Privacy Impact Assessment
for the

U.S. Coast Guard
Counter-Unmanned Aircraft Systems Pilot

DHS/USCG/PIA-030

October 28, 2019

Point of Contact
Michael R. Shumaker
Office of Maritime Security Response Policy (CG-MSR)
U.S. Coast Guard
(202) 372-2127

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

Abstract

The U.S. Coast Guard (USCG) is conducting an operational pilot to test and evaluate Counter- Unmanned Aircraft Systems (C-UAS) capabilities used to detect, identify, and mitigate UAS that pose a credible threat to "covered facilities or assets." USCG will conduct the pilot testing through 2020, after which the USCG C-UAS program may become fully operational. This Privacy Impact Assessment (PIA) discusses measures taken to mitigate privacy risks and protect against any impact to personally identifiable information (PII) during the deployment of C-UAS technologies under operational circumstances. If the USCG C-UAS program becomes fully operational, this PIA will be updated.

Introduction

The USCG is responsible for ensuring the Nation's maritime safety, security, and stewardship. USCG has eleven statutory missions codified in the Homeland Security Act of 2002. These missions are: Ports, Waterways, and Coastal Security; Drug Interdiction; Migrant Interdiction; Defense Readiness; Law Enforcement; Marine Safety; Search and Rescue (SAR); Aids to Navigation; Living Marine Resources; Marine Environmental Protection; and Ice Operations.

The USCG is developing and fielding C-UAS capabilities to protect covered facilities or assets during certain missions as provided for in the Preventing Emerging Threats Act of 2018, 6 U.S.C § 124n (the "Act"), which granted authorities to the Department of Homeland Security (DHS).[1] The Act provides the Secretary of Homeland Security with the authority to authorize personnel for the security or protection of people, facilities, or assets to mitigate a credible threat that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset. This can include the protection of a National Special Security Event (NSSE) and Special Event Assessment Rating (SEAR) event; providing support to state, local, territorial, or tribal law enforcement, upon request of the chief executive officer of the state or territory, to ensure protection of people and property at mass gatherings; providing protection of an active federal law enforcement investigation, emergency response, or security function; or missions authorized to be performed by the USCG as set forth in 14 U.S.C. § 528.

The purpose of this one-year pilot is to continue to develop the processes and procedures for using C-UAS consistent with the Act. The pilot includes every aspect of the process to deploy C-UAS including: coordination with other agencies; deployment of the C-UAS capability; detection, tracking, identification, and mitigation of threats from UAS;[2] and establishment of communication between USCG and federal, state, or local agencies for comprehensive response

[1] *See* https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section124n&num=0&edition=prelim.
[2] For the purpose of this PIA, UAS refers to those "small" UAS typically categorized as Group 1 and 2 (i.e., weighing less than 55 lbs.).

to UAS threats when necessary.

USCG will use C-UAS technology provided to it from the DHS Science and Technology Directorate (S&T), obtained by the USCG Research and Development Center (RDC), and other equipment that may be acquired via DHS, USCG, or partner agency projects. USCG C-UAS systems will use Radio Frequency (RF) detection, Radio Detection and Ranging (RADAR) imagery, and Electro-Optical / Infrared (EO/IR) Cameras, individually or in combination, to detect, track, positively identify, and seize control of airborne contacts as potential UAS.[3] These technologies are able to intercept and access radio frequency signals used to control airborne UAS; however, they do not capture any of the video imagery transmitted from the aircraft to the controller.

This pilot is not designed to collect personally identifiable information (PII). Any EO/IR sensors used for C-UAS will be directed only to search for and identify UAS in the immediate vicinity of the protected facility or asset. However, there is a remote possibility the C-UAS sensors might inadvertently capture images containing PII while monitoring the airspace near the protected facility or asset. Should this occur, no PII captured by C-UAS sensors will be stored or maintained.

USCG C-UAS Operations Plans developed for operational deployment will outline operating restrictions unique to individual facilities or assets. Each Operations Plan is developed in accordance with the USCG Interim C-UAS Policy, which outlines the requirements for use of C-UAS at USCG. This interim policy was completed in coordination with the USCG Privacy Office (CG-6P) prior to implementation.

When time and circumstances permit, efforts will be made to identify the operator of a UAS that has been identified as a potential threat. If successful, the USCG will coordinate with federal, state, or local law enforcement personnel to approach the UAS operator directly to discuss the threat. However, if they are not able to resolve the threat through personal contact, USCG personnel may use C-UAS technology to mitigate the threat consistent with that authorized by the Act. This action includes disrupting or disabling the UAS. C-UAS technology does not collect PII. Interactions between federal, state, or local law enforcement personnel and members of the public, are governed by existing laws and policies regarding law enforcement practices. If the USCG does mitigate a threat using C-UAS technology, and the USCG also recovers the UAS, it will follow "chain of custody" requirements and treat the UAS as evidence in accordance with federal law and existing policies and procedures. Extraction of any information from the device will adhere to constitutional and federal law including, when necessary, obtaining a warrant.

[3] 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.

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.[4] 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 premised upon the DHS 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.*

USCG is undertaking a one-year pilot to help determine the processes and procedures for using C-UAS technology in operational circumstances. The pilot includes every aspect of the process to deploy C-UAS, including: coordination with other agencies; deployment of the C-UAS capability; detection, tracking, identification, and mitigation of threats from UAS; and establishment of communication between USCG and federal, state, or local agencies for comprehensive response to UAS threats. This one-year pilot is not designed to collect PII.

Privacy Risk: There is a risk that individuals will be unaware that their images or other similar data could be captured during the deployment of C-UAS during this one-year USCG pilot.

Mitigation: This risk is partially mitigated. First, there will be a public awareness campaign to notify the public and those at nearby publicly accessible UAS operation areas ("drone parks") that UAS are not permitted in certain locations at certain times/dates. When possible,

[4] 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.

USCG will request event sponsors or other stakeholders to provide notice through those groups' communications platforms (e.g., event website) as well. Second, individuals entering the area where C-UAS technology is being deployed are unlikely to have their PII captured because the C-UAS technology is primarily used to search the sky for airborne UAS and will not be deploying capabilities to capture the devices images or other data.

Further, this PIA provides a measure of transparency to the public about USCG C-UAS activities conducted in accordance with its eleven statutory missions.

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 USCG given its maritime authorities. When the C-UAS technology is in operation, individuals 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 interfere with USCG's ability to carry out one of its eleven statutory missions.

Privacy Risk: There is a privacy risk that while monitoring the airspace using C-UAS, 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 view the activity of UAS and to minimize the risk of inadvertently capturing individuals. The one-year pilot does not seek to collect PII and it will not store any images it may inadvertently collect.

Further, USCG or, in the event USCG is working with a partner agency, may post signage at publicly accessible locations (e.g., "drone parks") advising of any temporary restriction 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. However, in some instances, signage may not be possible given the nature of USCG's eleven statutory missions.

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.*

The Act provides that C-UAS may "detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft… Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft" among taking other potential actions.

It then proceeds to explain what may be done with the interception or acquisition of communications to/from a UAS. These requirements were recently followed during the USCG's deployment of C-UAS in support of the United States Secret Service (USSS) during the United Nations General Assembly.[5] That operation, in part, provided USCG an opportunity to test deploying C-UAS in an urban environment, with multiple components and agencies involved, and under the authorities provided to USCG by the Act. The C-UAS technologies used then and during this one-year USCG pilot to facilitate the detection of credible threats to the safety or security of a covered facility or asset, will be in compliance with the Act and all other requirements for privacy protections.

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 while conducting C-UAS activities during this one-year pilot. However, even if there were inadvertent collection, the Act provides that "records of such communications are maintained only for as long as necessary, and in no event for more than 180 days, unless the Secretary of Homeland Security or the Attorney General determine that maintenance of such records is necessary to investigate or prosecute a violation of law, directly support an ongoing security operation, is required under federal law, or for the purpose of any litigation."

[5] *See* DHS/USSS/PIA-025 United States Secret Service Special Operations Division Counter-Unmanned Aircraft Systems in support of United Nations General Assembly, *available at* https://www.dhs.gov/privacy.

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.

Mitigation: This risk is mitigated. The C-UAS technologies used during the USCG pilot are not able to collect or store any PII-related data, such as video or 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. Moreover, they will be positioned to point directly up at the sky or out to the horizon and are used only once other systems have raised an alert. 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 avoid the collection of PII. The purpose of the pilot is to detect, deter, and defeat unauthorized UAS activity in a defined area, and to validate the processes and procedures for using C-UAS technology under operational circumstances. USCG determined that PII collection is not necessary to fulfill this purpose and the C-UAS systems that will be employed help facilitate this.

Any C-UAS systems used during this one-year pilot will be placed and directed in such a manner as to only make visible the activity of UAS in the immediate vicinity of the covered facility or asset. 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; however, there is a remote possibility that individuals and other PII could temporarily come into range. Should this occur, no images or video viewed by EO/IR cameras will be stored or maintained by USCG. USCG personnel using C-UAS 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 for the immediate evaluation of C-UAS, and therefore must be accurate, relevant, timely, and complete. The data collected from this

one-year pilot will include the assessment of EO/IR sensors and RF and RADAR technologies, but none of these pilot activities aim to collect or store PII and measures are taken to avoid accidental collection and any storage.

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 one-year C-UAS pilot, and the technology being used in this pilot will not store any PII. However, even if there is any unintended collection, the Act sets specific parameters and safeguard for disposing of that information.

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.*

USCG will ensure that its operators have the training necessary (including completion of approved Job Qualification Requirements) to operate the C-UAS technology in a safe, secure, and privacy-protecting manner. In addition, all USCG personnel receive annual privacy and cybersecurity training to ensure they understand the importance of handling and securing PII.

Prior to any approved deployment of C-UAS technology, USCG will develop a C-UAS Operations Plan specific to that deployment. The Operations Plan will outline operating restrictions, requirements, and equipment used during the deployment.

Finally, the USCG Privacy Office (CG-6P) will initiate a USCG Privacy Evaluation (CGPE) prior to the completion of this one-year pilot to ensure that USCG has adhered to the principles outlined in this PIA and the USCG Interim C-UAS Policy. Coast Guard Privacy will share the results of the CGPE with the DHS Privacy Office.

Conclusion

This one-year pilot will help determine the processes and procedures for USCG to continue using C-UAS in operational circumstances in the future. In addition, this pilot will assist USCG and any partner agencies in identifying and mitigating UAS that may pose a risk to covered facilities or assets, either because they accidentally enter a restricted location or because the operator is intentionally seeking to do harm. This one-year 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

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

Joseph A. Conroy
Office Chief, CG-MSR
U.S. Coast Guard

Approval Signature

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

_____

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