Privacy Impact Assessment

for the

Counter-Unmanned Aircraft Systems (C-UAS)

DHS Reference No. DHS/ALL/PIA-085

July 15, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) is leading efforts and coordinating across the federal government testing and evaluating technologies used to detect, identify, monitor, and, if needed, mitigate Unmanned Aircraft Systems (UAS) that pose a credible threat to covered facilities, assets, and other missions authorized to the it by law. These protective technologies are referred to as Counter-UAS (C-UAS). This Privacy Impact Assessment (PIA) discusses measures taken to mitigate privacy risks and protect personally identifiable information (PII) during DHS's use of C-UAS technologies during testing, evaluation, and operational deployment.

Introduction

On August 29, 2018, Federal Aviation Administration (FAA) rules regarding the use of small UAS (sUAS) took effect, opening up the National Airspace System (NAS) to certified sUAS flown by certificated operators. The FAA projects as many as 1.39 million sUAS may be in use in the United States for commercial and professional purposes (e.g., package delivery, medical prescription delivery, crop dusting, pipeline examinations) by 2023,[1] with over 1 million already in use today. sUAS are primarily used for commercial and professional purposes but may also be a source of deliberate or inadvertent threats to the Department's facilities, assets, or missions.

Criminal entities and terrorist organizations continue to promote or use UAS for illicit and illegal activity to support surveillance, smuggling, unauthorized access to protected information, harassment, and use as a weapon. With recent incidents and the rapid evolution of technology, the UAS threat from nefarious and non-nefarious actors to critical infrastructure and airports will likely increase in the near to midterm (out to five years) as the number of UAS in the national airspace continues to increase.[2]

In December 2018, for example, London's Gatwick Airport (LGW) cancelled or diverted approximately 1,000 flights affecting over 140,000 passengers due to repeated intrusions by UAS. During a 36-hour timeframe, observers reported 115 sightings of one or more UAS in the airspace over LGW, noting that the UAS flew unpredictably at an altitude as high as 1,000 feet, hovered near the air traffic control tower, and had an irregularly flashing light. When officials tried to resume service, a UAS reappeared, suggesting the operator was closely monitoring airport activity. Similarly, in January 2019, traffic at Newark Liberty International Airport in New York was halted for 90 minutes after a drone was spotted.

---

[1] *See* Federal Aviation Administration, FAA Aerospace Forecasts, FY 2020-2040 forecast, Unmanned Aircraft Systems, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/unmanned_aircraft_systems.pdf (last updated April 24, 2020).

[2] *See* DHS's Cybersecurity and Infrastructure Security Agency (CISA), Unmanned Aircraft Systems (UAS) – Critical Infrastructure, https://www.cisa.gov/uas-critical-infrastructure (last updated November 27, 2019).

In light of these threats, Congress passed the Preventing Emerging Threats Act of 2018,[3] explicitly granting DHS the authority to counter threats from unmanned aircraft systems (UAS) in the NAS. Specifically, the Act grants DHS the authority to conduct C-UAS activities in the United States (i.e., detect, identify, monitor, and track; warn the operator; disrupt control of UAS; seize or exercise control of UAS; seize or otherwise confiscate UAS; and use reasonable force, if necessary, to disable, damage, or destroy UAS) to protect covered facilities or assets, subject to the terms and requirements of the Act.[4] The Act also includes certain privacy, civil rights, and civil liberties protections, which DHS always applies to its activities.[5] The legislation defines "covered facilities or assets"[6] as:

- Located in the United States, including territories and possession, territorial seas, and navigable waters;
- Designated by the Secretary of Homeland Security, in coordination with the Department of Transportation (DOT), as high-risk and a potential target for unlawful UAS activity through a risk-based assessment; and
- Directly related to one or more following authorized missions:
    - U.S. Customs and Border Protection (CBP) security and protection operations;
    - U.S. Coast Guard (USCG) security and protection operations;
    - U.S. Secret Service (USSS) protection operations;
    - Federal Protective Services (FPS) protection of government facilities;
    - Protection of National Special Security Event (NSSE) and Special Event Assessment Rating (SEAR) events;
    - Support to state, local, territorial, or tribal law enforcement at the request of the Chief Executive of the entity to ensure protection at mass gatherings; or
    - Protection of active federal law enforcement investigations, emergency responses, and security operations.

In addition, other DHS Components may perform C-UAS operations to the extent such activities are authorized by law, statute, and policy, and outlined in the appendices of this PIA.

[3] Federal Aviation Administration Reauthorization Act of 2018, Division H, Preventing Emerging Threats, Pub. L. No. 115-24, 132 Stat. 3186 (codified as amended in scattered sections of U.S.C.), *available at* https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf.
[4] 6 U.S.C. § 124n(b)(1).
[5] *Id*. § 124n(e).
[6] *Id*. § 124n(k)(3).

Research, development, training, testing, and evaluation of C-UAS[7]

The Preventing Emerging Threats Act also prescribed that the Secretary conduct research, testing, training, and evaluation of any C-UAS equipment or technologies to determine their capability and utility.[8] To this end, the DHS Science and Technology Directorate (S&T) is leading efforts across the enterprise to gather and document technical and operational requirements from DHS Components as well as test and evaluate C-UAS technologies with the goal of determining system performance and applicability to various missions. Testing and evaluation results will inform future policies, processes, and acquisition plans for operationalizing C-UAS activities at the Department. Technical and operational requirements will guide system applicability and DHS Component acquisition.

S&T's role will generally be to test and evaluate systems to determine applicability for the missions specified by Components, effectiveness of each C-UAS function for the given mission, the potential for integration, and interoperability with other Departmental capabilities. Further, S&T coordinates those results with DOT and FAA to ensure there is no adverse impact on the NAS. S&T may also execute limited duration tests in cooperation with Components to further test, assess, and quantify C-UAS performance. Establishing these tests may include purchasing, installing, and integrating C-UAS equipment and training Component personnel assigned to support the C-UAS activities. Purchasing small quantities of C-UAS equipment is part of S&T's larger effort to assist DHS in understanding and documenting the requirements, test and evaluation, acquisition, and implementation process to use C-UAS in an operational environment. To do so, S&T will document the process and associated requirements to perform C-UAS missions at designated covered facilities or assets. S&T will also work with technology providers (and vendors) to ensure Component personnel have the training necessary to operate C-UAS in a safe and secure manner. S&T will work with these technology providers to ensure that the use of C-UAS technology does not interfere with other technologies operating in the designated area of operations.[9]

Research, development, training, testing, and evaluation (RDTT&E) of C-UAS systems will occur at test and evaluation sites, such as national laboratories, government-owned and

[7] DHS Components have previously conducted their own individual PIAs for C-UAS activities. For example, see DHS/S&T/PIA-034 Counter Unmanned Aircraft Systems Program and DHS/USCG/PIA-030 U.S. Coast Guard Counter-Unmanned Aircraft Systems Pilot, *available at* https://www.dhs.gov/privacy-impact-assessments. Those PIAs may still remain in place, but this PIA provides more wholistic guidance and coverage for DHS C-UAS activities.

[8] 6 U.S.C. § 124n(b)(3).

[9] S&T may test Radio Frequency (RF) detection equipment in an anechoic chamber, outside on a controlled test range, or through other means to ensure the technologies operate as specified by the manufacturers. However, because of the nature of the technology, there may still be instances where DHS is not able to ensure they do not cause interference. For those systems that S&T chooses to use and that may interfere with other technology, S&T has completed mitigation efforts with its Component partners if use should occur.

operated test ranges, other DHS-developed test sites, Component areas of responsibility, DHS facilities, or other covered assets.[10] RDTT&E activities for C-UAS systems may use Radio Frequency (RF) detection,[11] RADAR imagery,[12] perimeter alert systems,[13] acoustic sensors,[14] and Electro-Optical/Infrared (EO/IR) cameras,[15] or systems combining these technologies to scan for and correlate detected and/or observed flying objects to accurately determine the probability that the object is a UAS, rather than a non-threatening object such as flying debris or birds. These technologies are not meant to collect PII. Any video equipment is generally (but not always) pointed skyward; however, there is a remote possibility the C-UAS sensors might inadvertently capture images containing PII while monitoring the airspace or as a camera moves to follow a UAS that constitutes a potential threat. Similarly, there is a very remote possibility that acoustic sensors may inadvertently collect or sense human audio, such as an outdoor conversation. Operational use of RF technology may enable access to digital PII, such as the FAA registration number and a UAS's unique identification number, but reading, accessing, or retaining that information is not the intent of testing and evaluation activities. Any PII that may be inadvertently captured by C-UAS equipment will not be recorded, retained, or otherwise used by S&T, but such information may become part of a Component's law enforcement investigation; a Component's use and authority to collect and maintain such PII is described in further detail and outlined in the appendices of this PIA.[16]

Operational Use of C-UAS

DHS Components may employ a variety of techniques with the goal of detecting, identifying, monitoring, and tracking UAS (to include the aircraft and the ground controller) and mitigating the threat to covered facilities or assets. This includes warning the operator; disrupting control of a UAS; seizing or exercising control of a UAS; seizing or otherwise confiscating the UAS; or using reasonable force, if necessary, to disable, damage, or destroy the UAS. When time and circumstances permit, and if the operator of the UAS that has been identified as a potential threat can be determined, DHS personnel will attempt to approach the UAS operator directly to mitigate the threat. In the event that DHS personnel are unable to resolve the threat through

[10] The "Initial List of Recommended Priority Covered Assets and Facilities for C-UAS Protection (FY 2019/2020)" dated 8 July 2019 designates "Departmental Response (SEAR, Mass Gatherings, and Airports) Capabilities" as a covered asset, under the authorities granted by the Act.
[11] RF detection discerns electronic emissions on certain frequencies that are emitted by communication signals.
[12] Radar emits energy in the form of radio waves to determine the range, angle, or velocity of objects based on energy return. Some radar sensors are able to create a synthetic image of an object.
[13] Perimeter alert systems can include closed circuit TV surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, or geo-fencing to detect or deter threats.
[14] Acoustic sensors generally detect soundwaves in the air, but do not detect or collect the contents of those soundwaves.
[15] EO/IR cameras use light (electro-optical) or heat (infrared) to generate an image.
[16] Procedures for this situation will be discussed further in each Component's Appendix to this PIA.

personal contact, DHS personnel may use C-UAS technology to mitigate the threat by the means described above.[17]

Operational use of C-UAS systems will occur at select locations within designated public spaces, and in operational environments such as at the Southwest Border, DHS facilities, or other covered assets. DHS Components, in coordination with the Department's C-UAS Program Management Office (C-UAS PMO), develop site-specific C-UAS measures necessary to detect, identify, and mitigate credible UAS threats. When developing site-specific plans, Components will conduct additional coordination with federal, state, local, tribal, and territorial government partners to minimize disruption or degradation of vital communications capabilities or emergency response systems that may be caused by proposed site-specific C-UAS actions.

Operational use of C-UAS systems may use the same technologies as RDTT&E to scan for and correlate detected and/or observed flying objects to accurately determine the object. Again, these technologies are not meant to collect PII. Video equipment is generally (but not always) pointed skyward; however, there is a remote possibility the C-UAS sensors might inadvertently capture images containing PII. Similar to RDTT&E, RF technology may enable access to digital PII, such as the FAA registration number and a UAS's unique identification number. However, reading, accessing, or retaining that information is not needed to detect, track, identify, and mitigate UAS.

Although DHS does not anticipate that UAS detection and mitigation efforts will result in the capture of any PII, in those instances where an individual operates a UAS in a location or manner that may lead to a law enforcement response, DHS may obtain the individual's PII as part of that law enforcement response or in furtherance of the law enforcement investigation. Routine law enforcement investigative efforts might lead to the discovery of operator PII. This PII, however, would be collected through routine law enforcement activities covered by the Component's applicable PIA and SORN for the systems where the PII would be maintained.

As C-UAS technologies expand and new privacy risks arise, DHS Components will provide Appendices to this PIA, or this PIA will be updated to discuss the extent of the relevant risks and mitigation strategies.

[17] Any in-person interactions between DHS personnel and members of the public, and any PII acquired as a result of any interaction, for example the confiscation of a UAS, will be retained in the appropriate system of record and covered by that system or program's applicable PIA and SORN.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[18] 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.[19]

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.[20] 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[21] and the Homeland Security Act of 2002 Section 222.[22] This PIA examines the privacy impact of the use of C-UAS technologies across the Department 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.

DHS and its Components, generally in cooperation with S&T, continue to conduct testing and evaluation of C-UAS as the technologies become operationalized. These testing and evaluation activities were initially conducted on military, government, or privately-owned properties/testing ranges. However, as C-UAS capabilities have expanded, these activities have moved into public sites where they will eventually be operationalized. This PIA provides a measure of transparency, and any appendices will outline the testing and evaluation in public areas, as well as a discussion of a Component's operational posture of these technologies, as appropriate.

---

[18] 5 U.S.C. § 552a.
[19] 6 U.S.C. § 142(a)(2).
[20] *See* Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *available at* https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles.
[21] 44 U.S.C. § 3501 note.
[22] 6 U.S.C. § 142.

Privacy Risk: There is a risk that individuals will be unaware of C-UAS technologies in use and/or that their images or audio, belongings, or digital PII could be inadvertently captured as part of those C-UAS activities.

Mitigation: This risk is partially mitigated. For RDTT&E activities in non-public areas, DHS can control access to sites and give notice via signage to any individuals in the testing area or electronically online. For testing and evaluation activities that occur in public areas, signs will, to the extent practicable, be posted throughout the testing area, but notice to all individuals may be impractical (e.g., notifying motorists on the street). Event and restriction notices may be disseminated to drone enthusiast clubs, on social media sites, and through press releases to local and national media. Additionally, Temporary Flight Restrictions (TFR) will be issued for testing areas and Notice to Airmen (NOTAM),[23] which provides the public with information regarding the existence of the TFR, will be published. Local authorities and Department communications may also be assigned to assist with providing notice and ensuring compliance with a TFR.

For operational C-UAS use, it may impede the ability of the Department to complete its mission to publicly disclose the exact use and location of these technologies. However, this PIA provides notice of the types of areas C-UAS capabilities will be employed (i.e., covered facilities and assets and other authorized mission areas).

Additionally, the C-UAS PMO, Office of Public Affairs (OPA), the Office of Partnership and Engagement (OPE), and Cybersecurity and Infrastructure Security Agency (CISA), in coordination with other DHS Components, lead DHS external outreach and education regarding DHS C-UAS operations.

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.

Informed consent is required for all persons actively participating in C-UAS testing and evaluation activities at non-public sites. Physical notice in the form of handouts and signage or electronic notice online may be provided notifying individuals that their images or audio and belongings may be captured. Alternative areas may also be established for persons who do not want their images or belongings inadvertently captured. In public setting testing, DHS will, when possible, erect access control measures and post signage to demarcate testing areas. To the extent practical, DHS will ensure that there are demarcated detour routes around any testing site to ensure no individual is required to enter the site.

[23] Federal Aviation Administration, Air Traffic, Air Traffic Plans and Publications, Notices to Airmen, https://www.faa.gov/air_traffic/publications/notices/ (last updated on June 18, 2020).

Operationally, C-UAS will generally be employed at DHS covered facilities and assets, which generally relate to federal property or DHS mission areas. Individuals who enter into or are near federal property where use of C-UAS is occurring do not have a reasonable expectation of privacy, and therefore, no consent is required.

Because DHS C-UAS activity is unlikely to collect PII, redress procedures specific to C-UAS may not be necessary. However, individuals may submit a Freedom of Information Act (FOIA) or Privacy Act request to access or correct information maintained by DHS. Individuals may submit requests to the DHS Privacy Office: Chief Privacy Officer/Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628.

Due to the nature of C-UAS activities and any information captured by C-UAS sensors not being recorded or retrieved by personal identifiers, it would be difficult for an individual to be linked to any imagery. In the event that C-UAS activity becomes linked to an individual subject of a law enforcement or other investigation, access procedures are described in the appropriate PIA and SORN for the Component conducting that investigation, as outlined in the appendices of this PIA.

Privacy Risk: There is a risk that DHS may collect information from members of the public who have not consented to this collection and have no opportunity to opt out or be afforded redress.

Mitigation: This risk is partially mitigated. To the extent practicable, DHS will post barricades or signage to control access to any test sites. Those members of the public who enter an area where C-UAS testing activity is occurring have given consent to having their images (of their person and/or belongings) or audio inadvertently captured by not observing the signs and altering their path. Other notifications may be available online through social media, other media sites, and NOTAMs. Even in such cases, DHS does not intend to collect any PII during testing. Operationally, the intent still is not to collect PII. The likelihood PII is collected may increase during operational use of C-UAS due to practical notice limitations. However, and alternatively, the likelihood PII is collected may actually decrease as DHS continues to develop and refine the capabilities of its C-UAS use and techniques.

Generally, C-UAS technologies do not record or retrieve information by personal identifiers. In the event that C-UAS activity becomes linked to an individual subject of a law enforcement or other investigation, redress procedures are described in the appropriate PIA and SORN for the Component conducting that investigation, as outlined in the appendices of this PIA. Due to the investigative nature of these encounters, the applicable SORN may assert 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.

In all cases, an individual may also seek access to his or her records by either filing a Privacy Act or FOIA request. Only U.S. citizens, lawful permanent residents, and covered persons from a covered country under the Judicial Redress Act (JRA) may file a Privacy Act request to seek access and redress to their records. Individuals not covered by the Privacy Act or JRA still may obtain access to records consistent with FOIA unless disclosure is prohibited by law or if the agency reasonably foresees that disclosure would harm an interest protected by an exemption. If an individual would like to file a Privacy Act or FOIA request to view his or her record, he or she may mail the request to the following address:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Privacy Office, Mail Stop 0655
Department of Homeland Security
2707 Martin Luther King, Jr. Avenue SE
Washington, DC 20528-065

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 Preventing Emerging Threats Act stipulates that the Secretary shall conduct research, testing, training on, and evaluation of any equipment, including any electronic equipment, to determine its capability and utility prior to its use for detecting, identifying, monitoring, or tracking unmanned aircraft systems or unmanned aircraft.[24] Specifically, the Act grants DHS the authority to conduct C-UAS activities in the United States (i.e., detect, identify, monitor, and track; warn the operator; disrupt control of UAS; seize or exercise control of UAS; seize or otherwise confiscate UAS; and use reasonable force, if necessary, to disable, damage, or destroy UAS) to protect covered facilities or assets.[25]

The Preventing Emerging Threats Act also provides that the Secretary ensure that the that the use of C-UAS technology is conducted in a manner consistent with the First (against chilling of protected expression or freedom of association) and Fourth Amendments (against unreasonable searches and seizures) to the Constitution of the United States.[26]

The purpose of testing and evaluation activities is to determine the effectiveness of the C-UAS technologies. UAS test flight data is captured by C-UAS components in order to identify UAS and differentiate them from other objects. Images of individuals or their belongings or sounds of human audio during testing activities may be inadvertently captured, but this information will only be used for testing and evaluation of C-UAS capabilities, not to identify any person or the person's belongings. Operationally, the purpose and use of C-UAS is to take protective measures

[24] 6 U.S.C. § 124n(b)(3).
[25] *Id.* § 124n(b)(1).
[26] *Id.* § 124n(e)(1).

that are necessary to mitigate a credible threat that a UAS poses to the safety or security of an authorized DHS mission and is further analyzed in the Component-specific appendices at the end of this PIA.

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).

Collection of PII is not intended during C-UAS activities. The purpose of testing and evaluation is to determine the effectiveness of C-UAS abilities to detect, identify, monitor, and, if needed, mitigate risks associated with UAS.[27] Testing and evaluation activities[28] generally collect the following data from C-UAS technologies:

- Telemetry information of the UAS (e.g., speed, direction, altitude);
- Radar data – detecting moving objects in the sky;
- Weather information (e.g., temperature, humidity, wind);
- Log files from the C-UAS technologies;
- Audio signals;
- Geo-location data (latitude and longitude) of the aircraft and the ground controller; and
- Videos and still photographs of UAS in-flight or being tracked, of facilities and sensors being used, of surrounding trees, human shapes, vehicles, and other artifacts, and of program participants carrying out program roles.

DHS will also collect C-UAS technical performance data to include:

- Number of UAS detections;
- Number of UAS identifications;
- Number of successful mitigations; and

[27] Data will not be collected by any UAS used as test targets during testing and will not be used or stored in the execution of test activities.

[28] In order to perform certain C-UAS tests, DHS must apply to the FAA for Certificates of Authorization (COA) and/or Flying Restricted Zone (FRZ) waivers to fly target UAS against C-UAS systems. A federal agency must initiate the waiver application and must include the Social Security Number (SSN) or U.S. Passport number of each test pilot so that FAA can verify that they are registered with a Part 107 Drone Operator license. S&T will not retain any information collected from these individuals as the information is strictly for the FAA to verify the pilot is licensed and registered. S&T will only retain the verification that the pilot is registered.

- Metadata associated with these performances.

Support to RDTT&E will also be provided by C-UAS vendors, who will collect high-level preliminary data from tests that includes analysis related to system performance metrics. A comprehensive data analysis will also be done to determine and verify that the system was operating as described by the vendor and as required by S&T guidelines. Processed data will be summarized in technical plots and tables and ultimately combined into a final report designed to answer performance questions. All raw data that does not contain PII (e.g., weather data, RF background noise) will also be provided as a separate data transfer with the report. Any raw data that contains PII will be disposed of in accordance with DHS S&T Records and Disposition schedules as approved by the National Archives and Records Administration prior to transfer.

The C-UAS testing and evaluation activities may inadvertently collect images of individuals (of their person and/or belongings), human audio, or their digital PII. However, DHS will not attempt to identify the individuals whose images or other PII have been collected during these testing activities. In the event of an accident or crime unintentionally captured during a testing session, DHS may be required to produce the data and assist first responders or law enforcement officers with identification.

Operationally, information may be collected to detect, identify, monitor, and track; warn the operator; disrupt control of UAS; seize or exercise control of UAS; seize or otherwise confiscate UAS; and use reasonable force, if necessary, to disable, damage, or destroy UAS. PII is generally not required to conduct these activities. However, in the event that C-UAS activity becomes linked to an individual subject of a law enforcement or other investigation, the information collected would be covered by the appropriate PIA and SORN for the Component conducting that investigation, as outlined in the appendices of this PIA.

DHS will follow records retention schedules for testing as documented in DHS/S&T/SORN-001 Research, Development, Test, and Evaluation Records,[29] which states test and evaluation records are deleted or destroyed "when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes… Oftentimes, PII collected during the project is retained for the duration of the project; at the conclusion of the project, PII is destroyed." Operational records are covered by the mission area of the Component conducting the C-UAS activity and retained in accordance with those requirements. Retention schedules for operational records are described in each Component's appendix.

Privacy Risk: There is a risk DHS will collect more information than necessary to fulfill its responsibilities under the Preventing Emerging Threats Act.

[29] DHS/S&T-001 Research, Development, Test, and Evaluation Records, 78 FR 3019 (January 15, 2013), *available at* https://www.dhs.gov/system-records-notices-sorns.

Mitigation: This risk is mitigated. It is not the purpose of C-UAS to collect PII. The capture of images identifying individuals or an individuals' belongings inadvertently is usually unlikely due to the angle and focus of the camera technologies being used. The EO/IR camera's optics are generally not the primary method of initial UAS detection; they are usually positioned to point directly up at the sky or out to the horizon and only once other systems have raised an alert. RF and RADAR technologies can detect and collect frequencies, FAA registration number, UAS identification number, and control protocols. However, any of this possible digital PII is not recorded or retained for testing and evaluation purposes. Operationally, this potential digital PII is not required to detect, track, identify, and mitigate UAS.

Although unlikely, it is possible that acoustic sensors may capture human audio such as a conversation. Any capture of such information is entirely incidental, and this information will not be used for testing and evaluation purposes. Operationally, this information would not be valuable as the intent is to mitigate threats from UAS.

All DHS Components work with their respective Privacy Offices to ensure C-UAS are operationally used and deployed in a manner to limit unnecessary PII collection and follow the guidance laid out in this PIA. Any specific or additional risks are addressed in the Component-specific appendices below.

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.

Inadvertently captured images of individuals or their belongings may be contained within data that is used by researchers for additional C-UAS testing and activities. In addition, RF equipment may incidentally collect some digital PII, such as the FAA registration number and a UAS's identification number. As the identities of the individuals are unknown for testing environments, they cannot be conveyed to other operators, researchers, DHS Components, agencies, or C-UAS vendors. Overall testing and evaluation data (e.g., number of UAS detections/ identifications, telemetry data, log files) may be shared with respective C-UAS vendors so they may enhance and improve their systems. Data containing inadvertently collected images may also be shared with other DHS Components for purposes of evaluating the C-UAS technology.

Operationally, DHS Components will follow their own mission area guidelines for how information is used. In the reporting or investigation of any C-UAS incident, Components will follow the requirements outlined in the PIA and SORN for the system/program used to store investigatory data.

Privacy Risk: There is a risk that data collected during C-UAS operations may be used for purposes outside the scope of the C-UAS mission area.

Mitigation: This risk is mitigated. Members of the C-UAS deployment teams are regularly trained on the proper handling of sensitive information, and, through close coordination with their respective Privacy Offices, are aware that any use or capturing of otherwise irrelevant images or PII is not permitted.

All DHS personnel are also required to undergo annual privacy and security training. S&T provides additional system training for authorized project personnel and Component partners prior to C-UAS testing and deployment. S&T will also brief individual observers from participating agencies prior to any interaction with the system or testing events. Furthermore, in order to participate in S&T-led RDTT&E activities, all non-government agency entities, such as vendors, are required to sign an agreement that outlines their roles and responsibilities, such as a Rules of Behavior and/or a Cooperative Research and Development Agreement.

DHS Components also coordinate with the C-UAS PMO to develop site-specific C-UAS actions and ensure alignment with the Department's mission.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Data collected to evaluate C-UAS must be accurate, relevant, timely, and complete. The data collected from test activities will include the assessment of various C-UAS sensors, including radar and perimeter alert systems, which do not collect PII. While RF detection equipment is capable of collecting PII, such as FAA registration number or a UAS's unique identification number, such information is not recorded or retained for testing and evaluation purposes. Similarly, EO/IR cameras might inadvertently capture images containing PII while monitoring the airspace or as a camera moves to follow a potential threat UAS. Any data containing inadvertently captured PII may be used for testing and evaluating C-UAS but not to determine the identities of any individual whose image or other PII is inadvertently captured. DHS will therefore not attempt to guarantee the accuracy of incidental PII that may be captured for these testing and evaluation activities.

Operationally, any information C-UAS capabilities collected as relevant to an investigation as outlined above would be stored in the system applicable to that Component's authorities and mission space. The data accuracy would be ensured through the other measures in place for that system, and as described in the appropriate PIA, as outlined in the appendices below.

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 C-UAS activities, data is transmitted to secured DHS equipment with the appropriate privacy and security controls built into these workstations. These controls can include user name and password protection and credential access requirements. Access is limited to only those with an authorized need-to-know. C-UAS program managers will also determine what additional security features need to be added to C-UAS technologies specific to their Component.

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

Mitigation: This risk is partially mitigated. Systems collecting C-UAS data will only connect to accredited, cyber-secure, government-owned IT systems and have a limited number of devices that can connect to the system. Access to these devices are controlled through property and administrative controls. The data only temporarily[30] resides on the C-UAS system's memory before it is transferred to Component databases that are operationally hardened in compliance with DHS cyber security guidelines.[31]

Privacy Risk: During some preliminary RDTT&E C-UAS activities, there is a risk of unauthorized loss or disclosure of PII when a C-UAS equipment vendor transfers data to S&T.

Mitigation: The risk is fully mitigated. For those preliminary RDTT&E activities, vendors provide daily data transfers to S&T of all data collected. S&T personnel continuously review all data for PII, ensure proper deletion of any PII in the data files, and consolidate storage of collected data in a central location, such as an encrypted, secured laptop computer under custody of DHS personnel. While the data files are generally not expected to contain PII, vendors will delete all EO/IR images from their equipment after transfer to S&T and no later than the end of the test activity. S&T personnel then process and analyze the data on accredited S&T systems.

[30] Information temporarily resides on the actual C-UAS system until the detect, track, identify, and possibly mitigate event is over and the event information is pushed to the Component's data repository. This occurs in a matter of minutes to hours depending on the event timeline.
[31] For more information, *see* DHS 4300A Sensitive Systems Handbook, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All DHS personnel are required to complete annual privacy awareness training. Access controls are in place to ensure only authorized users access DHS systems that contain C-UAS data and images. Additionally, Components should develop their own auditing and accountability measures specific to their program.

Conclusion

UAS may pose a credible threat to covered facilities, assets, and other missions authorized to the Department by law, either by accidentally entering a restricted location or when the operator is intentionally seeking to do harm. DHS C-UAS use is designed to mitigate these risks while also avoiding infringement of the privacy of the people of the United States. This includes during the testing of any equipment and the interception or acquisition of unmanned aircraft or systems, in accordance with the Preventing Emerging Threats Act.

Responsible Officials

Brent Cotton
Director, Counter-Unmanned Aircraft Systems Policy
Department of Homeland Security
(202) 642-0960

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: U.S. Customs and Border Protection

1. U.S. Border Patrol Technology Demonstrations

The mission of the U.S. Customs and Border Protection (CBP) is to secure the borders of the United States while facilitating lawful international trade and travel. CBP employs various technologies to enforce hundreds of U.S. laws and regulations at the border, including immigration and narcotics enforcement laws. In an effort to enforce these laws, the United States Border Patrol (USBP) is testing the effectiveness of C-UAS to combat the use of Unmanned Aircraft Systems (UAS) near USBP facilities and between the ports of entry. This testing will provide the USBP with an opportunity to train on the use of C-UAS in an operational environment. Due to technological advances and improved costs, Transnational Criminal Organizations (TCO) are increasingly using UAS to smuggle contraband into the United States. The ability for TCOs to use UAS to smuggle narcotics, contraband, and surveil law enforcement operations has empowered TCOs and made it easier for them to evade law enforcement.

The USBP technology demonstration serves three purposes: 1) to better inform the USBP of the threat of UAS along the border; 2) to gather information regarding USBP operational requirements, training methods, and other capability gaps; and 3) to identify what capabilities and material solutions the market can provide.

When time and circumstances permit, and if the operator of a UAS that has been identified as a potential threat can be determined, USBP agents will attempt to approach the UAS operator directly to discuss the threat before employing C-UAS mitigating technology. In the event that CBP personnel are unable to resolve the threat through personal contact, CBP personnel may use C-UAS technology to mitigate the threat by disrupting or disabling the UAS. C-UAS are not intended to capture PII; however, there is a remote possibility that C-UAS sensors might capture images containing PII while monitoring the airspace within the area of operations. If this situation occurs, no PII captured by C-UAS sensors will be stored or maintained. Any in-person interactions between CBP personnel and members of the public, for any reason, are outside the scope of this technology demonstration. Any PII acquired as a result of this interaction, for example the confiscation of a UAS or contraband or apprehension of a subject, will be retained in the appropriate system of record and covered by that system's PIA[32] and SORN.[33]

[32] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT; DHS/CBP/PIA-040 Seized Assets and Case Tracking System; DHS/CBP/PIA-021 TECS System: Platform; DHS/CBP/PIA-008 Border Searches of Electronic Devices; and DHS/CBP/PIA-053 USBP Digital Forensics Programs, *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[33] DHS/CBP-023 Border Patrol Enforcement Records, 81 FR 72601 (October 20, 2016); DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (December 19, 2008); and DHS/CBP-024 CBP Intelligence Records System, 82 FR 44198 (September 21, 2017), *available at* https://www.dhs.gov/system-records-notices-sorns.