Privacy Impact Assessment
for the

Small Unmanned Aircraft Systems

DHS/CISA/PIA-031

July 25, 2019

Contact Point
Linda Solheim
Infrastructure Security Division
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
(703) 603-5075

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

Abstract

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Infrastructure Security (IS) Division plans to incorporate the use of small unmanned aircraft systems (sUAS) into its program offering exercises to critical infrastructure protection stakeholders to train for, assess, practice, and improve performance in prevention, protection, mitigation, response, and recovery capabilities for natural or man-made attacks. Uses during exercises include capturing photographic and video images of the exercise activities and to use the sUAS as a simulated payload delivery mechanism for certain exercise scenarios. CISA is conducting this Privacy Impact Assessment to address the privacy impacts of the sUAS image-capturing capabilities.

Introduction

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. Critical infrastructure provides services that are essential to the Nation's security, economic welfare, public health, and safety. Our critical infrastructure is highly complex and is majority owned and operated by entities other than the Federal Government. CISA works with these entities to help them mitigate the risk to critical infrastructure and provide them with information and analysis to make well informed decisions. CISA does this by assessing vulnerabilities at the asset[1] and system level; sharing strategic risk analysis and timely, actionable information; and providing tools and training to mitigate these risks.[2] Exercises are a useful tool in critical infrastructure security and resilience. Exercises can be used for testing and validating policies, plans, procedures, training, equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; improving individual performance; identifying gaps in resources; and identifying opportunities for improvement.[3]

The CISA Infrastructure Security (IS) Division Soft Targets and Crowded Places Task Force (STCP-TF) Infrastructure Stakeholder Security and Exercise Program (ISSEP) wishes to use small unmanned aircraft systems (sUAS)[4] for two purposes: (1) take aerial photo/video footage

[1] "[P]erson, structure, facility, information, material, or process that has value." DHS Lexicon, Terms and Definitions, 2017 edition – Revision 2, *available at* https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf.
[2] 6 U.S.C. § 652e.
[3] *See* the Homeland Security Exercise and Evaluation Program (HSEEP) April 2013, *available at* https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.
[4] An unmanned aircraft system is considered to be a small unmanned aircraft system if it weighs less than 55 pounds

during operational exercises and (2) use the sUAS as part of the scenario of an exercise itself. Aerial photo and video footage of an operational exercise would capture images, and video, of those individuals located within the predesignated exercise areas while also capturing the broader exercise location for exercise map-making purposes. It is an exercise best practice for controllers and evaluators to capture video and photographic evidence during the course of the exercise, so that exercise participants can fully understand what certain findings may be identified during the course of an after action. The second use is that the sUAS would be part of the scenario of the exercise itself. For example, as part of an exercise a non-sanctioned sUAS lands within a professional sports stadium with what looks like a suspicious payload. The sUAS would serve to land the suspicious payload in the area and have exercise participants respond to it as they would a real world incident. No photographic or video images will be captured by the sUAS as part of this second use.

ISSEP has procured three U.S.-manufactured sUAS that will be used during the course of the exercises. The sUAS will have the capability to take pictures and video, as well as be able to transfer that data via memory card. The operator terminals (either laptop or tablet) will be secured, but the sUAS's onboard data cannot be secured. The sUAS has a fail-safe that if the sUAS loses signal with the operator terminals it would return to the launch point. In addition, ISSEP plans to always keep the sUAS within the operator's line of sight while in use, per Federal Aviation Administration (FAA) regulations. Images from the sUAS platforms will be transferred via memory card, by either federal or contract support staff, and then transferred to the ISSEP shared drive. The shared drive is only accessible by members of the ISSEP exercise team and are not accessible by other federal or contract personnel. These images will then be used for generating exercise planning documents (e.g., maps, photos for the Situation Manual[5]), after action reports, as well as for reference during the post-exercise debriefs to capture any best practices or lessons learned. ISSEP will secure the sUAS and memory card during non-use in a secure storage case that will be locked with a combination only known to exercise personnel, and within a locked office that will be secured during all off hours. CISA will operate the sUAS in accordance with Office of Chief Counsel (OCC) guidance, and will abide by FAA laws and applicable regulations, either by applying for and acquiring a Certificate of Authorization (COA) for this activity as required for public aircraft, or by operating the sUAS as civil aircraft in accordance with Part 107 requirements.[6]

Participants in the exercises whose images could be captured by the sUAS will sign a participation liability waiver. The ISSEP team maintains the waivers electronically on the ISSEP

---

at takeoff, including everything attached to the aircraft. 14 C.F.R. § 107.3.

[5] A Situation Manual is provided for tabletop exercises and games as the core documentation that provides the textual background for a multimedia, facilitated exercise. It supports the scenario narrative and serves as the primary reference material for all participants during conduct. HSEEP Glossary, 11, 2013.

[6] *See* 49 U.S.C. §§ 40102, 40124; 14 C.F.R. § 1.1.

shared drive. Participants are also provided notice of the fact that their images will be collected and the intended use of the video and photos upon arrival at the exercise location at the sign-in table. The notice will also inform participants that signing in at the exercise location sign-in table will constitute affirmative consent to the collection of their images. The notice will include purposes for which the users' images will be collected. The same notice is provided in the email containing the participant briefing package, which describes what the participant will specifically be doing during the exercise. In addition, for events where the images of non-participants could be captured, ISSEP will provide notice to adjacent businesses and property owners, local first responders, and local politicians in an effort to maximize transparency.

ISSEP will be operating in a manner consistent with the "U.S. Department of Homeland Security Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs"[7] and the "Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems."[8] Both documents have stipulations about privacy and transparency.

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 sUASs and their associated devices are mechanical and operational systems rather than a distinct information technology system or collection of records under the Paperwork Reduction Act that would be subject to the parameters of the E-Government

[7] https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf.
[8] https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua

Act, Section 208, this PIA is conducted to relate the use of these observation and data collection platforms to the DHS construct of the FIPPs. In addition, inasmuch as the proposed use of the sUASs will not include the retrieval of any information using a unique identifier, the Privacy Act is not implicated. This PIA examines the privacy impact of CISA's sUAS 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 personally identifiable information (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.

CISA is issuing this PIA to provide notice to the public of its use of sUASs. CISA's use of sUASs is currently limited to use during exercises designed to better secure critical infrastructure.[9] When CISA uses the sUAS during exercises, exercise participants whose images could be captured by the sUAS sign a participation liability waiver. Participants are also provided notice of the fact that their images will be collected and the intended use of the video and photos upon arrival at the exercise location at the sign-in table. The same notice is provided in the email containing the participant briefing package, which describes what the participant will specifically be doing during the exercise. In addition, for events at which the images of non-participants could be captured, CISA will provide notice to adjacent businesses and property owners, local first responders, and local politicians, as appropriate, in an effort to maximize transparency.

If the sUAS incidentally captures discernable images of private citizens outside the boundaries of the exercise, the images are immediately identified by the team as they are reviewed during the process of downloading the memory card content to a secured file only accessible by the exercise team. Those images would not be used or shared outside of ISSEP and would not be used in any after action activity, report, or product. CISA is in the process of developing a retention schedule that reflects a shorter retention period for any inadvertently collected PII.

Privacy Risk: There is a risk that a member of the public will not know that a sUAS is operated by CISA and may be collecting photo or video images.

Mitigation: This risk is partially mitigated through the publication of this PIA, which provides notice of CISA'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, CISA cannot brand them in a way that will make their association easily discernable.

[9] The Preventing Emerging Threats Act of 2018, passed as part of the FAA Reauthorization Act of 2018 (Pub. L. 115-254), does not change this limitation to CISA's use of sUAS.

This risk is also mitigated by the fact that the imagery ISSEP intends to capture with the sUAS would likely not be clear enough to make out the identity of a member of the public during an exercise. Due to the altitude at which the sUAS will operate and the technical limitations of the sensors, the video images and photographs the sUAS-deployed observation tools generally do not provide enough detail for an operator to determine a person's identity. Generally, 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 wearing a firefighter or police officer uniform, or is carrying a backpack or a large item, such as a long gun). The video images and photographs are generally not sufficiently precise to permit actual identification. In addition, the boundaries maintained between the exercise area and publicly accessible areas will reduce the possibility that a member of the public will have his or her image inadvertently captured. If images captured by the sUAS do include images that contain discernable identities of individuals not participating in the exercise, CISA will immediately secure those images once the discernable identity is detected. Those images will not be shared outside of ISSEP and would not be used in any after action activity, report, or product. Stored images will not be retrieved by personal identifiers and will therefore not implicate the Privacy Act. Nor will stored images be used for any facial recognition purposes or analyzed in any way with the goal of identifying an individual. CISA may render assistance to law enforcement agencies investigating incidents that may have been captured by a sUAS camera once provided with a written request specifying the particular portion of the record desired and the law enforcement activity for which the record is sought.

CISA will conduct operations in accordance with a current, approved Federal Aviation Administration Certificate of Authorization (FAA COA) that covers the specific activity and identified locations for sUAS use.[10] This risk is further mitigated by the fact that the FAA COA restricts sUAS flights to Class G airspace.[11] Alternatively, CISA will conduct operations in accordance with Part 107 requirements, which require a remote pilot certificate with a sUAS rating,[12] visual line of sight by the pilot or observer,[13] operation below 400 feet,[14] and a prohibition against operating an sUAS above people,[15] among other requirements.

---

[10] For more information about FAA COAs, *see* https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/.

[11] Airspace not designated as Class A, B, C, D, or E is considered uncontrolled, Class G, airspace. Air Traffic Control does not have the authority or responsibility to manage air traffic within this airspace. In the Eastern U.S., Class G airspace lies between the surface and 700/1200 feet above ground level. For more information about airspace classification, *see* https://www.faa.gov/air_traffic/nas/nynjphl_redesign/documentation/feis/media/appendix_a-national_airspace_system_overview.pdf.

[12] 14 C.F.R. § 107.12.

[13] 14 C.F.R. § 107.31-33.

[14] 14 C.F.R. § 107.51.

[15] 14 C.F.R. § 107.39.

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.

For the use of sUAS during exercises, participants volunteer to participate in the exercises. The ISSEP team provides notice and obtains informed consent from the volunteers prior to the start of the exercise. By participating in the exercises, volunteers understand that the sUAS can capture and transmit their images to the operator terminals and save the images to the memory card on board the sUAS.

If the sUAS incidentally capture discernable images of individuals outside the boundaries of the exercise, the images are immediately identified by the team as they are reviewed during the process of downloading the memory card content to a secured file only accessible by the exercise team. Those discernable images would not be shared outside of ISSEP and would not be used in any after action activity, report, or product. These images are currently subject to DHS/NPPD/IP Records Control Schedule N1-563-08-31 Item (4)(b) "Records reflecting all other events/exercises."[16]

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 use of sUAS during critical infrastructure exercises is to capture photographic and video images during the course of the exercise, so that exercise participants can fully understand what certain findings may be identified during the course of an after action review of the exercise. This use is consistent with CISA authorities spelled out in 6 U.S.C. §§ 652 (e)(1)(B),[17] (e)(1)(F),[18] and (e)(1)(M).[19] These images will then be used for generating exercise planning documents (i.e., maps, photos for the Situation Manual), after action reports, as well as

[16] Records under this disposition are considered temporary and cut off at the end of the calendar year in which the exercise occurred. They are to be destroyed or deleted ten (10) years after the cutoff.
[17] "…To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States, including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks."
[18] "…To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities."
[19] "…To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department."

for reference during the post-exercise debriefs to capture any best practices or lessons learned. These documents, reports, and debriefs will be sanitized and will not contain identifiable facial images of individuals not participating in the exercise. Prior to participating in the exercises, volunteers receive notice about the exercises, the potential for their images to be collected during the exercise, the purposes for which their images to be collected, and then choose whether or not to provide informed consent to participate.

The sUAS can be programmed to fly on a prescribed flight path or manually controlled from the operator terminals 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. Data collection and transmission continues as long as the connection to the operator terminals are active. Images collected by the sUAS are not matched in any databases.

Privacy Risk: There is a risk that CISA will use UASs to collect or use PII for purposes other than those articulated in this PIA.

Mitigation: This risk is mitigated by the CISA Office of Privacy working closely with the program to ensure that all PII collected and used is consistent with the DHS privacy compliance documentation that the CISA sUAS Program has in place. For any proposed change in the purpose, the CISA Office of Privacy will work with the program to ensure privacy compliance before the change goes into effect. In addition, ISSEP will develop and follow Rules of Behavior during the operation of the sUASs, retrieval and storage of data from sUASs, and use of data in exercise products. Finally, all members of the ISSEP team receive annual privacy compliance training to ensure they understand their responsibilities for PII as a DHS employee or contractor.

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).

CISA seeks to minimize the collection and retention of photographic and video images to that which is necessary and relevant to CISA's mission.

Because of the altitude of operation during the exercise and the clarity of the cameras, the video images and photographs captured by the sUAS-deployed observation tools generally do not provide enough detail 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 wearing a firefighter or police officer uniform, or is carrying a backpack or a large item, such as a long gun). In addition, the boundaries maintained between the exercise

area and publicly accessible areas will reduce the possibility that a member of the public will have his or her image inadvertently captured. The video images and photographs are generally not sufficiently precise to permit actual identification. The images taken will not be matched to any database and will not be used in conjunction with a facial recognition program or analyzed in any way with the goal of identifying an individual, absent a written request from a law enforcement agency investigating an incident that may have been captured by the sUAS' camera(s).

Any inadvertent images captured that could be used to identify individuals not participating in the exercise will be immediately secured and protected. CISA will take all reasonable steps necessary to maintain the security of the images captured and, if PII is captured, will take measures to properly protect such records. All data and images retained from the sUAS will be protected from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. Any records created by the capturing and keeping of the photographic and video images will be disposed of in accordance with the NARA-approved DHS/NPPD/IP Records Control Schedule N1-563-08-31 Item (4)(b) "Records reflecting all other events/exercises."

Privacy Risk: The sUAS could capture inadvertent images of individuals.

Mitigation: This risk is partially mitigated by the fact that ISSEP intends to capture images that will not clearly identify individuals. In addition, ISSEP will take steps to ensure the security of the images captured and ensure no PII is captured. The operator will typically only engage the photographic camera and video camera function onboard the sUAS once the sUAS is well over the heads of the participants preventing someone viewing the images from distinguishing between specific humans other than the relative size of and distance between humans. The boundaries maintained between the exercise area and publicly accessible areas will reduce the possibility that a member of the public will have his or her image inadvertently captured. Images containing recognizable features of non-participants are not useful to the exercise since they would be too close to the ground and not able capture the broader exercise activity. Therefore, these images would be identified by the ISSEP team and not shared or included in any exercise report, presentation, or product.

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.

CISA will only capture the photographic and video images using the sUAS during exercises designed to better secure critical infrastructure. The images captured by the sUAS will generally not be precise enough to allow identification of a person. Any images collected by the sUAS during exercise activities would be used to generate exercise planning documents and after action reports, and images of identifiable individuals will be anonymized. Planning documents and

after action reports may be shared outside of the Department, but the images included in these materials would merely portray the presence of humans in relation to assets, and specific movements by humans in relation to the assets as part of an exercise. Specifically, federal, state, local, and tribal law enforcement and first responder entities with protection and response responsibilities for the critical infrastructure sites at which the exercise was conducted along with the owners and operators of the specific critical infrastructure will have access to the planning documents and after action reports. In some circumstances, critical infrastructure security and resilience partners (in both the public and private sector) may be given access to certain planning documents and after action reports as examples of products developed as part of the ISSEP exercise program.

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.

For the purposes of CISA's use of a sUAS, PII captured by the sUAS has no continuing value to CISA's critical infrastructure security and resilience mission. The quality of the imagery will be based on the altitude of the sUAS while in operation and should only be sufficient to distinguish between human, asset, the relative size differences between individuals, and movements by humans in relation to an asset. The images 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.

The sUAS can be programmed to fly on a prescribed flight path or manually controlled by the operators. In the case of a lost connection between the user and the aircraft, the system will be programmed to automatically return to the point of the lost connection or to the area of takeoff. The operator terminals will be secured, but the sUAS's onboard data cannot be secured. ISSEP plans to always keep the sUAS within the operator's line of sight while in use. Images from the sUAS platforms will be captured via memory card, by either federal or contract support staff, and then transferred to the ISSEP shared drive. The shared drive is only accessible by members of the ISSEP team and is not accessible by other federal or contactor personnel. Images collected by the sUAS are not matched in any databases. ISSEP will secure the sUAS and memory card during non-use in a secure storage case that will be locked with a combination only known to exercise personnel, and within a locked office that will be secured during all off hours.

Privacy Risk: The onboard data on the sUAS cannot be secured.

Mitigation: This risk is mitigated by the steps ISSEP takes during the operation of the sUAS, the transferring of the data from the sUAS to the ISSEP shared drive and the physical security of the sUAS when it is not in operation. By keeping the sUAS in the line of sight of the operator, the ISSEP team will be able to promptly recover the sUAS should it become disabled. In the event that the connection between the operator terminal and the sUAS, the system will be programmed to return to the point of lost connection or area of takeoff. Only members of the ISSEP team will handle the sUAS and the onboard memory card. The team will transfer the files captured on the memory card directly to the ISSEP shared drive and erase the images from the memory card. When not in use, the sUAS will be in a secure storage case and locked in an office during hours when a member of the ISSEP team is not in the office.

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 CISA employees are required to complete annual Privacy Awareness Training. When each employee completes the training, it is recorded in the employee's personnel file. CISA employees operating the controls of the sUAS must, if operating the sUAS as civil aircraft, have a remote pilot certificate or be under the direct supervision of a person who has the certification as required by Part 107. CISA must have a Certificate of Authorization from the FAA for the purpose and location(s) it desires to use the sUAS if operating it as a public aircraft. In either instance, CISA will ensure that this current certification or certificate is on file with the ISSEP team. In addition, physical and technological access controls are in place to ensure only authorized access to the sUAS and the images. Periodic audits will be conducted to ensure that the sUAS is being used appropriately and that the data is properly used and does not contain any inadvertent PII.

Conclusion

Small unmanned aircraft systems provide CISA the opportunity to offer better exercises to the critical infrastructure security and resilience stakeholder community by capturing video and photographic images of exercise activities from vantage points not previously available to this community. The overall purpose of this effort is not to collect PII, but collect images that would merely portray the presence of a human in relation to assets, and specific movements by humans in relation to the assets as part of an exercise. CISA has implemented access controls, procedures,

and protocols to ensure that stored images are properly handled and that proper protections and safeguards are in place to protect PII.

Responsible Officials

Linda Solheim
Infrastructure Security Division
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

_____

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