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

Privacy Impact Assessment Update
for the

Aircraft Systems

DHS/CBP/PIA-018(a)

April 6, 2018

Contact Point
Andrew Scharnweber
U.S. Border Patrol
U.S. Customs and Border Protection
(202) 325-4149

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

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) employs several types of aircraft, including manned helicopters, fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft may be equipped with video, radar, and sensor technologies to assist CBP in patrolling the border, conducting surveillance for law enforcement investigations or tactical operations, or gathering data to assist in disaster relief and emergency response. In addition, the United States Border Patrol (USBP) operates Small Unmanned Aircraft Systems (sUAS) in support of its border security mission. CBP is publishing this updated Privacy Impact Assessment (PIA) to provide notice of CBP's use of sUAS not addressed in the original PIA, and to assess the privacy impacts of its use of this technology.

Overview

CBP is responsible for securing nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. CBP employs various border surveillance technologies to provide comprehensive situational awareness along the U.S. border and to assist in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. CBP has previously described and assessed the privacy risks of Border Surveillance Systems (BSS),[1] including commercially available and Department of Defense reuse[2] technologies such as fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, and radio frequency sensors. In addition to BSS, CBP also employs several types of aircraft, including manned helicopters, fixed-wing aircraft, UAS, and sUAS for border surveillance and law enforcement purposes. These aircraft may be equipped with video, radar, and other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in disaster relief or emergency response.

[1] *See* DHS/CBP/PIA-022 Border Surveillance Systems (BSS) (August 29, 2014), *available at* https://www.dhs.gov/privacy.

[2] As part of CBP's efforts to seek innovative ways to acquire and use technology, CBP formed a partnership with the Department of Defense (DoD) to identify and reuse "excess" DoD technology. To date, CBP has acquired several types of technology, including sUAS, thermal imaging equipment, night vision equipment, and tactical aerostat systems. The technology from DoD increases CBP's situational awareness and operational flexibility in responding to border threats.

Reason for the PIA Update

CBP is conducting a PIA update for the original Aircraft Systems PIA[3] to a) clarify that Border Patrol Agents also operate aircraft with surveillance equipment and b) include CBP's new use of sUAS. Aircraft equipped with surveillance technologies enhance situational awareness for USBP Field Commanders and Agents in areas that are remote or otherwise inaccessible. In many cases, traditional manned air support is neither timely nor cost effective, and USBP Agents on patrol in conjunction with fixed location sensors cannot provide persistent, omnipresent, and discreet surveillance capabilities. Land-based, mobile, and fixed surveillance capabilities are also limited by the terrain and climatic conditions which frequently reduce the range for observation. To help close these gaps, CBP is deploying sUAS to complement the current inventory of manned aircraft and large UAS.

Unlike CBP's manned aircraft, the pilot controls UAS from the ground, and the large UAS are capable of flying longer distances and longer hours continuously. Like large UAS, sUAS are also piloted from the ground, but are generally limited in endurance and capability compared to the larger UAS. sUAS differ from UAS in that they provide a highly mobile, usually hand-launched system weighing less than 55 pounds. CBP's sUAS are operated by USBP and include both commercially available and DoD reuse technologies such as vertical take-off multi-rotor[4] and fixed-wing[5] unmanned aircraft, with optional payloads such as video surveillance systems, rangefinders,[6] thermal imaging devices,[7] and radio frequency sensors.[8] CBP's sUAS include limited-range platforms, which have an average flight time of 30-40 minutes; medium-range platforms, with flight times of 90 minutes; and longer-range platforms, with flight times of up to three hours.

Small UAS are highly portable and can be rapidly deployed to high-risk areas, allowing CBP to reduce surveillance and situational awareness gaps. CBP operates sUAS in accordance with Federal Aviation Administration (FAA) Certificate of Authorization (COA) requirements via an online notification process and in accordance with Part 107 rules and guidelines.[9] CBP works

---

[3] *See* DHS/CBP/PIA-018 Aircraft Systems (September 9, 2013), *available at* https://www.dhs.gov/privacy.
[4] Vertical Take Off and Landing platform is an unmanned aircraft which can hover in place, take off, and land vertically.
[5] Fixed-Wing platform is an unmanned aircraft that is capable of flight using wings that generate lift caused by the vehicle's forward airspeed and the shape of the wings. Fixed-wing aircraft are distinct from rotary-wing aircraft, in which the wings form a rotor mounted on a spinning shaft.
[6] A rangefinder measures distance from the sensor payload to an item of interest and assists the operator in determining location in relation to other objects.
[7] A thermal imaging device is a device that forms an image using infrared radiation, similar to a common camera that forms an image using visible light.
[8] Radio frequency sensors do not collect cell phone communications.
[9] Part 107 of the Federal Aviation Regulations provides rules for non-hobbyist small (*e.g.*, under 55 pounds) unmanned aircraft operations. *See* https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516.

with the FAA to develop the COAs to define airspace for unmanned operations. Consistent with the primary mission for the sUAS, these COAs define airspace (altitude, latitude, and longitude) along the border and generally outside of urban areas to support CBP sUAS flight operations. Pursuant to the FAA COA, USBP is authorized to operate sUAS at or below 1200 feet above ground level in Class G[10] airspace. In addition, USBP Internal Operating Procedures (IOP) further restrict operations to sparsely-populated locations, defined as those areas indicated in yellow on FAA Visual Flight Rule (VFR) sectional charts.[11] When planning operations, the sUAS Operator will refer to the FAA's Aeronautical Chart User's Guide,[12] as well as publicly available tools like SkyVector[13] to view FAA VFR sectional charts. As the FAA develops its roadmap to integrate sUAS into the National Airspace System (NAS), CBP will adjust to any new requirements and continue to employ sUAS in pursuit of its primary border security mission.

Except for those operations where it is necessary to safeguard human life, the FAA COA restricts USBP from flying sUAS over a human being unless that human being is directly participating in the operation of the sUAS or the human being is located under a covered structure or inside a stationary vehicle that may provide reasonable protection from a falling sUAS. For those operations in which it is necessary to operate the sUAS over a human being in order to safeguard human life, the sUAS operator must not operate in proximity to human beings or any lower than is necessary to accomplish the mission at hand.

In addition, sensor payloads onboard sUAS are oriented toward the border and away from communities and places of worship and commerce frequented by local residents, when operationally feasible. While sUAS may record lawful activity during official USBP operations, (*e.g.*, individuals entering a local establishment, in public places, associating with other individuals, or vehicle license plates), these recordings will be overwritten unless an authorized sUAS user determines the recording is needed for an approved purpose.

CBP is deploying sUAS in multiple phases during Fiscal Year (FY) 17 and FY18, beginning with limited pilot projects[14] throughout high risk USBP areas of operation. Following successful deployment of these pilot projects, CBP will finalize its technical operational

---

[10] Class G airspace is defined by the FAA as uncontrolled airspace. Uncontrolled airspace is generally defined as the airspace from the surface up to 700 or 1200 feet above ground level in most of the United States, but up to as high as 14,500 feet in some remote Western and sparsely-populated areas.
[11] *See* FAA VFR Sectional Charts, *available at* https://www.faa.gov/air_traffic/flight_info/aeronav/productcatalog/vfrcharts/Sectional/.
[12] *See* FAA Aeronautical Chart User's Guide, *available at* https://www.faa.gov/air_traffic/flight_info/aeronav/digital_products/aero_guide/.
[13] *See* Skyvector.com, *available at* https://skyvector.com/.
[14] Pilot projects will be initiated with the Special Operations Group and in the following U.S. Border Patrol Sectors: Tucson Sector, Rio Grande Valley Sector, and Swanton Sector.

requirements and refine tactics, techniques, and procedures to determine deployment of sUAS to all sectors/stations over a three-year period, or as funding permits.

Similar to other aircraft, CBP plans to deploy sUAS in the following scenarios: (1) to patrol the border; (2) to conduct surveillance for investigative operations; (3) to conduct damage assessment in disaster situations; and (4) in response to officer safety situations in support of agents on the ground.[15]

Patrolling the Border

CBP uses all of its aircraft to patrol different parts of the border based on the specific capabilities of the type of aircraft. sUAS provide USBP with access to previously inaccessible border areas (due to rugged or difficult terrain), while lowering the risk to agents patrolling those areas. sUAS will help to mitigate existing gaps in border security by providing aerial surveillance capabilities in situations in which manned helicopters and fixed-wing aircraft or UAS are either not available or are not practical due to the high cost or the remoteness associated with the area of operations. sUAS may enhance USBP Agent safety by providing the capability of surveilling and detecting threats from afar before agents enter high risk areas and situations. Prior to a mission, the sUAS Operator is responsible for coordinating the sUAS Operations Area (SOA) with the appropriate airspace controlling party. For example, in Tucson Sector, USBP Agents work with the Joint Intelligence Operations Center (JIOC) to de-conflict airspace in a given area. Usually, the SOA will be a 2.5-mile radius from a specific location, but could be larger. Use of the airspace is authorized for a set amount of time, usually an eight-hour period.

Investigative Operations

CBP uses both sUAS and other manned and unmanned aircraft to support investigative operations conducted by other DHS components, such as U.S. Immigration and Customs Enforcement (ICE), and by other federal law enforcement agencies, such as the Federal Bureau of Investigation (FBI) or Drug Enforcement Agency (DEA). Requests for sUAS support are directed to the respective USBP sector Chief Patrol Agent responsible for the geographic area in which operations are to be conducted for authorization. Each request follows a standard process and is reviewed and considered by the Chief Patrol Agent of each USBP Sector in terms of the requesting agencies' authorities to receive the information, CBP's authority to lend assistance, and CBP's ability to integrate the information collection into its mission. USBP must also determine the availability of sUAS and the integration of the requested activity into its operations.

[15] Particularly in regards to USBP support for disaster assistance and officer safety/recovery, USBP may operate sUAS in support of other federal agencies. As such, it is possible that USBP sUAS, when operated in support of an agency with the authority to do so, may conduct operations away from the border. All operations will be conducted in accordance with the current FAA COA.

Typical support missions include overhead observation of subjects of investigations, specific locations of interest, and conveyances for enhanced situational awareness and increased officer/agent safety. For example, CBP may deploy sUAS to conduct surveillance over a building to inform ground units of the general external layout of the building or rugged or inaccessible terrain in order to provide the location of vehicles or individuals along the border and between the ports of entry. When flying sUAS in support of another component or government agency for an investigative operation,[16] CBP may provide the other agency downloaded video images, photographs, radio frequency emissions, and location information of the operation, in whole or in part, based on the request.

Disaster Support

CBP may also use sUAS during natural disasters in support of other DHS components, other federal agencies, and state and local partners. For example, CBP may use sUAS to provide images of flooding or other damage to the Federal Emergency Management Agency (FEMA), state emergency operations centers, the United States Geological Survey (USGS), or the U.S. Army Corps of Engineers. In general, video and other data information from these operations are not used to identify individuals and are not typically associated with personally identifiable information (PII). As with other requests for support, disaster area overflight requests are assigned in accordance with the national policy regarding sUAS operations.

Officer/Agent Safety and Support to State and Local Law Enforcement

State and local law enforcement officials may request CBP sUAS support in emergency situations to improve officer safety when aerial surveillance is necessary or the terrain is too difficult for law enforcement personnel to navigate. Requests for sUAS support are directed to the respective USBP sector Chief Patrol Agent responsible for the geographic area in which operations are to be conducted for authorization. CBP may provide video images, photographs, radio frequency emissions, and location information taken during emergency situations to other DHS components. Sharing of this information with state and local partners, including foreign and other authorized entities, is on a case-by-case basis as determined through CBP's Request for Information process.

Information Captured by sUAS

Due to the altitude at which sUAS operate and the technical limitations of current sensors, the video images and photographs the sUAS-deployed surveillance tools generally do not provide enough detail for an operator to determine a person's identity. The only information about individuals that is collected or retained is the indication of a human form, as well as other contextual information (*e.g.*, that an individual is carrying a backpack or a large item, such as a

[16] CBP does not loan out sUAS for other agencies to use. At all times, CBP personnel will be in control of sUAS being operated to assist another agency.

long gun). Video images, photographs, radio frequency emissions, and location information captured by sUAS, however, may be associated with a person if the person is apprehended. For example, video images and photographs may show several individuals traversing the land border and being intercepted by officers/agents of CBP. While the video images and photographs are generally not sufficiently precise to permit actual identification, the circumstances of CBP interdiction and apprehension of a suspect in conjunction with the aerial surveillance are sufficient to link the indistinct images of persons traversing the ground to the suspect's case file. Individuals who are apprehended by CBP as a result of observation by sUAS at or near the border may have video images, photographs, radio frequency emissions, and location information of their crossing and apprehension associated with their enforcement case file. CBP obtains biographical data pertaining to the apprehended person following time of apprehension. CBP stores all biographic, biometric and case information obtained from apprehended individuals in the appropriate law enforcement case management system (in most USBP cases, in the CBP E3 system[17]). In general, CBP maintains any related video images, photographs, radio frequency emissions, and location information obtained from the sUAS on removable media in accordance with chain of custody protocols.

Video images, photographs, radio frequency emissions, and location information captured by sUAS are recorded via a ground control station (GCS).[18] In the case of medium-range and longer-range sUAS platforms, surveillance video is fed to a stand-alone computer through the GCS and is recorded in real-time. The controller on sUAS platforms acts as both the GCS and mechanism for controlling the platform. On small sUAS platforms, data is recorded to an SD card inside the controller. Data can be downloaded from the GCS of an individual sUAS system as individual video files and maintained on DVD or other digital medium as case file evidence for prosecution cases and for training purposes. Data may be copied for storage for training and prosecution purposes and titled by date of incursion, sUAS registration number, and number of individuals involved. When data is copied to a DVD for prosecution purposes, the prosecution case number will be added to the title. CBP stores DVDs consistent with its chain of custody protocols.

Following a flight, the video images, photographs, radio frequency emissions, and location information captured by sUAS are generally not downloaded unless required as evidence for prosecution, investigation, or training purposes. Subsequently, and only upon official request, access to a particular image may be provided to authorized persons who have a "need to know;" when the dissemination is in response to a particular law enforcement activity or case, that analysis may include PII. sUAS video images, photographs, radio frequency emissions, and location

[17] *See* DHS/CBP/PIA-012(a) CBP Portal (E3) to EID/IDENT (August 9, 2017), *available at* https://www.dhs.gov/privacy.

[18] A ground control station (GCS) is a land- or sea-based control center that provides the facilities for human control of the sUAS.

information of the crossing or apprehension of persons whose apprehension is the subject of a video recording by a sUAS or manned or unmanned aircraft, may be associated with a law enforcement case file that contains 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 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. Given that Aircraft Systems and their associated devices are mechanical and operational systems rather than a distinct information technology system or collection of records pertaining to an individual that would be subject to the parameters of the Privacy Act, this updated PIA is conducted to relate the use of these observation and data collection platforms to the DHS construct of the FIPPs. This updated PIA examines the privacy impact of Aircraft Systems operations as it relates to the DHS 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.

CBP is issuing this updated PIA to provide notice to the public of its use of small unmanned aircraft systems. In conjunction with the previously published BSS PIA, this PIA update serves to inform the public generally of the presence of surveillance capabilities at the border and the use of capabilities to detect and support the apprehension of persons crossing the border illegally. CBP

has also published the Border Patrol Enforcement Records (BPER) System of Records Notice (SORN),[19] which provides notice of CBP's collection of information related to enforcement activities between ports of entry. Although information collected through sUAS technology is not generally personally identifiable, when CBP associates sUAS video images, photographs, radio frequency emissions, and location information with an individual, that information may become subject to the requirements of the Privacy Act and the BPER SORN.

Per the approved FAA COA effective from November 2017 to November 2019, CBP is required to file Notice to Airmen (NOTAM) not more than 72 hours in advance but not less than 24 hours in advance of known operations. CBP has established and is currently testing the air space deconfliction process, which includes the notification of CBP Air and Marine Operations (AMO) and general/commercial aviation of sUAS operating locations via the NOTAM process. The area of operation is defined in the NOTAM and includes a point and the minimum radius required to operate except as authorized as a special provision. Due to the immediacy of some tactical operations, NOTAM notification may be reduced to no less than 30 minutes prior to operations in cases when CBP was not aware of the need to conduct the operation more than 24 hours in advance.

All individuals entering the United States at and between the ports of entry are subject to monitoring and data collection for operational and situational awareness. CBP posts signs at ports of entry to notify individuals of the monitoring and information collection requirements. However, CBP cannot reasonably provide timely notice for individuals encountered between ports of entry. This PIA and the BPER SORN serve as general notice of CBP's use of sUAS and other aircraft to monitor activities along the U.S. border.

Privacy Risk: There is a risk that a member of the public will not know that a sUAS is operated by CBP and may be collecting photo, video, or other information obtained through surveillance technology.

Mitigation: This risk is partially mitigated through the publication of this PIA, which provides notice of CBP's use of sUAS. The risk that an individual may not receive timely notice of an individual aircraft cannot be fully mitigated. Due to the size of these aircraft, CBP cannot brand them in a way that will make their association easily discernable. In addition, CBP may avoid providing notice of a sUAS in a particular area when doing so might compromise the integrity of a law enforcement operation or investigation.

USBP will conduct operations in accordance with the current, approved Federal Aviation Administration Certificate of Authorization (FAA COA) and USBP Internal Operating Procedures (IOP). This risk is further mitigated by the fact that the FAA COA restricts sUAS flights to Class G airspace. The USBP IOP further limits operations to sparsely-populated areas as defined by the FAA's Aeronautical Chart User's Guide. USBP IOP further restricts operations to sparsely

[19] *See* DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).

populated locations, defined as those areas indicated in yellow on FAA Visual Flight Rule (VFR) sectional charts.[20] When planning operations, the sUAS Operator will refer to the FAA's Aeronautical Chart User's Guide[21] to identify unpopulated areas of the border, as well as, publicly available tools like SkyVector[22] to view FAA VFR sectional charts.

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.

In general, the impacts to individual participation have not changed since the publication of the 2013 Aircraft Systems PIA. Like traditional fixed wing aircraft and large UAS, CBP primarily uses sUAS to maintain situational awareness of the border area and to locate individuals who are crossing the border illegally or engaged in illegal activity in the border area. Allowing an individual to consent to the collection, use, dissemination, and maintenance of sUAS video images, photographs, radio frequency emissions, and location information would compromise operations and would interfere with the U.S. government's ability to protect its borders.

In the event that sUAS information is linked to an individual subject of a CBP law enforcement or other investigation, access procedures are described in this PIA and in the BPER SORN.[23] Although the BPER SORN asserts exemptions from the access provisions of the Privacy Act for the information maintained pursuant to its terms, such exemptions are reviewed in the context of each request. To seek access to information collected via sUAS and linked to a law enforcement case file maintained in E3,[24] individuals may request information about themselves, pursuant to the access provisions of the Privacy Act of 1974 (5 U.S.C. § 552a(d)), as applicable, or pursuant to the Freedom of Information Act (FOIA) (5 U.S.C. § 552).

Any individual, regardless of citizenship or immigration status, may seek notification of and access to any CBP record contained in E3 pursuant to procedures provided by FOIA, and can do so by visiting https://www.cbp.gov/site-policy-notices/foia, or by mailing a request to:

---

[20] *See* FAA VFR Sectional Charts, *available at* https://www.faa.gov/air_traffic/flight_info/aeronav/productcatalog/vfrcharts/Sectional/.
[21] *See* FAA Aeronautical Chart User's Guide, *available at* https://www.faa.gov/air_traffic/flight_info/aeronav/digital_products/aero_guide/.
[22] *See* Skyvector.com, *available at* https://skyvector.com/.
[23] *See* DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 FR 72601 (October 20, 2016).
[24] *See* DHS/CBP/PIA-012(a) CBP Portal (E3) to EID/IDENT (August 9, 2017), *available at* https://www.dhs.gov/privacy.

U.S. Customs and Border Protection (CBP)
Freedom of Information Act (FOIA) Division
1300 Pennsylvania Avenue NW, Room 3.3D
Washington, DC 20229

When seeking records about one's self from any of the system of records applicable or any other Departmental system of records, the request must conform to the Privacy Act regulations set forth in federal regulations regarding Domestic Security and Disclosure of Records and Information. The individual must first verify his or her identity, meaning that the requestor must provide his or her full name, current address, and date and place of birth. The requestor must sign his or her request, and the signature must either be notarized or submitted under federal statute regarding Unsworn Declarations Under Penalty of Perjury, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While an inquiry requires no specific form, forms may be obtained for this purpose from the DHS Chief Privacy Officer and DHS Chief FOIA Officer, https://www.dhs.gov/freedom-infomration-act-foia, or 1-866-431-0486. In addition, the request should:

- Explain why the requestor believes the Department would have information on him or her;
- Identify which component(s) of the Department the requestor believes may have requested information about him or her;
- Specify when the requestor believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS Component agency may have responsive records.

If individuals are uncertain what agency or database manages the information, they may seek redress, regardless of citizenship, through the DHS Traveler Redress Program ("TRIP"), 601 South 12th Street, TSA- 901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

Privacy Risk: There is a risk that individuals are not aware of their ability to make record access requests for CBP records.

Mitigation: This risk is partially mitigated. This updated PIA and the BPER SORN describe how individuals may make access requests under FOIA or the Privacy Act, as applicable. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. To ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law and policy.

Privacy Risk: Due to the law enforcement nature of the information collected by sUAS and maintained in E3 or another case management system, there is a risk that individuals will not be able to access, correct, or amend their records since the records are exempted from access, correction, and amendment under the Privacy Act.

Mitigation: This risk is partially mitigated. Information from certain CBP source systems may be amended as indicated in the applicable SORN. However, providing individual access or correction of records may be limited for law enforcement reasons, including as expressly permitted by the Privacy Act. Permitting access to the records could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, or to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

Privacy Risk: With the recent cancellation of the DHS Mixed Systems policy[25] through DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*,[26] there is a risk that persons other than U.S. Citizens and Lawful Permanent Residents are now unable to access, correct, and amend their information as they were previously able to do.

Mitigation: This risk is partially mitigated. This updated PIA and the BPER SORN describe how individuals can request access under FOIA or the Privacy Act, as applicable. Redress is available for U.S. Citizens and Lawful Permanent Residents through requests made under the Privacy Act as described above. U.S. law prevents DHS from extending Privacy Act redress to individuals who are not U.S. Citizens, Lawful Permanent Residents, or the subject of covered records under the Judicial Redress Act. However, these individuals still may seek notification of and access to records pursuant to procedures provided by FOIA. Additionally, to ensure the accuracy of CBP's records, CBP may permit access and amendment, regardless of citizenship, on a case-by-case basis, consistent with law and policy.

---

[25] For more information, please *see* Privacy Policy Guidance Memorandum 2007-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, *available at* https://www.dhs.gov/privacy.

[26] For more information about the recent cancellation of the DHS Mixed Systems policy, please *see* the DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, *available at* https://www.dhs.gov/privacy.

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.

CBP's use of sUAS conforms to the purposes specified in 2013 Aircraft Systems PIA. Like other aircraft surveillance technology covered in the original PIA, CBP uses sUAS surveillance capabilities for the same purposes as other UAS in order to perform its law enforcement missions under the Immigration and Nationality Act of 1952, as amended, and other pertinent provisions of immigration laws and regulations,[27] as well as pertinent provisions of customs laws and regulations.[28] CBP collects information in conformance with the Electronic Communications Privacy Act of 1986, as amended, and the Communications Act of 1934, as amended.[29] CBP is authorized to collect video, other images, signals information, and data using surveillance capabilities to include sUAS in support of its border security mission. These authorities allow CBP to obtain information in support of the border interdiction of narcotics and other contraband, the prevention of the illegal entry of aliens into the United States, and in support of federal, state, and local law enforcement, counterterrorism, and emergency humanitarian efforts.

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).

CBP seeks to minimize the collection and retention of video images, photographs, radio frequency emissions, location, and other information that is necessary and relevant to carry out CBP's mission. sUAS missions are generally carried out in remote unpopulated areas of the border where criminal activity is known or suspected to occur. The collection and retention of this information has not changed with the addition of sUAS technology. Unlike other aircraft systems, sUAS do not stream video images, photographs, radio frequency emissions, and location information to CBP systems (*e.g.*, BigPipe).[30] Instead, the information remains on the device originally used for recording until it is overwritten through re-use, which is dependent on the system memory but is generally limited to 30 days or less.

---

[27] Pub. L. 82-414. *See* 8 U.S.C. §§ 1225 and 1357.
[28] 19 U.S.C. §§ 482, 507, 1461, 1496, 1581, 1582, and 1595a(d).
[29] 18 U.S.C. § 2510 et seq; 47 U.S.C. § 151 et seq.
[30] BigPipe serves as a conduit, similar to a television cable, that transports live mission video feeds from the source systems owned by CBP Air and Marine Operations (AMO) and U.S. Border Patrol (USBP) to users within CBP and other DHS Components.

Like other aircraft systems, the information collected by sUAS is not subject to the Privacy Act unless it is retrieved by using an individual's name or other unique identifier. If an individual is apprehended by CBP as a result of observation by sUAS or subsequent association from the presence of CBP assets, CBP may have video images, photographs, radio frequency emissions, and location information of that individual's apprehension associated with the individual's enforcement case file. Those video images, photographs, radio frequency emissions, and location information may be retained for up to 75 years if associated with an arrest, detention, or removal, in accordance with the retention schedule of the BPER SORN.

Privacy Risk: There is an over-collection risk associated with the fact that CBP may operate sUAS in Class G airspace, which may include populated areas.

Mitigation: Although CBP generally uses sUAS to monitor areas that are inaccessible and generally sparsely-populated, the FAA COA does not specifically prevent CBP from operating sUAS in populated areas. This risk is partially mitigated by the fact that CBP retains information obtained from sUAS for 30 days or less, unless the information is linked to an enforcement event. Further, the risks to the individual are limited by the fact that sUAS do not collect personally identifiable information unless the images are then linked to an enforcement action.

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.

As with all video and still images captured by CBP operated aircraft, CBP uses sUAS to collect video images, photographs, radio frequency emissions, and location information pursuant to its law enforcement authority, as part of its border security mission, or in support of another agency when that other agency's authority covers the mission either through delegation of authority or direct control of the information collected. Per the FAA COA, sUAS may operate along the northern and southwest borders, but may not operate over urban areas. While the images or information collected is generally not sufficiently precise to permit actual identification of a person, the images or information may be associated with an individual from context within the image, circumstances surrounding the activity occurring in the image, or additional information obtained directly from the person by an officer/agent. The images or information are only associated with an individual if the individual is apprehended or if the images are taken as part of an ongoing law enforcement investigation. Accordingly, the data can only be used for the purposes specified in Section 3 of this updated PIA.

When sUAS data is needed as evidence for prosecution, a sUAS Operator retrieves the recorded incident information from the respective sUAS GCS. Surveillance video recordings can be downloaded from the GCS of an individual sUAS system as individual video files and maintained on DVD or other digital medium as case file evidence for prosecution cases and for training purposes. Surveillance video events may be copied for storage for training and prosecution purposes and titled by date of incursion, sUAS registration number, and number of individuals involved. When video is copied to a DVD for prosecution purposes, the prosecution case number will be added to the title. CBP follows evidentiary and chain of custody procedures, including proper markings, while handling recorded incident information. Not all "evidence" will include persons under arrest. Events can occur solely for intelligence collection or seizure of property, not involving persons, and tagged with an event number or field information report number.

In some circumstances, non-PII video recordings and other data that is not associated with an apprehended individual(s) may provide value in an intelligence context. USBP may share these images with the CBP Office of Intelligence (OI). These unassociated images are separately maintained by OI for a maximum of five years.

Privacy Risk: There is a risk that sUAS may capture information about individuals or activities that are beyond the scope of CBP's authorities. For example, sUAS cameras may capture individuals entering places or engaging in lawful activities as they relate to their daily lives because the border includes populated areas. Although unlikely during normal operations, there is a possibility that sUAS may collect video images, photographs, radio frequency emissions, and location information of an individual entering a doctor's office, attending public rallies, social events, or meetings, or associating with other individuals.

Mitigation: This risk is mitigated by the fact that sUAS are generally flown along the northern and southwest border and away from urban areas, communities, and places of worship when operationally feasible. While sUAS cameras may record lawful activity at or near the border, these recordings are automatically overwritten unless an authorized sUAS Operator determines the recording is needed for an approved purpose. Specifically, CBP copies and retains sUAS video images, photographs, radio frequency emissions, and location information only when the images captured are relevant to an active case file for law enforcement or border security purposes. CBP does not associate the sUAS recorded video or other data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation. Any video images, photographs, radio frequency emissions, and location information associated with a law enforcement case is covered by the SORN that maintains the case file.

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 addition of sUAS capability does not change data quality or integrity as described in the 2013 Aircraft Systems PIA, as the technology deployed on sUAS does not differ substantially from the tools deployed on other aircraft. As explained in Section 4 above, to ensure that the PII captured by sUAS is relevant and timely, video images, photographs, radio frequency emissions, and location information must be associated within 30 days with the individual(s) CBP apprehends, or all information is overwritten. Although sUAS are capable of operating for the entirety of the designated mission at lower altitudes than larger aircraft, the video resolution and images are under normal circumstances not precise enough to permit the actual identification of the individual(s). Unless the information is linked to an apprehension or other investigative case file, video recordings and related data offer no continued value in a law enforcement support context.

To help ensure the quality and integrity of the information collected and used as evidence, CBP requires its USBP Agents to successfully complete training on the proper operation of sUAS and the associated recording equipment. This training includes correct techniques to copy recorded evidence from a non-portable hard drive to portable digital media and procedures to ensure that such evidence is not co-mingled with data from other investigations; procedures in maintaining chain of custody for all recorded evidence; and training to ensure that the USBP Agent making a recording transfers the recordings in their original unedited format, to portable media. The USBP Agent making the recording must label all copies of portable media with the corresponding case number (if available), the date and place of the original recording, and the names of the USBP Agent and sUAS Operator. The USBP Agent making the recording must also label, initial, and maintain possession of the evidence until custody is properly transferred to the appropriate designated evidence custodian, case agent, Assistant United States Attorney, or other appropriate Government official. As with any information associated with a case file, once the images are cross referenced to an investigation or case, they become covered by the system of records for that case file system and subject to the access and amendment provision of that system.

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.

As with all data captured by CBP operated aircraft, CBP has taken steps to protect the video

images, photographs, radio frequency emissions, and location information captured by sUAS. Whenever possible, CBP uses encrypted feeds to pass video and other information recorded on a flight to the GCS. Although not all sUAS video feeds are currently encrypted, CBP is awaiting advancements in sUAS technology that is expected to resolve this concern. Video, photographs, and other information captured by sUAS is subject to access controls and an approval process requiring clearance by system administrators to ensure that only authorized users with a need to know have access to the video images, photographs, radio frequency emissions, and location information. Any recorded images that are saved to be used as evidence must be handled in accordance with CBP policy to maintain and preserve chain of custody. Images that are used as evidence must be handled according to the procedures detailed in Section 6 of this updated PIA. All recorded evidence must be kept in a locked container, segregated from other property or equipment. Video that is collected during an investigative operation that contains sensitive analytical surveillance, or reconnaissance-related data may not be disclosed unless a request for disclosure has been submitted. The request must include a copy of the information that is to be disclosed, and must clearly specify the name of the intended recipient, how the information will be used, restrictions on further dissemination, and the reasons justifying the disclosure.

Privacy Risk: There is a risk that the transmission of unencrypted video images, photographs, radio frequency emissions, and location information could be intercepted by unauthorized parties.

Mitigation: This risk is partially mitigated. CBP intends to use sUAS to identify if there is an operational utility to using sUAS to support its border security mission. CBP believes the privacy risk posed by sUAS is minimal since, in the event of an unauthorized disclosure of information from the sUAS, the identity of the individual(s) is not known unless and until the image is associated with a prosecution case. As technology advances in commercial systems, CBP will continue to evaluate the capability offered and will incorporate platforms offering these advanced technologies.

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.

With the addition of sUAS, there is no change in CBP's accountability and auditing practices. All CBP employees are required to complete annual privacy awareness training, in addition to training on ethics and the CBP Code of Conduct. Access controls, both physical and technological, are in place to ensure only authorized access to the aircraft systems and the collected data/images. All USBP Agents using sUAS must be certified. CBP requires employees to

successfully complete training on techniques to copy recorded evidence to portable digital media and requires them to follow procedures to ensure that such evidence is not co-mingled with data from other investigations. CBP employees must follow procedures to maintain an adequate chain of custody in the event that the information is used as evidence.

CBP has a process in place for restricting the dissemination of sUAS video images, photographs, radio frequency emissions, and location information and keeps a log of the disclosures. CBP redacts law enforcement sensitive information, PII, and other sensitive related data unless the requestor has a valid need to know. CBP periodically reviews the logs or disclosure records to ensure compliance with established privacy policies, practices, and procedures for associated systems.

Responsible Officials

Andrew Scharnweber
Associate Chief
U.S. Border Patrol
U.S. Customs and Border Protection

Debra L. Danisek
CBP Privacy Officer
Privacy and Diversity Office
U.S. Customs and Border Protection

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Privacy Impact Assessment
for the

USCG Research and Development Center (RDC) Small Unmanned Aircraft Systems (sUAS) Program

DHS/USCG/PIA-026

February 22, 2018

Contact Point
Evan Gross
United States Coast Guard
Research and Development Center (RDC)
(860) 271-2647

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

Abstract

The Department of Homeland Security (DHS) United States Coast Guard (USCG) Research and Development Center (RDC) has been tasked and funded to evaluate small Unmanned Aircraft Systems (sUAS) for potential use by USCG for operational missions. sUAS include small aircrafts (typically less than 55 pounds in weight) that are generally operated using a wireless ground control station (GCS). The aircraft are equipped with sensors and cameras that can capture images and transmit them to standalone GCSs to provide aerial views of USCG missions for situational awareness to the operators and users. USCG is conducting this Privacy Impact Assessment (PIA) to address the privacy impacts of sUAS surveillance and image capturing capabilities.

Introduction

sUAS technology has the potential to be a valuable tool for rapid response and situational awareness prior to and during USCG operations. The sUAS are equipped with electro-optical (EO) and infrared (IR) cameras that feed images to standalone, non-networked flight computers (GCSs). Part of the research being conducted by the RDC is evaluating various commercially available EO/IR camera payloads for capability, capacity, limitation, and overall mission impact. All imagery collected during sUAS evaluations is transmitted directly to the operator for the purpose of safely operating the aircraft and evaluation of the system's target detection capabilities. The scope of this research includes the ongoing deployment and evaluation of sUAS from USCG vessels and shore sites at locations around the country over the next several years. This technology is meant to eventually be a tool to supplement manned assets performing USCG missions by providing critical situational awareness.

The overall objective of the RDC's research efforts is not to collect personally identifiable information (PII), but to understand how sUAS technology could facilitate USCG operations. This technology could enable more effective responses in all 11 USCG mission sets: ports, waterways, and coastal security; drug interdiction; aids to navigation; search and rescue; living marine resources; marine safety; defense readiness; migrant interdiction; marine environmental protection; ice operations; and other law enforcement activities.

Testing sUAS for USCG mission sets typically requires flights over the open water area surrounding USCG cutters. No PII is collected during these test flights by the sUAS (see below for the information USCG collects and uses). However, USCG requires USCG test participants to assist in simulating targets of interest, whether they be disabled boaters, drug smugglers, alien smugglers, or vessels fishing illegally. Tests include search patterns, EO/IR payload evaluations, and sUAS endurance and capabilities as technology advances. All individuals acting as test

participants in sUAS testing will be active and consenting members of the USCG RDC program, briefed on the capabilities of each sUAS system, assigned a portion of the test plan to execute to generate only the information required to assess sUAS for USCG research purposes.

EO and IR cameras provide the means for collecting images/information and are capable of capturing video at any altitude. However, the level of altitude impacts whether objects and images are recognizable. The higher the altitude, the less visibility and detail of a particular object/image. At no point will the test participant's personal identification information (*e.g.*, name) be available to link to the image. In addition, the quality of the imagery should only be sufficient enough to distinguish between human, animal, and target type, and the relative size differences between individuals. Any inadvertent images captured during this test will not clearly differentiate between individuals, and no facial recognition technology is used.

Nonetheless, RDC programs and projects will take all reasonable steps necessary to maintain the security of any potential PII, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. All of the data (images/video) that is initially captured in the GCS is for research exercises and can only be accessed by a few select individuals. The data is typically deleted from the GCS at the end of each day of the testing event. There are instances when images/video useful in supporting the ongoing analysis would be transferred to the USCG workstation project folder, which has access limited to the project team only. None of the images/video will constitute PII because the sUAS cameras and test procedures do not allow for such visual clarity and the data will not be maintained in a manner that allows it to be linked to any PII. Should any of the images/video be selected for use in a briefing/presentation/report, the RDC has a rigidly controlled review process that includes the Program Manager (PM), Branch Chief, Scientific and Technical Information (STINFO) Officer, Public Affairs Officer (PAO), Security Officer Technical Director, and Executive Director on a review panel to ensure that the appropriate level audience, markings, and security have been addressed.

The test plans, controls, and Federal Aviation Administration (FAA) regulations[1] that govern each test event will prohibit reckless operation of a sUAS. The images captured by sUAS are transmitted and stored on the GCS, which includes a standalone laptop. The GCS have access controls in place that ensure only those with an authorized need to know can access images. RDC stores relevant images such as snapshots of test scenarios to show validity of various payload evaluations under password protection and typically deletes all images at the end of each day of the test event, unless it is useful in supporting ongoing analysis.

[1] *See* Federal Aviation Administration regulations at 14 CFR Part 107 – Small Unmanned Aircraft Systems.

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. 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. USCG RDC is a research entity rather than particular information technology system. This PIA examines the privacy impact of USCG RDC sUAS research activity 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.

This PIA provides a level of transparency to the public regarding USCG RDC sUAS testing efforts. All individuals designated as test participants will be active and consenting members of the RDC program. Participants will be briefed on the capabilities of each sUAS system, assigned a portion of the test plan to execute, and fulfill a test team support role in generating only non-PII required to assess sUAS for USCG research.[2] Each participant will be made aware that his or her unidentifiable image could potentially be captured during the execution of a test and at no point will the participant's personal identification be available to correspond with the image.

None of the sUAS systems as part of this research effort are secret. Prior to each evolution of testing, RDC notifies the FAA (through the filing of publicly-available Notices to Airmen

[2] The information generated and how it is generated depends on the test performed. Often it involves determining payload performance; tactics, techniques, and procedures for operating sUAS on USCG surface platforms; and the impact the sUAS system can have on USCG mission sets.

(NOTAMs)), the local air station, CG Office of Aviation Forces (CG-711)), and local and tribal leaders.

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.

All designated test participants will be personnel from the RDC program. Participants will be briefed on the capabilities of each sUAS system, assigned a portion of the test plan to execute, and fulfill a test team support role in generating only the information required to assess sUAS for USCG research. The RDC sUAS program is designed to not collect PII. Prior to testing, all systems will be calibrated to ensure data quality and integrity. The imagery will only be of sufficient quality to distinguish between human, animal, and asset, and the relative size differences between individuals. The images taken will not be matched to any database or names of the participants, and will not be capable of performing facial recognition.

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 research is to determine the effectiveness of sUAS in supporting various USCG operations, consistent with the requirements and authorities spelled out in 14 U.S.C. §§ 81 and 87-89. This technology is meant to eventually be a tool to supplement manned assets performing USCG missions by providing critical situational awareness.

USCG RDC currently owns unmanned aircraft systems that include aircraft typically under 55 pounds with wingspans of three (3) to six (6) feet or less that are characteristically operated using a GCS. Each sUAS is equipped with sensors and cameras capable of capturing images or other data, and transmitting them to GCSs to provide aerial views in support of numerous USCG missions.

The systems under test will not collect PII when operated in accordance with the test plans, FAA regulations, and DHS and USCG policies that govern this effort.

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).

sUAS are only being tested for use as a potential situational awareness tool to support USCG missions. The RDC will provide its own test participants and platforms to generate imagery and telemetry to assess sUAS capabilities. While not collecting PII from sUAS, the RDC will have access to the basic PII of participants necessary to run the program. This PII will never be linked to data collected by sUAS.

Any information generated during this research will be from consenting RDC program personnel. Prior to testing, all systems will be calibrated to ensure data quality and integrity. The quality of the imagery should only be sufficient enough to distinguish between human, animal, and asset, and the relative size differences between individuals. The images taken will not be matched to any database and will not be used to support a facial recognition program.

Any inadvertent images captured during this test will not clearly identify individuals. Images taken would consist of things like letter boards or an item in the water to simulate an oil spill. The RDC will take all reasonable steps necessary to maintain the security of the images captured and ensure no PII is captured. All data and images retained from the sUAS testing events will be protected from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

Information collected by or on behalf of the RDC using sUAS is deleted from the GCS at the end of each day of the test operation, unless retention of the information is determined to be necessary to the ongoing technology assessment; it is then maintained in a system of records relative to the applicable USCG mission.

Privacy Risk: There is a potential risk that sUAS operators may inadvertently collect more information than needed.

Mitigation: RDC programs and projects use the least amount of information consistent with the documented purpose(s), and use minimization techniques such as synthetic data or anonymization where appropriate and practicable. The sUAS research projects do not need, nor would use any images of non-USCG targets for use in reporting test results. If any private or public images are inadvertently captured they will be deleted immediately and steps will be taken to minimize the possibility of recurrence.

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.

Although research test analysis data may be shared with federal partners, no PII data is collected from the sUAS, and thus none is shared externally or internally.

The systems under test will not collect PII when operated in accordance with the test plans, FAA regulations, and DHS and USCG policies that govern this effort. The authority to collect or purpose for the collection and use of PII harbor no conceivable benefit to the research effort.

Information will only be used to assess the platform and payloads of the sUAS. Detection and vessel identification are key components to evaluating the systems and their ability to facilitate USCG missions. RDC will provide its own test participants and assets to generate imagery for this assessment.

Privacy Risk: There is risk that identifiable images of test participants will be collected inadvertently during the test efforts and used in analysis reports/presentations.

Mitigation: USCG mitigates this risk by only using technology that does not allow for such visual clarity to identify any specific individuals. The RDC further mitigates this risk by carefully reviewing video and images captured by the GCS and used in analysis reports/presentations to ensure no images contain PII.

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.

Information collected will only be used to assess the platform and payloads of the sUAS. The video and images generated by the sUAS are used only to evaluate the system. There is no need for PII to be collected to perform the assessment of the sUAS.

RDC will be providing its own test participants and assets to generate imagery for this assessment. Prior to testing, all assets and systems will be calibrated to ensure data quality and integrity. The quality of the imagery should only be sufficient enough to distinguish between human, animal, and asset, and the relative size differences between individuals. The images taken will not be matched to any database and will not be capable of performing facial recognition.

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.

DHS and USCG will adhere to the security safeguards that govern all DHS and USCG operations as they would in the course of any research effort. All images captured by sUAS during the test exercises are transmitted to an encrypted, password-protected GCS, and only those individuals with an authorized need to know will have access to the GCS and the information contained therein.

Any private or public images/video captured by the sUAS will be deleted from the GCS immediately. The sUAS research projects do not need, nor would use any footage of non-USCG targets for use in reporting test results.

Privacy Risk: There is a risk unauthorized individuals may access the data.

Mitigation: RDC programs and projects will take all reasonable steps necessary to maintain the security of all data collected, and will protect the data from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. All images captured by the sUAS during the test exercises are transmitted to an encrypted, password protected, standalone GCS and accessed only by those having a need to know. Any PII inadvertently collected will be safeguarded along with all other data collected, but the PII will be deleted from the GCS once discovered.

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.

No PII will be collected by sUAS as part of this research effort; however, all RDC personnel are required to complete annual DHS privacy training regarding the safe handling and protection of PII.

The images/video data initially captured in the GCS for research exercises is only accessible to a few select individuals. Data is deleted from the GCS at the end of each day of testing unless there are instances in which the data might be useful in supporting the ongoing analysis. In such cases, the data would then be transferred to the USCG workstation project folder, which only the project team can access.

Conclusion

Unmanned aircraft technology has the potential to be a valuable tool for rapid response and increased situational awareness prior to and during potentially dangerous USCG operations. The overall objective of the RDC research efforts is not to collect PII, but to understand how this technology could facilitate USCG operations. Using sUAS for USCG mission sets typically requires flights over unpopulated areas or over open water, to determine the location or presence of vessels without the fidelity to collect images of individuals aboard. All data captured by sUAS are transmitted and stored on the GCS, which includes a standalone, non-networked laptop. The GCS has access controls in place that ensure that only those with an authorized need to know access the system. RDC only stores relevant images of USCG test targets and conducts all test events in accordance with the sensitive information protection policies of DHS and USCG. RDC does not retain any imagery collected by sUAS that is not relevant to evaluating the operational utility of the system(s).

Responsible Officials

Evan Gross
Research and Development Center
United States Coast Guard

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Domestic Use of Unmanned Aircraft Systems (UAS)

Policy Framework

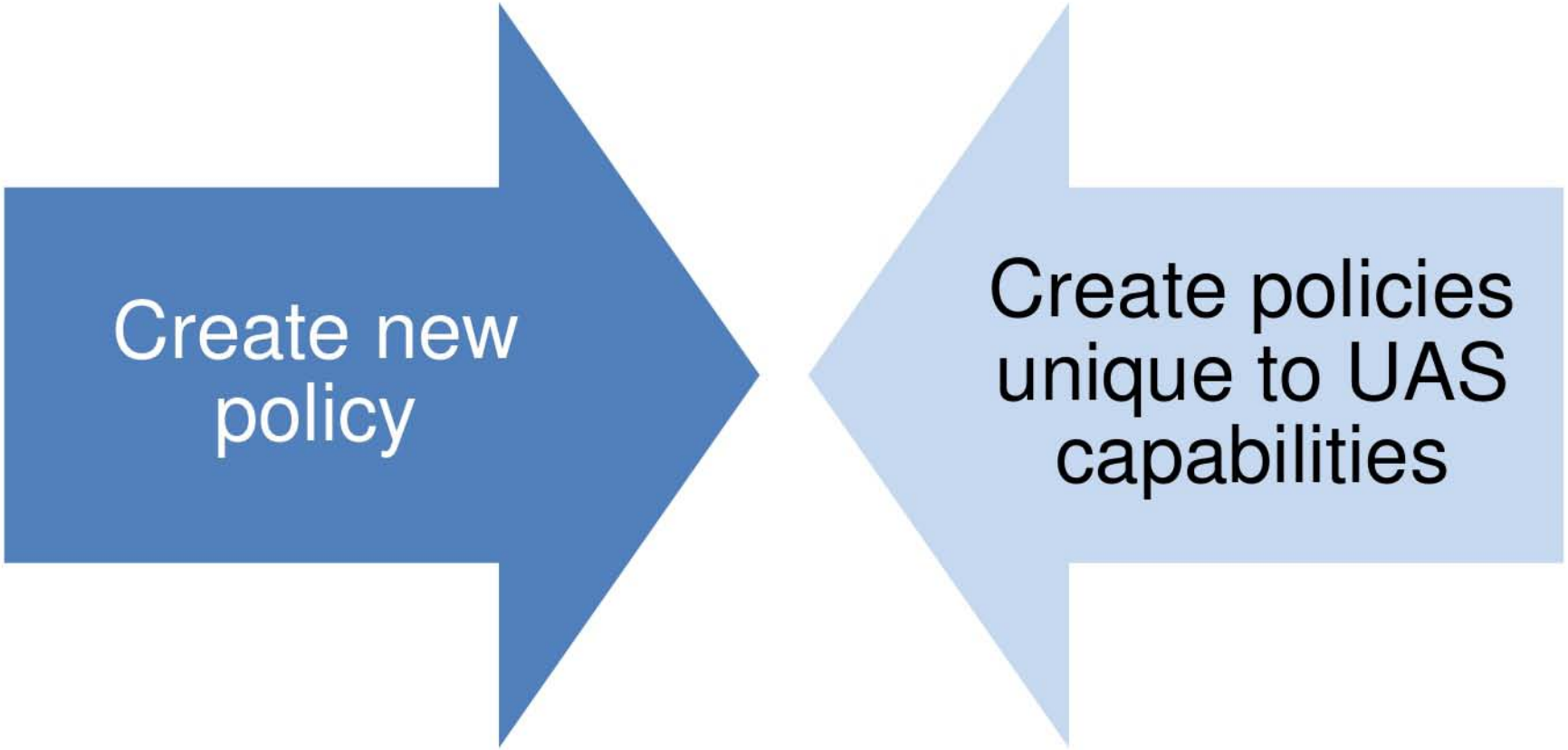
Policy Framework

TRANSPARENCY - RESPONSIBLE USE		
	PUBLIC	**CIVIL**
Privacy Safety/Security Vetting	• Law Enforcement	• Commercial

	• Non Law Enforcement
	  • Emergency Response
	  • Scientific/Research/ Property management
		• General Aviation

		• Recreational/Hobby
Air Defense		

Policy Objective



Capabilities unique to UAS

- Persistent Surveillance
- Inability to detect
- Ability to compromise

Overarching Principles

TRANSPARENCY	ACCOUNTABILITY (RESPONSIBLE USE)

Overarching Principles

TRANSPARENCY	ACCOUNTABILITY (RESPONSIBLE USE)
Consistent and transparent U.S. Government position: • Data: Collection, use, retention, sharing • Consistent policy for all public operations – Federal/State and Local • Consistent messaging to public	Ensure UAS operations are safe, secure, and have established standards for operation: • Ensure Accountability • Establish appropriate vetting standards • Establish standards for cyber and communications security (safety of flight)

Public Operations (Gov't)

TRANSPARENCY AND RESPONSIBLE USE		
Law Enforcement	**Response**	**Non-Emergency**

• Border surveillance (DHS CBP)
• Enforcement operations (eg FBI, DEA, State and Local partnerships)
	• Disaster Preparedness and response (DHS, FEMA)
	• Search and Rescue (State and Local partnerships)
		• Scientific Research (NASA, USCG)
		• Property Monitor (DOI, DHS)
		  • Monitor infrastructure
		  • Monitor Federal land/property/ animal migration

TRANSPARENCY AND RESPONSIBLE USE

Public - Law Enforcement

Privacy	Safety/Security	Vetting

• Persistent surveillance
• FOIA
• 4th amendment alignment (Notice of surveillance)
• Protection of data and info sharing
	• Ensure safety of flight and protect the UAS from attempts to disrupt flight operations
	  • Spectrum allocation
	  • Wayward UAS protections
	  • Position/location identifiers
	• Determine appropriate scoping (55 pounds or less, flown within visual line of site, less than 400 feet above the ground, during daylight, within Class G airspace, and outside of 5 statute miles from any airport, or other location with aviation activities)
		• Manned Aircraft process
		  • Public Operators responsible for vetting/training
		• Consensus to align UAS vetting requirements for Public Operators with Manned aircraft requirements?

TRANSPARENCY AND RESPONSIBLE USE

Public – Response (Emergency)

Privacy	Safety/Security	Vetting

• Persistent surveillance?
• Info sharing
• 4th amendment alignment (Notice of surveillance)?
	• Ensure safety of flight and protect the UAS from attempts to disrupt flight operations
	  • Spectrum allocation
	  • Wayward UAS protections
	  • Position/location identifiers
	• Determine appropriate scoping
		• Manned Aircraft process
		  • Public Operators responsible for vetting/training
		• Consensus to align UAS vetting requirements for Public Operators with Manned aircraft requirements?

TRANSPARENCY AND RESPONSIBLE USE

Public - Non-Emergency

Privacy	Safety/Security	Vetting

• Persistent surveillance?
• Info sharing
• 4th amendment alignment (Notice of surveillance)?
	• Develop appropriate cyber and communications security polices to ensure safety of flight and protect the UAS from attempts to disrupt flight operations
	  • Spectrum allocation
	  • Wayward UAS protections
	  • Position/location identifiers
	• Determine appropriate scoping
		• Manned Aircraft process
		  • Public Operators responsible for vetting/training
		• Consensus to align UAS vetting requirements for Public Operators with Manned aircraft requirements?

Civil Operations

TRANSPARENCY AND RESPONSIBLE USE		
Commercial	**General Aviation**	**Recreational**
• ConocoPhilips operations in Arctic • Permitted on case-by case basis by FAA	• Guided by Small UAS Rule (once implemented) • When operated outside of Hobbyist guidelines, and not commercially.	• Hobbyist organizations • FAA Guidelines for operations • Mandated by Congress not to impose Federal regulations on recreational use UAS

TRANSPARENCY AND RESPONSIBLE USE

Civil - Commercial Use

Privacy	Safety/Security	Vetting

• Collection
  • Use
  • Disclosure
  • Security of data
  • Retention
• Licensing, registration, auditing requirements
• Determine framework and scope
	• Ensure safety of flight and protect the UAS from attempts to disrupt flight operations
	  • Spectrum allocation
	  • Wayward UAS protections
	  • Position/location identifiers
	• Determine appropriate scoping
		• Manned aircraft process
		  • Where FAA certificate is required, vetting is completed (students, trainers, pilots)
		• Determine appropriate scoping and impact to agencies and public

TRANSPARENCY AND RESPONSIBLE USE

Civil - General Aviation

Privacy	Safety/Security	Vetting

Who has authority over what GA collects? How might UAS regs differ from manned aircraft?
• Licensing, registration, auditing requirements
	• Ensure safety of flight and protect the UAS from attempts to disrupt flight operations
	  • Spectrum allocation
	  • Wayward UAS protections
	  • Position/location identifiers
	• Determine appropriate scoping
		• Manned aircraft process
		  • Where FAA certificate is required, vetting is completed (students, trainers, pilots)
		• Determine appropriate scoping

TRANSPARENCY AND RESPONSIBLE USE

Recreational/ Hobbyist Use		
Privacy	**Safety/Security**	**Vetting**
Who has authority over what GA collects? How might UAS regs differ from manned aircraft? • Licensing, registration, auditing requirements	Congressional mandates to not overregulate model aircraft use (Public Law 112-95, Section 336) that must follow a community-based set of safety guidelines within a nationwide community organization.	Congressional mandates to not overregulate model aircraft use (Public Law 112-95, Section 336) that must follow a community-based set of safety guidelines within a nationwide community organization.

Defensive Use

TRANSPARENCY AND RESPONSIBLE USE		
Protect National Airspace System		
Privacy	**Safety/Security**	**Vetting**
N/A	• Scoping to determine when and how UAS in NAS a viable threat. • Differentiating between known users and unknown threat	N/A

Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems

Unmanned Aircraft Systems (UAS) technology continues to improve rapidly, and increasingly UAS are able to perform a variety of missions with greater operational flexibility and at a lower cost than comparable manned aircraft. A wide spectrum of domestic users -- including industry, private citizens, and Federal, State, local, tribal, and territorial governments -- are using or expect to use these systems, which may play a transformative role in fields as diverse as urban infrastructure management, farming, public safety, coastal security, military training, search and rescue, and disaster response.

The Congress recognized the potential wide-ranging benefits of UAS operations within the United States in the FAA Modernization and Reform Act of 2012 (Public Law 112-95), which requires a plan to safely integrate civil UAS into the National Airspace System (NAS) by September 30, 2015. As compared to manned aircraft, UAS may provide lower-cost operation and augment existing capabilities while reducing risks to human life. Estimates suggest the positive economic impact to U.S. industry of the integration of UAS into the NAS could be substantial and likely will grow for the foreseeable future.

As UAS are integrated into the NAS, the Federal Government will take steps to ensure that the integration takes into account not only our economic competitiveness and public safety, but also the privacy, civil rights, and civil liberties concerns these systems may raise.

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to establish transparent principles that govern the Federal Government's use of UAS in the NAS, and to promote the responsible use of this technology in the private and commercial sectors, it is hereby ordered as follows:

Section 1. UAS Policies and Procedures for Federal Government Use. The Federal Government currently operates UAS in the United States for several purposes, including to manage Federal lands, monitor wildfires, conduct scientific research, monitor our borders, support law enforcement, and effectively train our military. As with information collected by the Federal Government using any technology, where UAS is the platform for collection, information must be collected, used, retained, and disseminated consistent with the Constitution, Federal law, and other applicable regulations and policies. Agencies must, for example, comply with the Privacy Act of 1974 (5 U.S.C. 552a) (the "Privacy Act"), which, among other things, restricts the collection and dissemination of individuals' information that is maintained in systems of records, including personally identifiable information (PII), and permits individuals to seek access to and amendment of records.

(a) Privacy Protections. Particularly in light of the diverse potential uses of UAS in the NAS, expected advancements in UAS technologies, and the anticipated increase in UAS use in the future, the Federal

Government shall take steps to ensure that privacy protections and policies relative to UAS continue to keep pace with these developments. Accordingly, agencies shall, prior to deployment of new UAS technology and at least every 3 years, examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected. Agencies shall update their policies and procedures, or issue new policies and procedures, as necessary. In addition to requiring compliance with the Privacy Act in applicable circumstances, agencies that collect information through UAS in the NAS shall ensure that their policies and procedures with respect to such information incorporate the following requirements:

(i) Collection and Use. Agencies shall only collect information using UAS, or use UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose.
(ii) Retention. Information collected using UAS that may contain PII shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.
(iii) Dissemination. UAS-collected information that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements.

(b) Civil Rights and Civil Liberties Protections. To protect civil rights and civil liberties, agencies shall:

(i) ensure that policies are in place to prohibit the collection, use, retention, or dissemination of data in any manner that would violate the First Amendment or in any manner that would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law;
(ii) ensure that UAS activities are performed in a manner consistent with the Constitution and applicable laws, Executive Orders, and other Presidential directives; and
(iii) ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.

(c) Accountability. To provide for effective oversight, agencies shall:

(i) ensure that oversight procedures for agencies' UAS use, including audits or assessments, comply with existing agency policies and regulations;
(ii) verify the existence of rules of conduct and training for Federal Government personnel and contractors who work on UAS programs, and procedures for reporting suspected cases of misuse or abuse of UAS technologies;
(iii) establish policies and procedures, or confirm that policies and procedures are in place, that provide meaningful oversight of individuals who have access to sensitive information (including any PII) collected using UAS;
(iv) ensure that any data-sharing agreements or policies, data use policies, and record management policies applicable to UAS conform to applicable laws, regulations, and policies;

(v) establish policies and procedures, or confirm that policies and procedures are in place, to authorize the use of UAS in response to a request for UAS assistance in support of Federal, State, local, tribal, or territorial government operations; and
(vi) require that State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.

(d) Transparency. To promote transparency about their UAS activities within the NAS, agencies that use UAS shall, while not revealing information that could reasonably be expected to compromise law enforcement or national security:

(i) provide notice to the public regarding where the agency's UAS are authorized to operate in the NAS;
(ii) keep the public informed about the agency's UAS program as well as changes that would significantly affect privacy, civil rights, or civil liberties; and
(iii) make available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to State, local, tribal, or territorial governments.

(e) Reports. Within 180 days of the date of this memorandum, agencies shall provide the President with a status report on the implementation of this section. Within 1 year of the date of this memorandum, agencies shall publish information on how to access their publicly available policies and procedures implementing this section.

Sec. 2. Multi-stakeholder Engagement Process. In addition to the Federal uses of UAS described in section 1 of this memorandum, the combination of greater operational flexibility, lower capital requirements, and lower operating costs could allow UAS to be a transformative technology in the commercial and private sectors for fields as diverse as urban infrastructure management, farming, and disaster response. Although these opportunities will enhance American economic competitiveness, our Nation must be mindful of the potential implications for privacy, civil rights, and civil liberties. The Federal Government is committed to promoting the responsible use of this technology in a way that does not diminish rights and freedoms.

(a) There is hereby established a multi-stakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the NAS. The process will include stakeholders from the private sector.

(b) Within 90 days of the date of this memorandum, the Department of Commerce, through the National Telecommunications and Information Administration, and in consultation with other interested agencies, will initiate this multi-stakeholder engagement process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS use. For this process, commercial and private use includes the use of UAS for commercial purposes as civil aircraft, even if the use would qualify a UAS as a public aircraft under 49 U.S.C. 40102(a)(41) and 40125. The process shall not focus on law enforcement or other noncommercial governmental use.

Sec. 3. Definitions. As used in this memorandum:

(a) "Agencies" means executive departments and agencies of the Federal Government that conduct UAS operations in the NAS.

(b) "Federal Government use" means operations in which agencies operate UAS in the NAS. Federal Government use includes agency UAS operations on behalf of another agency or on behalf of a State, local, tribal, or territorial government, or when a nongovernmental entity operates UAS on behalf of an agency.

(c) "National Airspace System" means the common network of U.S. airspace; air navigation facilities, equipment, and services; airports or landing areas; aeronautical charts, information, and services; related rules, regulations, and procedures; technical information; and manpower and material. Included in this definition are system components shared jointly by the Departments of Defense, Transportation, and Homeland Security.

(d) "Unmanned Aircraft System" means an unmanned aircraft (an aircraft that is operated without direct human intervention from within or on the aircraft) and associated elements (including communication links and components that control the unmanned aircraft) that are required for the pilot or system operator in command to operate safely and efficiently in the NAS.

(e) "Personally identifiable information" refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, as set forth in Office of Management and Budget Memorandum M-07-16 (May 22, 2007) and Office of Management and Budget Memorandum M-10-23 (June 25, 2010).

Sec. 4. General Provisions.

(a) This memorandum complements and is not intended to supersede existing laws and policies for UAS operations in the NAS, including the National Strategy for Aviation Security and its supporting plans, the FAA Modernization and Reform Act of 2012, the Federal Aviation Administration's (FAA's) Integration of Civil UAS in the NAS Roadmap, and the FAA's UAS Comprehensive Plan.

(b) This memorandum shall be implemented consistent with applicable law, and subject to the availability of appropriations.

(c) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or
(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(d) Independent agencies are strongly encouraged to comply with this memorandum.

(e) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(f) The Secretary of Commerce is hereby authorized and directed to publish this memorandum in the Federal Register.

BARACK OBAMA

Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems

Unmanned Aircraft Systems (UAS) technology continues to improve rapidly, and increasingly UAS are able to perform a variety of missions with greater operational flexibility and at a lower cost than comparable manned aircraft. A wide spectrum of domestic users -- including industry, private citizens, and Federal, State, local, tribal, and territorial governments -- are using or expect to use these systems, which may play a transformative role in fields as diverse as urban infrastructure management, farming, public safety, coastal security, military training, search and rescue, and disaster response.

The Congress recognized the potential wide-ranging benefits of UAS operations within the United States in the FAA Modernization and Reform Act of 2012 (Public Law 112-95), which requires a plan to safely integrate civil UAS into the National Airspace System (NAS) by September 30, 2015. As compared to manned aircraft, UAS may provide lower-cost operation and augment existing capabilities while reducing risks to human life. Estimates suggest the positive economic impact to U.S. industry of the integration of UAS into the NAS could be substantial and likely will grow for the foreseeable future.

As UAS are integrated into the NAS, the Federal Government will take steps to ensure that the integration takes into account not only our economic competitiveness and public safety, but also the privacy, civil rights, and civil liberties concerns these systems may raise.

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to establish transparent principles that govern the Federal Government's use of UAS in the NAS, and to promote the responsible use of this technology in the private and commercial sectors, it is hereby ordered as follows:

Section 1. UAS Policies and Procedures for Federal Government Use. The Federal Government currently operates UAS in the United States for several purposes, including to manage Federal lands, monitor wildfires, conduct scientific research, monitor our borders, support law enforcement, and effectively train our military. As with information collected by the Federal Government using any technology, where UAS is the platform for collection, information must be collected, used, retained, and disseminated consistent with the Constitution, Federal law, and other applicable regulations and policies. Agencies must, for example, comply with the Privacy Act of 1974 (5 U.S.C. 552a) (the "Privacy Act"), which, among other things, restricts the collection and dissemination of individuals' information that is maintained in systems of records, including personally identifiable information (PII), and permits individuals to seek access to and amendment of records.

(a) Privacy Protections. Particularly in light of the diverse potential uses of UAS in the NAS, expected advancements in UAS technologies, and the anticipated increase in UAS use in the future, the Federal

Government shall take steps to ensure that privacy protections and policies relative to UAS continue to keep pace with these developments. Accordingly, agencies shall, prior to deployment of new UAS technology and at least every 3 years, examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected. Agencies shall update their policies and procedures, or issue new policies and procedures, as necessary. In addition to requiring compliance with the Privacy Act in applicable circumstances, agencies that collect information through UAS in the NAS shall ensure that their policies and procedures with respect to such information incorporate the following requirements:

(i) Collection and Use. Agencies shall only collect information using UAS, or use UAS-collected information, to the extent that such collection or use is consistent with and relevant to an authorized purpose.
(ii) Retention. Information collected using UAS that may contain PII shall not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.
(iii) Dissemination. UAS-collected information that is not maintained in a system of records covered by the Privacy Act shall not be disseminated outside of the agency unless dissemination is required by law, or fulfills an authorized purpose and complies with agency requirements.

(b) Civil Rights and Civil Liberties Protections. To protect civil rights and civil liberties, agencies shall:

(i) ensure that policies are in place to prohibit the collection, use, retention, or dissemination of data in any manner that would violate the First Amendment or in any manner that would discriminate against persons based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity, in violation of law;
(ii) ensure that UAS activities are performed in a manner consistent with the Constitution and applicable laws, Executive Orders, and other Presidential directives; and
(iii) ensure that adequate procedures are in place to receive, investigate, and address, as appropriate, privacy, civil rights, and civil liberties complaints.

(c) Accountability. To provide for effective oversight, agencies shall:

(i) ensure that oversight procedures for agencies' UAS use, including audits or assessments, comply with existing agency policies and regulations;
(ii) verify the existence of rules of conduct and training for Federal Government personnel and contractors who work on UAS programs, and procedures for reporting suspected cases of misuse or abuse of UAS technologies;
(iii) establish policies and procedures, or confirm that policies and procedures are in place, that provide meaningful oversight of individuals who have access to sensitive information (including any PII) collected using UAS;
(iv) ensure that any data-sharing agreements or policies, data use policies, and record management policies applicable to UAS conform to applicable laws, regulations, and policies;

(v) establish policies and procedures, or confirm that policies and procedures are in place, to authorize the use of UAS in response to a request for UAS assistance in support of Federal, State, local, tribal, or territorial government operations; and
(vi) require that State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds.

(d) Transparency. To promote transparency about their UAS activities within the NAS, agencies that use UAS shall, while not revealing information that could reasonably be expected to compromise law enforcement or national security:

(i) provide notice to the public regarding where the agency's UAS are authorized to operate in the NAS;
(ii) keep the public informed about the agency's UAS program as well as changes that would significantly affect privacy, civil rights, or civil liberties; and
(iii) make available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to State, local, tribal, or territorial governments.

(e) Reports. Within 180 days of the date of this memorandum, agencies shall provide the President with a status report on the implementation of this section. Within 1 year of the date of this memorandum, agencies shall publish information on how to access their publicly available policies and procedures implementing this section.

Sec. 2. Multi-stakeholder Engagement Process. In addition to the Federal uses of UAS described in section 1 of this memorandum, the combination of greater operational flexibility, lower capital requirements, and lower operating costs could allow UAS to be a transformative technology in the commercial and private sectors for fields as diverse as urban infrastructure management, farming, and disaster response. Although these opportunities will enhance American economic competitiveness, our Nation must be mindful of the potential implications for privacy, civil rights, and civil liberties. The Federal Government is committed to promoting the responsible use of this technology in a way that does not diminish rights and freedoms.

(a) There is hereby established a multi-stakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the NAS. The process will include stakeholders from the private sector.

(b) Within 90 days of the date of this memorandum, the Department of Commerce, through the National Telecommunications and Information Administration, and in consultation with other interested agencies, will initiate this multi-stakeholder engagement process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS use. For this process, commercial and private use includes the use of UAS for commercial purposes as civil aircraft, even if the use would qualify a UAS as a public aircraft under 49 U.S.C. 40102(a)(41) and 40125. The process shall not focus on law enforcement or other noncommercial governmental use.

Sec. 3. Definitions. As used in this memorandum:

(a) "Agencies" means executive departments and agencies of the Federal Government that conduct UAS operations in the NAS.

(b) "Federal Government use" means operations in which agencies operate UAS in the NAS. Federal Government use includes agency UAS operations on behalf of another agency or on behalf of a State, local, tribal, or territorial government, or when a nongovernmental entity operates UAS on behalf of an agency.

(c) "National Airspace System" means the common network of U.S. airspace; air navigation facilities, equipment, and services; airports or landing areas; aeronautical charts, information, and services; related rules, regulations, and procedures; technical information; and manpower and material. Included in this definition are system components shared jointly by the Departments of Defense, Transportation, and Homeland Security.

(d) "Unmanned Aircraft System" means an unmanned aircraft (an aircraft that is operated without direct human intervention from within or on the aircraft) and associated elements (including communication links and components that control the unmanned aircraft) that are required for the pilot or system operator in command to operate safely and efficiently in the NAS.

(e) "Personally identifiable information" refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, as set forth in Office of Management and Budget Memorandum M-07-16 (May 22, 2007) and Office of Management and Budget Memorandum M-10-23 (June 25, 2010).

Sec. 4. General Provisions.

(a) This memorandum complements and is not intended to supersede existing laws and policies for UAS operations in the NAS, including the National Strategy for Aviation Security and its supporting plans, the FAA Modernization and Reform Act of 2012, the Federal Aviation Administration's (FAA's) Integration of Civil UAS in the NAS Roadmap, and the FAA's UAS Comprehensive Plan.

(b) This memorandum shall be implemented consistent with applicable law, and subject to the availability of appropriations.

(c) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or
(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(d) Independent agencies are strongly encouraged to comply with this memorandum.

(e) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(f) The Secretary of Commerce is hereby authorized and directed to publish this memorandum in the Federal Register.

BARACK OBAMA