Privacy Impact Assessment
for the

Counter
Unmanned Aircraft Systems Program

DHS/S&T/PIA-034

November 9, 2018

Contact Point
Shane Cullen
Program Manager
Unmanned Aerial Systems/
Countermeasures for Unmanned Aerial Systems
Science & Technology Directorate
(202) 254-5798

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

Abstract

The Department of Homeland Security's (DHS) Science & Technology Directorate (S&T) is leading DHS efforts and coordinating across the Federal Government testing and evaluating technologies used to detect, identify, and monitor small Unmanned Aircraft Systems (sUAS) that may pose a potential threat to covered facilities and assets and other missions authorized to the Department by law. These protective technologies are referred to as Counter-UAS (C-UAS). This Privacy Impact Assessment (PIA) discusses measures taken to mitigate privacy risks and protect personally identifiable information (PII) during S&T's testing and evaluation of C-UAS technologies.

Introduction

On August 29, 2018 FAA rules regarding the use of sUAS took effect, opening up the National Airspace System to certified sUAS. The Federal Aviation Admiration projects as many as 717,895 may be in use in the United States for commercial and professional purposes (i.e. package delivery, medical prescription delivery, crop dusting, pipeline examinations) by 2022.[1] sUAS are primarily used for beneficial purposes, but may also be a source of deliberate or inadvertent threats to the department's facilities, assets, or missions.

Over the last few years, sUAS have interfered with airport flight operations forcing airplanes to divert and make emergency course corrections,[2] forced wildfire aircraft water tankers to be grounded,[3] and crashed into the bleachers at sports stadiums.[4] To minimize risks to life and property, DHS S&T is conducting a series of C-UAS Test & Evaluation (T&E) activities. The goal is to identify, test, and evaluate C-UAS technologies to determine system strengths and weaknesses. DHS S&T will present authorized federal agencies with the T&E results to inform future acquisition plans. C-UAS T&E activities are being conducted in three phases, Spiral I, Spiral II, and Spiral III. Spiral I involves a series of tests in controlled areas such as military test sites or privately owned test ranges. Spiral II involves testing in a public venue. Spiral III involves transitioning the technology out of the testing environment into the operational environment. This PIA covers testing conducted during Spiral I and Spiral II. Spiral III will be documented in a new PIA or PIA updates prior to deployment of the technology.

Spiral I Testing:

To assess the effectiveness of the C-UAS technology, use of C-UAS systems will occur in test ranges, where only individuals involved with the testing will be within the acquisition range

[1] *See* https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/Unmanned_Aircraft_Systems.pdf.
[2] *See* https://www.wxyz.com/news/local-news/investigations/dangerous-drones-invade-protected-airspace-at-metro-detroit-airports.
[3] *See* http://www.koaa.com/story/38532419/co-legislators-introduce-bill-to-make-flying-drones-over-wildfires-a-felony.
[4] *See* http://www.niemanlab.org/2015/09/the-journalists-guide-to-drones-over-or-crashing-into-stadiums.

of the equipment. DHS S&T will collect sUAS flight information (for those sUAS deployed as part of the test) from C-UAS systems during T&E activities in order to identify sUAS and differentiate them from other objects, such as birds in the sky. T&E activities will not involve any collection of audio signals or personal data. The test activities will only include the assessment of Electro-Optical (E/O) sensors, radar, video equipment, and perimeter alert systems.

Although video equipment will be pointed towards the sky, images of individuals participating in T&E activities may be incidentally captured during testing as the camera moves to follow the sUAS. The images will only be used for testing and evaluation of C-UAS capabilities, not to identify any person whose image is inadvertently captured. DHS S&T sUAS will also be used in the testing. Data will not be collected by the sUAS during testing and will not be used or stored in the execution of test activities.

Spiral II Testing:

C-UAS equipment will be placed in select locations within designated public spaces. The C-UAS will scan for unmanned aircraft and work to identify and track only the sUAS deployed specifically for the tests. Spiral II testing will be conducted on secure locations with access control, signage, and the ability for those not involved in the test to opt out or avoid testing locations.

Similar to Spiral I, the test activities will only include the assessment of Electro-Optical (E/O) sensors, radar, video equipment, and perimeter alert systems. All sensors are designed to physically detect and track an sUAS, and not any signal it may produce. Images of individuals near the T&E activities may be incidentally captured during testing as the camera follows an sUAS. Since Spiral II tests take place in public areas, there is a greater risk of inadvertently capturing images of the public. Any captured images will only be used for testing and evaluation of C-UAS capabilities, not to identify any person whose image is inadvertently captured.

C-UAS capabilities encompass a broad scope; sUAS detection and deterrence requirements are heavily dependent and different from one venue to another – requiring different solutions for different scenarios. This Privacy Impact Assessment contains a general overview of sUAS privacy risks and mitigation strategies. DHS S&T will provide detailed risk assessments and mitigation strategies in future updates and appendices to this PIA.

As the C-UAS technologies move out of the testing phase and into operational use, the operational entities will offer Privacy Impact Assessments explaining risks and mitigation strategies relevant to their use of C-UAS.

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 personally identifiable information. The

Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

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. 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. This PIA examines the privacy impact of Countermeasures for Unmanned Aircraft System T&E activities 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.

DHS S&T is conducting a series of C-UAS T&E activities. These activities were initially conducted on military, government, or privately owned properties/testing ranges. Upcoming tests will include public sites. A synopsis of the testing planned for each T&E venue will be added to the appendix at the end of this PIA prior to initiation of the test. This PIA, and any appendices, provide a measure of transparency.

Privacy Risk: There is a risk that individuals will be unaware that their images could be captured as part of a C-UAS test.

Mitigation: This risk is partially mitigated. For testing in non-public areas, S&T will control access to test sites and give notice via signage that their images may be captured, and a set-aside zone will be available for individuals who do not want their images even inadvertently captured.

For public situational awareness, signs will be posted throughout the testing area. Those individuals entering the test area, who may have failed to observe the signage, are still unlikely to have their images captured, as the C-UAS systems in public spaces will be angled to minimize the capture of images 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 risks to the individual in the testing area. These additional steps with be covered in the sections below.

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.

Notices are provided and informed consent is required for all persons actively participating in C-UAS T&E activities. This includes government employees, contractors, vendors and researchers. Notice in the form of handouts and signage are provided to individuals participating in testing activities that their images may be captured. Alternative areas are established for persons who do not want their images captured.

No members of the public are involved in any T&E activities occurring on military bases, government test sites or privately owned test facilities. In public settings DHS S&T will erect obvious access control measures and post signage to demarcate testing areas. An individual must physically pass through such controls to enter an area before their image may be incidentally captured to any degree of clarity. DHS S&T will ensure that there are demarcated detour routes around any testing site to ensure no individual is required to enter the site.

Privacy Risk: There is a privacy risk that DHS S&T may collect information from members of the public who have not consented to this collection and have no opportunity to opt out of the collection.

Mitigation: DHS S&T will post barricades or signage to control access to any test sites. Those members of the public who enter an area where C-UAS T&E activity is occurring have given consent to possibly having their images inadvertently captured by not obeying the signs and altering their path. Even in such cases, as S&T has no desire to collect any PII during this testing, such images will not be used to identify persons.

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 Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs."

In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support research, development, and other T&E activities related to improving the security of the homeland.

The 2018 Preventing Emerging Threats Act (Division H, §1601 of the FAA Reauthorization Act of 2018) stipulates that the Secretary shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to its use for detecting, identifying, monitoring or tracking unmanned aircraft systems or unmanned aircraft. The Preventing Emerging Threats Act also provides that the Secretary ensure that the T&E activities described in this PIA are conducted in a manner consistent with the First and Fourth Amendments to the Constitution of the United States.

The purpose of the C-UAS T&E activities is to determine the effectiveness of the commercial C-UAS technologies. UAS flight data is captured by C-UAS components in order to identify sUASs and differentiate them from birds, kites, and other objects in the sky. Images of individuals participating in testing activities may be incidentally captured during testing. The images will only be used for testing and evaluation of C-UAS capabilities, not to identify any person whose image is inadvertently captured. T&E activities will not involve any collection of audio signals or radio frequency data.

Privacy Risk: Incidental PII may be collected by C-UAS systems that is beyond the scope of C-UAS operations.

Mitigation: The risk to the individual is mitigated by the T&E collection method. The C-UAS is designed to track sUASs, and all other data is considered "noise" and is purposely excluded. The C-UAS systems used during the testing and evaluation activities are also pointed skyward, significantly limiting the chance that an image of an individual or an individual's belongings will be collected. Furthermore, any images containing inadvertently captured PII will not be used to determine the identities of any individual.

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).

The purpose of the tests is to determine the effectiveness of C-UASs' abilities to detect and track risks associated with sUASs. The C-UAS T&E activities may incidentally collect images of individuals. However, DHS S&T will not attempt to identify the individuals whose images have been collected during related T&E activities. In the event of an accident or crime unintentionally captured during a testing session, DHS S&T may be required to produce the data and assist first responders or law enforcement officers with identification.

DHS S&T will follow DHS records retention schedules, as documented in GRS 3.1, item 11, which covers test files, data, and evaluation. T&E files are considered temporary and cut off

at the end of the calendar year after completion or cancellation of a project. All records are then destroyed or deleted one year after the responsible office determines it is no longer needed for legal, audit, administrative, or business purposes.

Privacy Risk: C-UAS data, including incidentally collected PII, may be retained for a longer period than required for T&E or Countering sUAS.

Mitigation: DHS S&T Records Management staff conduct annual reviews with program managers to determine if data should be retained, archived, or destroyed. If DHS S&T shares any data with vendors, the vendors will be required to follow DHS records retention schedules. Vendors will also be under the same obligation as DHS and not attempt to identify individuals whose information may have been inadvertently obtained.

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.

Incidentally captured images of persons, may be contained within data that is used by other researchers for additional C-UAS T&E activities. As the identities of the individuals is unknown to DHS S&T, it cannot be conveyed to the other researchers. Other authorized researchers are also required not to attempt to identify the individuals whose images may have been inadvertently captured. Overall data (not PII) may be shared with respective C-UAS vendors so they may enhance and improve their systems. Data retained by DHS S&T is only used for T&E activities. Data containing inadvertently collected images may be shared with other DHS Components who are partnering with DHS S&T for purposes of evaluating the C-UAS technology. In extreme cases, for example the C-UAS cameras capture evidence of a crime, DHS S&T will immediately share that information with the DHS Component partners. Those partners will follow their operational guidelines, outlined in the Privacy Impact Assessment and System of Records Notice for the system used to store the data, in the reporting or investigation of such an incident.

C-UAS vendors partnering with DHS S&T are contractually obligated by the project's Cooperative Research and Development Agreement (CRADA). Under the CRADA a vendor must confer and consult with DHS S&T, as well as provide a reasonable review period of 2 weeks, prior to sharing protected information to any third party, to assure that no proprietary information is released, and that any concerns, including the disclosure of PII, are addressed.

Privacy Risk: There is a risk that data collected during C-UAS test operations may be used by DHS S&T or C-UAS vendors for purposes other than testing C-UAS.

Mitigation: DHS S&T will provide system training for authorized project personnel and vendor partners prior to C-UAS demonstrations. DHS S&T will also brief individual observers

from participating agencies prior to any interaction with the system. The training/briefings will include proper use of the system, a copy of this Privacy Impact Assessment, DHS privacy policies, and the requirement to avoid collecting PII, and if PII is inadvertently collected to delete, mask, or not attempt to identify the individual to who the image belongs. Use of stored images for research and development activities will be in accordance with the approved Statement of Work in the laboratory contracts with DHS.

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 for these T&E 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 Electro-Optical (E/O) sensors, radar, and perimeter alert systems, none of which collect PII. Images containing inadvertently captured PII may also be used for testing and evaluating C-UAS, but not to determine the identities of any individual whose image is incidentally captured. The data will not be retrievable by a unique identifier nor used to identify any individuals. DHS will therefore not attempt to guarantee the accuracy of incidental PII that may be captured.

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.

During the DHS S&T C-UAS T&E activities data is transmitted to a secured set of DHS S&T workstations with the appropriate privacy and security controls built into the workstations. These controls include user name and password protection. Access is limited to only those with an authorized need-to-know. The C-UAS T&E process will also determine what additional security features need to be added to C-UASs.

Privacy Risk: There is a risk of unauthorized loss or disclosure of PII due to a security incident.

Mitigation: This risk is partially mitigated. The system collecting C-UAS data does not connect outside the DHS firewall, and has a limited number of devices that can connect to the system. Access to these devices are controlled through property and administrative controls. The data only resides on workstations for a limited amount of time before it is transferred to DHS S&T databases that are operationally hardened in compliance with DHS cyber security guidelines.[5]

[5] For more information *see* DHS 4300A Sensitive Systems Handbook v12, November 15,2015 *available at* https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf.

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 DHS S&T staff, including vendors, contractors, and employees, are required to complete annual privacy awareness training. Access controls are in place to ensure only authorized users access to the system and images.

Conclusion

sUASs may pose a risk to covered facilities and assets and other missions authorized to the Department by law; either by accidentally entering a restricted location, or when the operator is intentionally seeking to do harm. The DHS S&T C-UAS T&E Program is designed to mitigate potential privacy risks when testing and evaluating potential C-UAS solutions to protect the public and national security.

Responsible Officials

Shane Cullen
Program Manager
Unmanned Aerial Systems/Countermeasures for Unmanned Aerial Systems
Science & Technology Directorate

Approval Signature Page

Original, signed copy on file with the DHS Privacy Office
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A

US Secret Service

Winter/Spring 2019 Test Event: National Capital Region

The purpose of this test event is to ensure key C-UAS systems are working in a manner that is free from regular errors and malfunctions and to collect relevant information to perform component calibration. Additionally, imagery, and flight information in the operational environment will be collected for use in calibration of equipment. The test facilitator will provide several commercial off-the-shelf UASs for the specific reason of testing of the c-UAS systems. All UASs are registered with the FAA.

The primary objective of this test event is to collect the following C-UAS technical performance data against sUASs in an operational environment that has an access-controlled perimeter:

1. Imagery
2. Geographical data related to flight routes of test sUAS flying over the test site.

The flight test will be conducted in a designated area within the National Capitol Region. Signs, cones, or other barrier devices will be used to ensure nonparticipants are notified and do not inadvertently enter the test area. The perimeter will be access controlled and overt law enforcement will be present along with perimeter signage.

Tests will:

1. Occur over a six-month period.
2. Tests will average approximately one test event every two months.
3. Be conducted during daylight hours.
4. Be coordinated with the program sponsor.
5. Not collect data from the UAS used in the test.