7)(E) system to locate and counter Unmanned Aerial Systems (UASs). Part of that testing included nighttime flights of UASs in restricted airspace (as defined by 14 C.F.R. Part 93) in Washington, D.C. The UASs were not flown over private property. These UAS flights took place during the evening hours of February 25 and 26, 2015. All required authorizations/waivers were obtained from the Federal Aviation Administration prior to conducting these test flights. The purpose of these nighttime UAS flights was to measure the capabilities of the (b) (7)(E) system to detect and counter UASs.

During the two evenings when UASs were part of the tests, multiple UASs were utilized, the majority of which are owned by AMRDEC. Two UASs owned by the USSS were used in this test. The two UASs owned by the USSS and used in the test each contain an on-board camera that is used for see-and-avoid purposes during flight, *i.e.*, the UAS operator uses the camera to "see" where the UAS is going and to control and steer the vehicle when it is not in visual range. The images "seen" by the UAS are relayed to and recorded on the operator's control panel module. The on-board cameras do not themselves retain any data. The capturing of images by the on-board cameras cannot be turned off and is incidental and part of the normal operation of the UAS. Such images were irrelevant to the testing being conducted and the purposes for which the UASs were being used as part of that testing.

Neither the UASs nor the (b) (7)(E) system are being used as surveillance systems. Operation of the on-board camera was necessary for safe navigation of the UAS. (b) (7)(E) (b) (7)(E) (b) (7)(E). Furthermore, all captured images were subsequently deleted from the control panel.

There are currently no plans for further testing of the (b) (7)(E) system using UASs in D.C. restricted airspace.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and*	☐ Closed Circuit Television (CCTV) ☐ Social Media

want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.	☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☒ This program does not collect any personally identifiable information[2] ☐ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?	
Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individuals. None.	
4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text. Not applicable.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. Please describe applicable information sharing governance in place:
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.
[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Latita Payne**
Date submitted to Component Privacy Office:	**February 26, 2015**
Date submitted to DHS Privacy Office:	March 13, 2015
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
USSS FOIA and PA Program recommends that the UAS project is not privacy sensitive because it does not collect or process personally identifiable information. USSS FOIA and PA Program will draft any required privacy documentation for any related project that collects, or could in anyway collect, PII.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	**1069598**
Date approved by DHS Privacy Office:	March 17, 2015
PTA Expiration Date	March 17, 2016

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	Other If "other" is selected, please describe: Click here to enter text.

Determination:

☐ PTA sufficient at this time.

☐ Privacy compliance documentation determination in progress.

☐ New information sharing arrangement is required.

☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies.

☐ Privacy Act Statement required.

☒ Privacy Impact Assessment (PIA) required.

☐ System of Records Notice (SORN) required.

☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

	☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**New PIA is required.** If covered by existing PIA, please list: New FIPPs based PIA required.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

In light of recent media reports about the UAS flights, the DHS Privacy Office requested this PTA from USSS. The DHS Privacy Office finds that the USSS nighttime UAS flights to measure the capabilities of the (b) (7)(E) system to detect and counter UASs was a privacy-sensitive test that occurred in February 2015. While it is our understanding that the UAS test did not collect PII and would not require a PIA or SORN under the E-Government Act and Privacy Act respectively, the DHS Chief Privacy Officer is responsible for "assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information" (Section 222 of the Homeland Security Act). To accomplish this statutory requirement, we regularly conduct Privacy Impact Assessments on *technologies* that may be considered privacy sensitive.[5]

Therefore, DHS Privacy Office requires USSS to conduct a FIPPs-based PIA to fully describe this test and the privacy risks and mitigations. Our understanding, based on this PTA, and a high level briefing from the operators, is that this is actually a positive privacy story to tell.

Though this PIA will publish after the test conducted, it will provide transparency to the public, document the privacy-protective measures that USSS incorporated into the test, and clarify any media inaccuracies.

While the DHS compliance posture for component use of UAS and drones is still evolving, the following factors contribute to our determination as to whether a PIA is required:

1. Whether the UAS flies over inhabited public spaces (as opposed to military airspace);
2. Whether the UAS has the capability to collect images of members of the public; and
3. Whether the existing public perception of the UAS program warrants additional transparency from DHS to maintain the public trust in DHS operations.

The DHS Privacy Office finds that the USSS UAS test from February 2015 meets all three of these factors and therefore a new FIPPs-based PIA is required. Note that CBP and S&T have also completed PIAs for their use of UAS.[6] This PTA expires in one year.

[5] For example, please see the TSA FIPPs-based PIA regarding Advanced Imaging Technology (AIT): http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf.
[6] DHS/CBP/PIA-018 Aircraft Systems, http://www.dhs.gov/publication/dhscbppia-018-aircraft-systems and DHS/S&T/PIA-026 Robotic Aircraft for Public Safety (RAPS) Project, http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_st_raps_nov2012.pdf

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**Unmanned Aerial Systems**		
Component:	U.S. Secret Service (USSS)	**Office or Program:**	Counter Surveillance Division
Xacta FISMA Name (if applicable):	Click here to enter text.	**Xacta FISMA Number (if applicable):**	Click here to enter text.
Type of Project or Program:	**New project**	**Project or program status:**	**Development**
Date first developed:	**March 27, 2017**	**Pilot launch date:**	Click here to enter a date.
Date of last PTA update	Click here to enter a date.	**Pilot end date:**	Click here to enter a date.
ATO Status (if applicable)	Choose an item.	**ATO expiration date (if applicable):**	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	**Rich Ricciardi**		
Office:	**Counter Surveillance Division**	**Title:**	Special Agent
Phone:	**202-841-3837**	**Email:**	(b) (6), (b) (7)(C) @usss.dhs.gov

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	Click here to enter text.		
Phone:	Click here to enter text.	**Email:**	Click here to enter text.

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: Choose an item.

The United States Secret Service is developing a program to incorporate the use of several types of Unmanned Aerial Systems (UAS) and tethered systems as a tool to further the Agency's protective mission. The Agency currently utilizes a manned aircraft platform ([redacted] for aerial counter-surveillance purposes. The intent behind the use of the UAS and tethered systems is to increase situational awareness around our protectees and enhance our current aerial counter-surveillance platforms.

These UAS and tethered systems will be deployed between [redacted] feet above the protected venue.. They will be equipped with [redacted] zoom Electro Optical (EO), Infrared (IR), [redacted] cameras. [redacted] While EO/IR cameras are not identical in size and capabilities they are similar in performance specifications. These systems will provide an overall "bird's eye view" of the environment, with the capabilities of taking and recording video and taking still photos. They will not have audio capabilities.

During UAS operations, the UAS operator's crew (remote pilot in command) will be required to maintain visual line of sight of the aircraft at all times for safe maneuvering of the UAS itself and to see and avoid other aircraft and infrastructure and will ensure radio line of sight is maintained throughout the flight. The UAS's autopilots and related autonomy capabilities will assist the operator(s) in maintaining a safe distance between the aircraft and obstacles and infrastructure. The operator will also have control of the camera, and will control its direction of view as well as determining when to zoom in/pan out.

Tethered UAS operations will provide the USSS with a small, quiet, long-endurance imaging capability [redacted]. The microfilament tethered system provides secure communication and ensures continuous flight with an operational altitude of 400 feet.

The EO/IR cameras on these systems will have digital zoom capability that could assist the operator with identifying such detail as a vehicle license plate or to estimate a person's physical characteristics such as [redacted] and hair color. The data collected by the tethered system will be limited to the extent necessary for the USSS to implement protective measures and to assist in its protective mission.

The live video feed or still pictures captured from the EO/IR camera will be transferred from the camera to the UAS ground control station (GCS) through an encrypted feed. Once this happens it may be pushed to other USSS personnel on a secure USSS system. Any video files that are retained will be associated with a corresponding investigative case file.

All video, still pictures, and other data not pertaining to an incident obtained through the UAS or tethered system will be stored on the digital video recorders and will be overwritten within 30 days. Data would only be maintained beyond 30 days if it pertains to an incident that is connected to a USSS protective function. Such data will be retained in accordance with the needs of a law enforcement or protective action, the approved records retention schedules, and applicable DHS policy; and will be stored in secure facilities with proper environmental controls as described in USSS directive.

UAS will only be operated by USSS authorized personnel that have been certificated to operate UAS by the FAA. Additionally, USSS personnel whose responsibility it is to manage, supervise, maintain, fly or use UAS systems will receive mandatory training on USSS/DHS policies.

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☒ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☐ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☐ This program does not collect any personally identifiable information[2] ☒ Members of the public ☒ DHS employees/contractors (list components): ☒ Contractors working on behalf of DHS ☒ Employees of other federal agencies

4. What specific information about individuals is collected, generated or retained?
Please provide a specific description of information that is collected, generated, or retained (such as names, addresses, emails, etc.) for each category of individuals. **Photographic images of groups, individuals, and vehicle license plate numbers**

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list: Click here to enter text.
6. Does this project, program, or system connect, receive, or share PII with any external (non-DHS) partners or systems?	No. X Yes. If yes, please list:

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

	It is contemplated that this program may have the capability to share photographic images with local and state law enforcement.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	Choose an item. Please describe applicable information sharing governance in place: It presently is not, but if any sharing were to take place it would be for law enforcement purposes only and in exigent circumstances until an appropriate ISAA or policy is concluded.
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	No. X Yes. If yes, please list: It is contemplated that individuals utilizing this platform will be trained in its operation and capabilities.
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☐ No. What steps will be taken to develop and maintain the accounting: ☒ Yes. In what format is the accounting maintained: Will conform to USSS Policy on FOIA requests. Transactional audit logs are generated and kept in text file format.
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☒ No. ☐ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☐ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☐ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☐ High ☐ Undefined

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b) (6), (b) (7)(C)
Date submitted to Component Privacy Office:	**March 29, 2017**
Date submitted to DHS Privacy Office:	April 6, 2017
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
Unmanned Aerial Systems (UAS) will be a privacy sensitive system, requiring both PIA and SORN coverage. A new PIA will be required to cover the images, PII, captured by the EO/IR cameras. SORN coverage is provided by DHS/USSS-004 Protection Information System.	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b) (6), (b) (7)(C)
PCTS Workflow Number:	**1141513**
Date approved by DHS Privacy Office:	May 5, 2017
PTA Expiration Date	May 5, 2018

DESIGNATION

Privacy Sensitive System:	Yes If "no" PTA adjudication is complete.
Category of System:	IT System If "other" is selected, please describe: Click here to enter text.
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required.

	☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer. ☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	**New PIA is required.** If covered by existing PIA, please list: Click here to enter text.
SORN:	**System covered by existing SORN** If covered by existing SORN, please list: DHS/USSS-004 - Protection Information System October 28, 2011 76 FR 66940

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

The DHS Privacy Office finds that the Unmanned Aerial Systems (UAS) and tethered systems program being developed by the USSS represents a privacy-sensitive effort, and requires both PIA and SORN coverage. The use of UAS and tethered systems is designed to increase situational awareness around USSS protectees and enhance our current aerial counter-surveillance platforms. The systems will employ (b) (7)(E) zoom Electro Optical (EO), Infrared (IR), (b) (7)(E) cameras in order to capture video and still images, and will be capable of capturing information such as license plates and the physical characteristics of individuals involved in incidents or events related to a protectee. Any images captured by these systems, and are determined to be of investigative value, will be retained in association with a corresponding case file. Any images captured that do not pertain to an incident will be overwritten within 30 days of capture.

The DHS Privacy office finds that due to the privacy sensitive nature of UAS technology, a PIA is needed in order to sufficiently identify the privacy risks and mitigations associated with the use of Unmanned Aerial Systems (UAS) and tethered systems as a tool to further the Agency's protective mission. SORN coverage is provided by DHS/USSS-004 - Protection Information System, which outlines the Secret Service's collection and maintenance of records in order to assist the USSS in protecting its protectees and to investigate individuals who may come into proximity with a protectee, including individuals who have been involved in incidents or events which relate to the protective functions of the USSS, and individuals who have sought to make contact with a protectee.