Privacy Impact Assessment
for the

Robotic Aircraft for Public Safety (RAPS) Project

November 16, 2012

DHS/S&T/PIA-026

Contact Point
John Appleby
Borders and Maritime Security Division
Science and Technology Directorate
(202) 254-5620

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

Abstract

The Department of Homeland Security (DHS), Science &Technology (S&T) Directorate and the State of Oklahoma are partnering on the Robotic Aircraft for Public Safety (RAPS) project to test and evaluate Small Unmanned Aircraft Systems (SUAS) for potential use by the first responder community and DHS operational components. SUAS include small aircraft (typically under 55 pounds and having wingspans of 3-6 feet or less) that are operated using a wireless ground control station (GCS). The aircraft are equipped with sensors and cameras that can capture images and transmit them to a ground control system to provide aerial views of emergency situations and situational awareness. DHS S&T is conducting a Privacy Impact Assessment (PIA) to address the privacy impacts of the system's surveillance and image capturing capabilities.

Introduction

SUAS could be valuable tools for emergency responders for rapid response and gaining invaluable situational awareness before responding to and engaging in potentially dangerous operations. They could enable emergency responders to conduct more effective responses in critical operations, including: fire and wildfire response, natural and hazardous materials disaster evaluation and response, real-time law enforcement tactical operations support, and crime scene situational awareness. To assist emergency response agencies in the analysis and potential acquisition of these tools, the DHS S&T Borders and Maritime Security Division (BMD) is conducting the RAPS test project, which tests and evaluates current SUAS platforms available to the first responder and homeland security operational communities. The tests will examine SUAS capabilities, effectiveness, and utility in helping first responders and their operations. Users may then use the published test results to support future decisions on acquisition and deployment of the systems.

SUAS include small aircraft, usually weighing 55 pounds or less. The SUAS can be programmed to fly on a prescribed flight path or manually controlled from the ground control station by the operators. The SUAS are equipped with sensors and cameras that can capture images and transmit them to the GCS to provide aerial views of emergency situations and situational awareness. In the case of a lost connection between the user and the aircraft, the system can be programmed to automatically return to the point of the lost connection or to the area of takeoff, depending on the system being tested. Data collection and transmission continues as long as the connection to the GCS is active, though some systems have the ability to store data on the aircraft itself.

The systems tested in RAPS vary in size of the aircraft and camera resolution depending on the model of the aircraft and needs of the potential operational user. For example, some systems can take snapshots or still images by using screenshots of full motion surveillance video. Most systems include a date and time stamp on the footage captured and the cameras can capture latitudinal and longitudinal coordinates if needed. Any data that contains imagery not related to the test activities (e.g., non-volunteers or areas outside the testing perimeter) are deleted and are not used for the project. The images taken are not matched in any databases. The systems being tested are not capable of performing facial recognition.

The initial testing is being conducted at the Fort Sill U.S. Army post in Oklahoma. Other U.S. military facilities may also be used for testing. The SUAS test flights are limited to restricted airspace where tests and drills are already conducted (e.g., firing ranges). The SUAS do not fly over or capture images of the living quarters, shopping areas, or any other public spaces at Fort Sill. All test volunteers receive notice and provide consent prior to participating in the tests; no members of the public are affected by these tests.

During the tests, the S&T RAPS team evaluates each system using key performance parameters (e.g., endurance, stability, and resolution) under a wide variety of simulated, but realistic and relevant real-world operational scenarios, focusing on response to situations where human lives or property are in imminent danger. Safety concerns are also assessed, including the aircraft's capability for safe flight in the event of a loss of communications between the aircraft and the ground controller.

Typical test scenarios include search and rescue missions, fire and hazardous material spill responses, and simulated law enforcement tactical operations. During this time, volunteer participants conduct the test and evaluation activities based on the various test scenarios to determine how effectively the SUAS facilitate the response. The SUAS have the ability to fly over large areas and capture images of volunteers during the tests.

During the tests, the images captured by the SUAS are transmitted and stored on the GCS, which includes a standalone laptop. The GCS has access controls in place that ensure that only those with an authorized need to know (S&T RAPS team) can access the images. The RAPS team stores images under password protection. The RAPS team immediately deletes any images that unintentionally captured private citizens or property during the course of the testing.

Once the SUAS capabilities are validated through these tests, S&T may conduct pre-operational tests with DHS Customs and Border Protection (CBP) at border locations. The locations will be determined at a later date. This PIA will be updated prior to such tests.

The different systems being tested offer a range of capabilities; some systems are more sophisticated than others. As such, privacy mitigations may vary depending on system capabilities. For example, a system with low camera resolution may not require face-blurring or anonymizing features, as no footage would capture identifiable images.

As the technology continues to mature and develop, the privacy risks and concerns will evolve as well. To proactively address these concerns and risks, DHS is establishing a UAS issue working group to explore departmental roles and equities involving privacy and civil liberties. The working group aims to identify and address privacy and civil liberties issues related to DHS uses of UAS by providing policies, procedures, and best practices. The working group will produce a white paper that contains further privacy analysis and recommendations that can be used as best practices or foundational principles for other federal, state, and local government users, as well as non-government users.

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 (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. 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 the test and evaluation activities of the SUAS as it relates to the Fair Information Principles.

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.

The tests at Fort Sill only involve volunteer research participants. All volunteers receive notice and provide informed consent prior to participating in the tests. No members of the public are affected by the tests.

If operational tests are conducted with CBP, DHS will update this PIA, and if applicable, any SORNs, to address privacy concerns associated with those tests.

Individual notice depends on the specific operation in which the SUAS is used. Depending on where the system operates, how the system is used, and the users' legal authority, notice may or may not be provided. For example, FEMA may use the system to look for victims stranded in a flood zone. In such cases, providing advanced notice would not be feasible.

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.

Research participants volunteer to participate in the tests conducted at Fort Sill. The S&T RAPS team provides notice and obtains informed consent from the volunteers prior to the start of the study. By participating in the tests, volunteers understand that the SUAS can capture and transmit their images to

the ground control system. If the SUAS incidentally capture images of private citizens or property, the images are immediately deleted by the S&T RAPS team, in accordance with program protocol.

If operational tests are conducted with CBP, CBP will develop policies regarding notice, and DHS will update this PIA prior to the tests. However, once in operational use, depending on the SUAS use, individuals may not always be given the opportunity to consent to image collection, as it may compromise operations and diminish the operational utility of the system. The SUAS operational user will ultimately be responsible for ensuring that the appropriate policies and procedures are in place prior to deployment of the systems.

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 purpose of the test and evaluation activities is to determine the effectiveness of the SUAS in supporting various emergency responder operations. Prior to participating in the tests, volunteers receive notice about the tests and provide informed consent to participate. The images captured during the tests are only used to evaluate the effectiveness of the SUAS to determine its utility in supporting emergency responder operations and providing situational awareness. The images of volunteers may also be used in reports or presentations to demonstrate the SUAS capability. The images are not matched in any databases, used, or shared for any other purposes. The results of the SUAS tests are compiled into a final report, which may be distributed to the emergency responder community and used to support acquisition or purchasing decisions.

The SUAS can be programmed to fly on a prescribed flight path or manually controlled from the GCS by the operators. In the case of a lost connection between the user and the aircraft, the system can be programmed to automatically return to the point of the lost connection or to the area of takeoff, depending on the system being tested. Data collection and transmission continues as long as the connection to the GCS is active, though it is possible some systems have the ability to store data on the aircraft itself. Any data that contains imagery not related to the test activities (e.g., non-volunteers or area outside the test perimeter) is deleted.

Any tests conducted with CBP are done to determine the utility of the SUAS in an operational setting. In the future, the SUAS may be used to conduct various border security activities. This PIA and if applicable, any SORNs, will be updated prior to use of SUAS for border security purposes. Similarly, if and when the SUAS are deployed for other operational use, DHS users need very specific purposes of flight, and the images and footage captured will only be used to support legitimate law enforcement and first responder activities.

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 SUAS collects and retains images of volunteers for the duration of the tests. No additional information from the volunteers is required or collected for the tests. The purpose of the tests is to determine the effectiveness of the SUAS in providing situational awareness to emergency responders. Some images of volunteers may be used in test reports or presentations to demonstrate the SUAS capabilities. If any images of private citizens or property are incidentally captured during the tests, the S&T RAPS team immediately deletes the images; they are not used for any purposes, related to the project or not.

If the SUAS are deployed for operational use, the amount of data captured and the use of data minimization, such as face blurring, will depend on the specific system, program, and purpose. For example, if the SUAS are deployed to detect illegal activities at the border, CBP would program the SUAS to only fly in the predetermined, designated border areas. Even so, images of innocent individuals crossing the border may be incidentally captured. Data minimizing technologies, such as face-blurring, could be used by CBP to protect the identities of such individuals while the data is stored. Additionally, policies and rules of behaviors will be in place to guide how the data is used, and the data should be disposed of once it is no longer needed.

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.

During the tests, the images of volunteers are only used for the purpose of testing and evaluating the SUAS performance. The images captured by SUAS may also be shared with the emergency responder community or other potential end users to demonstrate system capabilities. S&T does not use the images for any other purposes.

Operational users should develop and implement policies and rules of behavior to guide the collection and use of images and footage captured by SUAS.

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.

The images captured by SUAS are used only to evaluate the system. The development portion of the testing determines the image quality using resolution boards under different environmental conditions (e.g., sun conditions, humidity). During the operational evaluation, the imagery can help identify the location of individuals during search and rescue and police operations. The sensors are measured for their effectiveness in various operational scenarios, such as whether an individual is armed or unarmed. The sensor and camera resolution of the SUAS vary and depends on the system itself as well as on the needs of the end user. All imagery is transmitted via a data link from the SUAS to the GCS at near-real time. The quality of the video image should be sufficient to distinguish between a human and an animal and the relative size difference between individuals. The images taken are not matched in any databases; the systems being tested are not capable of performing facial recognition.

The S&T RAPS team does not attempt to identify individuals based on the images, unless that is part of the test scenario (e.g., locating and tracking person of interest). Even then, the focus is the physical characteristics of the individual, rather than the physical identity.

When the SUAS are deployed for operational use, they should only be used in a manner that is consistent with DHS policies and the published program PIA and/or SORN.

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 S&T test and evaluation activities, the images are transmitted to a standalone laptop with access controls in place, including user name and password protection, to limit access to only those with an authorized need to know. The test and evaluation process will also determine what security features are available for SUAS.

In an operational setting the SUAS will capture and transmit images to emergency responders who access the images and take appropriate response actions. The SUAS users can opt to use security measures such as encryption, if available, to protect image transmission from the aircraft to the ground control system, in addition to access controls. Hacking a SUAS while in flight in order to control its movement or intercept its imagery has proven to be very difficult even under strict experimental settings, but the threat does exist. The operational community will take measures to mitigate these risks as the technology matures and the operational settings become clearer.

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 S&T staff are required to complete annual privacy awareness training. Access controls are in place to ensure only authorized access to the system and images. Furthermore, the test and evaluation activities, only volunteers who provide informed consent participate in the simulated test scenarios. No members of the public are impacted by the tests.

Operational users may opt to conduct periodic audits on systems, to ensure that the SUAS are being used appropriately, and in support of legitimate law enforcement or first responder activities. Periodic audits would also ensure that data is properly disposed when it is no longer needed.

Conclusion

SUAS provide rapid response and situational awareness capabilities to the emergency responder community that enables them to make operational decisions which could ultimately save lives. In the simulated test and evaluation activities, SUAS are used on various realistic and relevant scenarios to

emergency responders to determine the effectiveness and utility of the systems. Privacy concerns are mitigated by only using volunteer participants for these tests. Furthermore, technical safeguards and access controls are built into the system to ensure authorized access to the system and images. CBP or any other DHS operational users will have the responsibility to ensure that standard operating procedures and policies are in place guide the use of SUAS prior to deployment.

Responsible Officials

John Appleby
Program Manager
Borders and Maritime Security Division
Science and Technology Directorate
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

_____

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