Privacy Impact Assessment
for the

United States Secret Service
Special Operations Division
Counter-Unmanned Aircraft Systems in support of United Nations General Assembly

DHS/USSS/PIA-025

September 12, 2019

Point of Contact
Linda Canfield
USSS Special Operations Division
(202) 406-7135

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The United States Secret Service's (USSS or Secret Service) Special Operations Division (SOD) is conducting a pilot, in coordination with the U.S. Coast Guard (USCG) and Science & Technology Directorate (S&T), to test and evaluate technologies used to detect, identify, and mitigate Unmanned Aircraft Systems (UAS) that may pose a potential threat to "covered facilities" and assets at the September 2019 United Nations General Assembly (UNGA). These protective technologies are referred to as Counter-UAS (C-UAS) systems. This Privacy Impact Assessment (PIA) discusses measures taken to mitigate privacy risks and the impact to protect personally identifiable information (PII) during the deployment of C-UAS technologies in an urban setting under operational circumstances.

Introduction

The Secretary of Homeland Security has designated the 2019 United Nations General Assembly (UNGA) as a National Special Security Event (NSSE), which means that the Secret Service will coordinate the design and implementation of the operational security plan for the event. USSS will also provide protection to the foreign heads of state/heads of government in attendance, as well as to the President of the United States when he is in attendance. Because the Secretary has designated UNGA as an NSSE, UNGA is considered a temporary "covered facility," as defined in the *Preventing Emerging Threats Act of 2018*.[1] The location of UNGA is New York City, with the pilot impacting a two-mile radius around United Nations (UN) Headquarters, including surrounding roads, airspace, and adjacent East River.

USSS will partner with S&T and USCG in conducting this pilot of C-UAS systems during the NSSE. The purpose of the pilot will be to detect, deter, and defeat unauthorized UAS activity in the defined area, and to validate the processes and procedures for using C-UAS technology in an urban setting under operational circumstances. The operation includes every aspect of the process to deploy C-UAS technology, including coordination with other agencies (e.g., the Federal Aviation Administration (FAA)); positioning and installing the C-UAS technologies; and detecting, tracking, identifying, and mitigating threats from unauthorized UAS. This pilot will also provide an opportunity to train personnel on the process and use of C-UAS systems. Protocols have been established to coordinate communications between USSS and USCG and refer any resulting investigative case to the appropriate law enforcement agencies.

C-UAS systems will use Radio Frequency (RF) detection and Radio Detection and Ranging (RADAR) imagery, and Electro-Optical/Infrared (EO/IR) cameras will be used for their

[1] *See* 6 U.S.C. 124n(k)(3).

telescopic capacity rather than be used to collect images/video.[2] An EO/IR camera's optics are generally not the primary method of initial UAS detection; they will be positioned to point directly up at the sky or out to the horizon. All these technologies will be used to scan for and correlate detected and/or observed flying objects to accurately determine the probability that they are UAS, rather than non-threat items like flying debris or birds. These technologies are able to intercept and access radio frequency signals used by UAS; however, the functions of storing or capturing the signals are not part of the pilot and will not be used.[3]

The pilot is not designed to collect PII, but rather to determine the processes and procedures for using C-UAS in an urban setting under operational circumstances. The C-UAS systems will be placed and directed in such a manner as to only make visible the activity of a UAS in the immediate vicinity of the NSSE. None of these technologies' capabilities include the collection or storage of any PII. The RF and RADAR systems do not have detection abilities beyond RF energy levels. The EO/IR cameras will be used only for their telescopic capacity to scan the sky and horizon and only once the sensors have raised an alert; images are only viewed in real time and are not able to be collected, retained, or stored.

The Secret Service has previously deployed C-UAS under existing authorities. This pilot provides an opportunity to test deploying C-UAS at an NSSE, in an urban environment, with multiple DHS components and federal and local agencies involved, and under the authorities provided by the *Preventing Emerging Threats Act of 2018*. The C-UAS systems that USSS and USCG will deploy facilitate the detection of credible threats to the safety or security of a covered facility or asset from UAS and are not intended to collect PII. USSS will communicate with USCG for any relevant training needs to carry out the C-UAS pilot.

In addition, and similarly to the USSS C-UAS capabilities described immediately above, USCG is providing additional C-UAS capability in coordination with USSS in support of UNGA security, and in support of its mission of ensuring the Nation's maritime safety, security, and stewardship. USCG personnel will coordinate and provide support under the operational control of USSS airspace security personnel. The UNGA C-UAS Operations Plan outlines operating restrictions and equipment for both USSS and USCG.

---

[2] RF and RADAR are not capable of producing images of individuals as they display only RF energy levels. EO/IR cameras are capable of capturing high-quality images, but will be positioned to the sky and horizon only to confirm presence of a UAS; however, these images are only viewed in real time and are not able to be collected, retained, or stored.

[3] The *Preventing Emerging Threats Act of 2018* specifies that: the interception, or access to, or maintenance or use of, communications to or from an unmanned aircraft system must be conducted in a manner consistent with the Constitution and applicable federal law; that communications to or from a UAS are intercepted only to the extent necessary to support certain prescribed actions; and places limits on the disclosure and dissemination of those communications.

S&T's role in this pilot is to provide C-UAS technology to USCG. Providing the C-UAS systems will be part of a larger effort to understand and document the identification, test and evaluation, acquisition, and implementation process to use these systems at this and future events.[4] Specifically, this event will document the process with associated requirements and schedules to perform C-UAS missions at a designated covered facility. S&T will work with the C-UAS manufacturers to ensure USCG operators have the training necessary to operate the systems in a safe and secure manner. S&T will also work with the C-UAS manufacturers to ensure that the C-UAS technology operated by USCG does not interfere with other technologies operated by the USSS. If required by the FAA, S&T will support USCG in running limited tests of the technology in the operational environment to identify or mitigate radio frequency disruption. S&T will not operate any of the C-UAS equipment during this event and will not collect or retain any data from the equipment.

Some C-UAS systems may allow USSS and USCG to determine the location of the signal from a UAS. If this occurs, then the UAS operator could be identified based on the location.[5] If, during this pilot, a potential UAS threat is detected, law enforcement officers will attempt to approach any identified UAS operator directly to discuss the threat, when time and circumstances permit. However, if NSSE-assigned personnel are not able to resolve the threat through personal contact, USSS and USCG personnel may use C-UAS technology to mitigate the threat by disrupting or disabling the UAS.

UAS must be registered with the FAA when they weigh more than one-half pound and must display the FAA registration number on the UAS. The "C-UAS Project Team," consisting of members form USSS, USCG, and S&T, will not link or trace the serial number displayed to any person or entity. If the UAS is deemed a threat and then mitigated, the C-UAS Project Team will share the serial number with law enforcement investigators but not retain the serial number itself. Those investigators could then use their own authorities and resources to request owner information from the FAA. The C-UAS Project Team will not be part of the law enforcement investigation. Mitigating UAS through C-UAS technology does not involve the collection of PII, and any interactions between NSSE-assigned personnel and members of the public, for any reason, are outside the scope of this pilot and are covered under other USSS or USCG authorities. Any interception or access of communications used to control a UAS is also outside the scope of this testing and PIA, and would be conducted in strict compliance with the privacy protections contained within the *Preventing Emerging Threats Act of 2018.*

[4] *See* DHS/S&T/PIA-034 Counter Unmanned Aircraft Systems Program, *available at* https://www.dhs.gov/privacy.
[5] The system does not identify an individual, but does point to the general location of the signal. The appropriate personnel, whether DHS or local law enforcement, would respond to the location and look for a visible operator.

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 ensure 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.[6] 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 and the Homeland Security Act of 2002 Section 222. Given that C-UAS are mechanical and operational systems rather than a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of C-UAS operations as it relates to 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. There should be no system the existence of which is a secret.*

For public situational awareness, USSS will post signage and/or barricades at publicly accessible UAS operation areas ("drone parks") located within the two-nautical mile Temporary Flight Restriction (TFR), advising of the TFR during UNGA in order to control access to areas where C-UAS activity is occurring. Notice will also be provided in the form of a Notice to Airmen,[7] which provides the public with information regarding the existence of the TFR. Local authorities also assigned to assist with UNGA security will occasionally monitor the activity at these drone parks to ensure compliance with the TFR.

Information about the flight restrictions will also be posted to various social media platforms and delivered to media outlets for further distribution. USSS will contact various

[6] 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, *available at* https://www.dhs.gov/policy.
[7] All Notice to Airmen alerts can be found at: https://www.FAA.gov.

hobbyist groups to provide information about the TFR for dissemination to the group's members. Those individuals entering the area under the TFR who may have failed to observe the signage and notices about the TFR are still unlikely to have their PII captured because the C-UAS systems will be angled to minimize the risk of inadvertent viewing of PII of the public. The C-UAS system enhances the existing monitoring capabilities, but steps will be taken to ensure that the C-UAS does not increase the privacy risk to individuals in the testing area. These additional steps will be covered in the sections below.

Further, this PIA provides a measure of transparency to the public about C-UAS activities to be conducted at UNGA 2019.

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 a dual investigative and protective mission, and especially in the case of UNGA. Once the C-UAS systems are in operation, individuals outside the secure zone of protection may not always be given the opportunity to consent to temporarily coming into the range of the cameras being used for their telescopic capability to scan the horizon as it may compromise protective operations and interfere with the USSS' and USCG's ability to carry out their missions.

Privacy Risk: There is a privacy risk that while monitoring the airspace near UNGA, the C-UAS sensors might inadvertently capture images containing PII of individuals who have temporarily come into the range of the cameras being used. Those individuals may not have consented to being part of the C-UAS pilot and have no opportunity to opt out.

Mitigation: This risk is partially mitigated. The C-UAS sensors will be placed and directed in such a manner as to make visible the activity of UAS in the immediate vicinity of the NSSE and to minimize the risk of inadvertently capturing individuals. Even in such cases, the purpose of this pilot is not to collect any PII. None of the technologies being used are capable of collecting or storing images/video that contain PII.

Further, USSS will post signage at publicly accessible "drone parks" advising of the temporary restriction during UNGA in order to control access to areas where UAS activity is restricted. Those members of the public who enter an area where UAS activity is restricted have given tacit consent to possibly having their images captured by not obeying the signs and altering their path.

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.*

SOD performs operations that include planning, directing, and executing surveillance and counter-surveillance operations to better detect suspicious activity and/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, other designated individuals, and NSSEs.[8] Further, USSS is authorized to enforce zones of protection.[9]

The Secret Service has previously deployed C-UAS under existing authorities. This operation, in part, provides an opportunity to test deploying C-UAS for an NSSE, in an urban environment, with multiple components and agencies involved, and under the authorities provided to USSS and to USCG by the *Preventing Emerging Threats Act of 2018*. The C-UAS technologies used in this pilot facilitate the detection of credible threats to the safety or security of a covered facility or asset from UAS and are not capable of collecting PII.

4. Principle of Data Minimization

Principle: *DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).*

There is no intent to collect PII during the planned C-UAS activities. If, during this pilot, a potential UAS threat is detected, NSSE-assigned personnel will attempt to approach any located UAS operator directly to discuss the threat when time and circumstances permit. However, if NSSE-assigned personnel are not able to resolve the threat through personal contact, USSS and USCG personnel may use C-UAS technology to mitigate the threat by disrupting or disabling the UAS. Interactions between NSSE-assigned personnel and members of the public, for any reason, are outside the scope of this pilot and are covered under other USSS and USCG authorities.

Privacy Risk: There is a privacy risk that individuals or PII may come temporarily into the range of the EO/IR cameras being used for their telescopic capacity to scan the horizon and more information than necessary is collected.

[8] 18 U.S.C. § 3056.
[9] 18 U.S.C. § 1752.

Mitigation: This risk is mitigated. The C-UAS technologies used in this pilot are not able to collect or store any PII-related data, such as video/images. Only the detection frequencies and control protocols are collected by the RF and RADAR technologies. The EO/IR camera's optics are generally not the primary method of initial UAS detection; they will be positioned to point directly up at the sky or out to the horizon and only once other systems have raised an alerted. These cameras are being used as a telescopic viewer to "zoom in on" airspace (where possibly an object exists) that the sensors have alerted as a possible UAS. It is possible that when the cameras have been alerted some object with PII could come into view. However, this imagery/video cannot be collected or stored; it is only viewed in real-time.

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 is designed to not collect PII. The purpose of the pilot is to detect, deter, and defeat unauthorized UAS activity in the defined area, and to validate the processes and procedures for using C-UAS technology in an urban setting under operational circumstances. USSS, USCG, and S&T have determined that PII collection is not necessary to fulfill this purpose and the C-UAS systems that will be employed help facilitate this.

The C-UAS systems will be placed and directed in such a manner as to only make visible the activity of UAS in the immediate vicinity of the NSSE. RF and RADAR technologies are not capable of producing images of people or any other PII. The EO/IR cameras are being used for their telescopic capacity to scan the horizon, and there is a remote possibility that individuals and other PII could temporarily come into range. However, no images/video viewed by EO/IR cameras will be stored or maintained by USSS, USCG, or S&T. Members of the C-UAS Project Team are regularly trained on the proper handling of sensitive information, and are aware that any use or capturing of otherwise irrelevant images is not permitted.

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.*

Data collected through these C-UAS efforts is used to evaluate C-UAS, and therefore must be accurate, relevant, timely, and complete. The data collected from test activities will include the

assessment of EO/IR sensors and RF and RADAR technologies, but none of these test activities are able to collect or store PII.

7. Principle of Security

Principle: *DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

There is no intent to collect PII during the planned C-UAS activities, and the technology being used in this pilot is not able to collect or store any PII.

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.*

S&T will work with the C-UAS manufacturers to ensure USCG operators have the training necessary to operate the systems in a safe and secure manner. S&T will also work with the C-UAS manufacturers to ensure that the C-UAS technology operated by USCG does not interfere with other technologies operated by the USSS. If required by the FAA, S&T will also support USCG in running limited tests of the technology in the operational environment to identify or mitigate radio frequency disruption. None of the tests described herein will collect or retain PII.

The UNGA C-UAS Operations Plan outlines operating restrictions, requirements, and equipment for both USSS and USCG. In addition, all DHS personnel receive annual privacy and cybersecurity training to ensure they understand the importance of handling and securing PII.

Conclusion

This pilot will help determine the processes and procedures for using C-UAS in an urban setting under operational circumstances. In addition, this pilot will assist the USSS in identifying and mitigating UAS that may pose a risk to covered facilities and assets at UNGA 2019, either because they accidentally enter a restricted location or because the operator is intentionally seeking

to do harm. This pilot is designed to mitigate potential privacy risks when testing and evaluating potential C-UAS solutions to protect the public and national security.

Responsible Officials

Linda Canfield
Special Operations Division
United States Secret Service
(202) 406-7135

Edna Rucker
Privacy Officer
United States Secret Service
(202) 406-5838

Kathleen L. Claffie
Chief, Privacy Program (CG-6P)
U. S. Coast Guard
(202) 475-3515

Maria Petrakis
Acting Privacy Officer
Science and Technology Directorate
(202) 254-5611

Approval Signature

[Original, signed copy complete and on file with the DHS Privacy Office]

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security