Privacy Impact Assessment

for the

United States Secret Service Unmanned Aircraft Systems Program (UAS)

DHS Reference No. DHS/USSSPIA-028(a)

September 27, 2023

Homeland Security

Abstract

The Department of Homeland Security (DHS) U.S. Secret Service (Secret Service or USSS) employs Small Unmanned Aircraft Systems (sUAS) for surveillance and law enforcement purposes in support of its protective and investigative mission. sUAS identify threats, mitigate vulnerabilities, and create secure environments for protected people, places, and events and further support Agency investigations into crimes against U.S. financial systems committed by criminals around the world and in cyberspace. sUAS-platformed video technology assists the Agency with securing protective sites/interests and further allows surveillance for law enforcement investigations or tactical operations. The Secret Service is publishing this updated Privacy Impact Assessment (PIA) to provide notice of the Secret Service extending its use of sUAS for investigative purposes not addressed in the original Privacy Impact Assessment,[1] and to assess the privacy impacts of using this technology for that purpose.

Introduction

The Secret Service has two primary mandates: 1) providing physical protection of select individuals, places, and events, and 2) conducting criminal investigations. The Secret Service protective mission is achieved through identifying threats, mitigating vulnerabilities, and creating secure environments for protected people, places, and events. The USSS is further charged with ensuring the integrity of U.S. currency and protecting financial institutions from those seeking to defraud, damage, or disrupt United States financial systems.

Both mission sets, protective and investigative, rely on the use of surveillance personnel and systems to gather intelligence and evidence. Intelligence serves to identify protective threats, locate potential suspects during investigations, and gather information necessary to safely and successfully carry out search and arrest warrants on behalf of the Federal Government. The USSS sUAS Program was initiated so that the Secret Service does not have to rely exclusively on other federal, state, and local agencies to provide aerial observation functions in furtherance of these USSS activities.

Reason for the PIA Update

The Secret Service is updating its UAS Privacy Impact Assessment to clarify that its Technical Security Division Investigative Support Branch has determined that sUAS platforms used during investigations will greatly increase situational awareness and enhance officer safety when conducting surveillance operations and throughout the execution of search and arrest warrants. The Technical Security Division's use of this technology for investigative purposes will

[1] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. SECRET SERVICE, PRIVACY IMPACT ASSESSMENT FOR THE USSS UNMANNED AIRCRAFT SYSTEMS PROGRAM, DHS/USSS/PIA-028 (2020), *available at* https://www.dhs.gov/privacy-documents-us-secret-service.

optimize officer safety and reduce the risk of a surveillance team or search and arrest warrant team being discovered, because it allows investigators to maintain situational awareness while remaining on the periphery of established surveillance perimeters. This provides a safer environment for search and arrest warrant teams, as well as informants and undercover law enforcement personnel during covert operations. There is the possibility that video recordings of individuals and/or their surroundings captured by the sUAS could allow individuals to be identified. There is also the possibility that recordings could reveal additional activity requiring investigation, provide evidence to support criminal prosecutions, or identify potential suspects. Such additional evidence or information could be subsequently shared with law enforcement partners in furtherance of criminal investigations.

The use of sUAS renders target surveillance and visual information from a viewpoint not available through traditional surveillance tactics or with traditional video or photography equipment. sUAS can be effective in providing information to enable law enforcement personnel to assess a potentially hostile environment before any personnel approach the perimeter of a target location while not exposing potential law enforcement activity to the target. sUAS are also capable of providing overwatch - a wide, overall perspective of target locations not available through traditional non-aerial surveillance methods.

sUAS would also provide critical information such as the location of vehicles, people, potential evidence, possible suspect escape routes, obstacles to search and arrest warrant teams, or the presence of a sensitive group, such as children. sUAS operators minimize, to the greatest extent possible and practical, capturing video images of members of the public, those parties who are not potential suspects, or individuals who are otherwise not involved in the investigation. The use of sUAS technology will allow surveillance teams to confirm the location of the suspect(s) prior to executing an arrest warrant while minimizing exposure of bystanders and law enforcement personnel in non-permissive environments (e.g., rugged terrain, a rooftop, or an area where the presence of a person would compromise the investigation or operation).

Additionally, search and arrest warrant teams will have enhanced awareness because the sUAS platform allows investigators to maintain a "bird's eye view" of the designated location(s). The video feed from these platforms not only ensures investigators are aware of their surroundings at the scene, it also allows for offsite assets such as associated local police units to be aware of events in real time should their services be required during the operation. These feeds can be shared, monitored, and reviewed at the responsible USSS office should a critical incident occur, thus increasing awareness for decision makers and supporting entities (typically sworn/deputized USSS Task Force officers or other law enforcement personnel directly related to the operation).

The use of sUAS technology would allow the surveillance or search and arrest warrant team to determine the most efficient and safest deployment of assets in real time as events may evolve in an unpredictable manner. sUAS platforms would assist with preserving evidence,

mitigating the risk of subject escape and/or flight, and overall contribute to the successful prosecution of USSS cases.

It is anticipated that most sUAS flights for investigative missions will be conducted between 200 – 400 feet above ground level (AGL). Systems do not have audio capabilities. Absent exigent circumstances, all sUAS observations will take place within public navigable airspace and be physically non-intrusive, operating under 14 C.F.R. § 107 guidelines.

Cameras that are integrated or mounted on the sUAS are limited in digital zoom capability, and any recorded video or images are unlikely to be of sufficient quality to permit facial recognition or to determine characters (i.e., letters, numbers, and personally identifiable information (PII)) on documents that may be in view of the camera(s). Therefore, it is unlikely that personally identifiable information of this sort captured in these recordings can be corroborated. However, the possibility that some personal information may be of sufficient quality to permit analysis raises potential privacy risks and is addressed below.

Data that has a higher probability of being captured with the potential for verification includes vehicle license plate numbers, vehicle descriptions, locations/descriptions of relatively large objects, and physical descriptions of people (e.g., clothing, hair color) which can help investigators identify individuals when used in conjunction with data from other sources. The data collected is also tied to a specific location captured by the sUAS; therefore, the geolocation of individuals and recognizable objects is also collected.

Cameras on the sUAS will be equipped with digitally stabilized pan, tilt, zoom, electro optical (EO), infrared (IR), low light, and high-definition (HD) cameras. The electro optical/infrared cameras attached to the systems can provide daytime and nighttime visual video observation and take still images of buildings, vehicles, and people. While electro optical/infrared cameras are not identical in size and capabilities, they are similar in performance specifications. sUAS will pass encrypted live video feeds and control information through a microfilament wire running from the aircraft to the Ground Control Station (GCS) for tethered sUAS. Non-tethered sUAS will use secure cellular/radio frequency to transmit video feed encrypted from the aircraft to the Ground Control Station.

The program will ensure encrypted data from sUAS will be transmitted to a Video Management System (VMS) near the remote pilot in command (RPIC) which will, in turn, transfer video images to a secure server located at the James J. Rowley Training Center. End users can then view the video via virtual private network (VPN) utilizing two-factor authentication. Technical Security Division personnel that will deploy sUAS in support of an investigation will document the action in flight logs submitted to the USSS's Aviation Program in accordance with USSS policy. The Aviation Program maintains records of all flights and can provide statistical usage over time. In most cases, recordings generated under this program are expected to be considered

evidentiary recordings. sUAS recordings will be kept and maintained in the respective USSS office's vault, and/or with the respective case file. All investigative video recording data shall be maintained and stored in accordance with USSS and National Archives and Records Administration (NARA) guidelines. Additionally, data shall also be disclosed in accordance with the applicable System of Records Notice and, if applicable, the Federal Rules of Criminal Procedure or state evidentiary rules, through consultation with the prosecuting U.S. Attorney's Office or state/local prosecutor's office.

Current policy requires evidentiary recordings be cut off/destroyed at closure of the case or three years after the date of recording, whichever is longer. To the greatest extent possible, collection of information about individuals will be limited to those persons who are the subject of a criminal investigation or are suspected of being involved in criminal activity.

The sUAS remote pilot in command will be required to maintain visual line of sight of the aircraft to ensure safe maneuvering of the sUAS and to see and avoid other aircraft or obstacles. sUAS will only be operated by Secret Service authorized personnel that have been licensed to operate sUAS by the Federal Aviation Administration (FAA). Additionally, Secret Service personnel whose responsibility it is to manage, supervise, maintain, fly, or use sUAS systems will receive mandatory training on Secret Service/DHS policies, including privacy policies.

The program will further ensure sUAS operators minimize, to the greatest extent possible and practical, when capturing video images of members of the public, those parties who are not potential suspects or individuals who are otherwise not involved in the investigation in accordance with current policies and procedures in use with other Secret Service surveillance systems. Further, there is the possibility of other criminal acts being captured during recordings which subsequently shall be disseminated to other federal, state, or local law enforcement partners/agencies in furtherance of a criminal investigation or in the interest of public safety.

In addition, Secret Service Technical Security Division Investigative Support Branch will not provide notice of sUAS during investigative operations because notice could compromise the integrity of a law enforcement operation or investigation. sUAS use for the purpose of the Secret Service protective mission specified in the May 2020 Privacy Impact Assessment remains the same.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[2] 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

[2] 5 U.S.C. § 552a.

that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[3]

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.[4] The Fair Information Practice Principles 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[5] and the Homeland Security Act of 2002, Section 222.[6] This Privacy Impact Assessment examines the potential privacy impact of sUAS related to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to an 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.

This Privacy Impact Assessment provides general notice that USSS may operate sUAS as part of its law enforcement investigations and tactical operations. However, for specific law enforcement investigative operations, notice will not be provided due to the need to maintain mission integrity. sUAS operators for investigative purposes will make best efforts to concentrate on the area of operation and subject(s) of interest only.

USSS must operate sUAS consistent with all applicable requirements, including DHS Policy requirements, FAA Regulations, and Federal Management Regulations.[7] DHS requires that the Office of the Chief Readiness Support Officer provide an Aviation Program Certification, in writing. Additionally, USSS requires approval from the USSS Chief Information Security Officer (CISO) for all Aviation Program sUAS assets, which must meet and adhere to the requirements in DHS Policy Memorandum 119-08, OCIO Memorandum "Interim Policy Memorandum: Securing DHS Small Unmanned Aircraft Systems (sUAS), and DHS Small Unmanned Aircraft Systems (sUAS) Cybersecurity Guidance Version 3.0," September 16, 2021.

---

[3] 6 U.S.C. § 142(a)(2).
[4] U.S. DEPARTMENT OF HOMELAND SECURITY, 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 (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[5] 44 U.S.C. § 3501 note.
[6] 6 U.S.C. § 142.
[7] 41 CFR part 102-33.

Privacy Risk: There is a risk that individuals will not know that the Secret Service is collecting information through sUAS.

Mitigation: This risk is partially mitigated. This Privacy Impact Assessment and associated System of Records Notice provide a measure of notice to the public. Any video images associated with criminal investigative files are covered by the DHS/USSS-001 Criminal Investigation Information System of Records Notice. However, the Secret Service does not provide notice to individuals when collecting data in support of a criminal investigation.

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.

A traditional means of consent is not practical or possible for Secret Service to appropriately execute its law enforcement mission. The video and images captured from sUAS will be used primarily for investigative purposes to successfully execute search and arrest missions. Any images or video obtained related to criminal activity will become part of a law enforcement investigation and treated as evidence, in accordance with the DHS/USSS-001 Criminal Investigative Information System of Records Notice.

While individuals cannot participate in the initial collection of their information by sUAS, they may contest or seek redress through appropriate means. The DHS/USSS-001 Criminal Investigative Information System of Records Notice provides correction and redress procedures. However, certain records in this System of Records Notice may be exempt from access and redress provisions of the Privacy Act. For those who are eligible for redress, access requests should be directed to Communications Center, FOIA/PA Officer, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223, and will be considered on a case-by-case basis.

Should a criminal investigation result in prosecution, the individual will have the opportunity to access the information collected by sUAS, to the extent it is used in a criminal proceeding, and may be able to seek correction or redress through that criminal case.

Privacy Risk: There is a risk that individuals other than the subject(s) of an investigation (e.g., bystanders) will not have any involvement in the collection, use, dissemination, and maintenance of their images, because their images will be captured only due to their proximity to the location where the sUAS will be operated.

Mitigation: This risk is partially mitigated. Notice of potential image capture is provided through publication of this Privacy Impact Assessment update. Individuals within the operating area of sUAS during an executed search and arrest mission will not be given the opportunity to

consent to image collection because doing so may compromise investigative operations and interfere with the Secret Service's ability to carry out its mission. While sUAS will be used primarily for aerial views to promote safe operations—by providing investigators awareness of their surroundings as law enforcement events take place—it is possible that images captured will include individuals other than investigative subjects. The USSS does not expect the nature and quality of images taken while at altitude in flight will permit the use of facial recognition or the ability to discern letters, numbers, or personally identifiable information on documents that will be within the range of the camera(s). sUAS are likely to identify surrounding objects within viewing range such as vehicle descriptions, license plate numbers, locations and/or descriptions of relatively large objects. USSS seeks to use the least amount of information necessary to meet mission objectives and only that which is aligned solely for law enforcement purposes documented within this Privacy Impact Assessment. Accordingly, unless related to the investigative mission, incidentally collected information will not be used. Therefore, unless the information is linked to an apprehension or other investigative case file, video recordings containing content beyond the subject are retained for 30 days or less and offer no continued value in a law enforcement support context.

Privacy Risk: Due to the law enforcement nature of the information collected by sUAS and maintained in case file records, there is a risk that individuals will not be allowed access to recordings that involve themselves.

Mitigation: This risk is partially mitigated. Individual access 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 interests. 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, and to avoid detection of confidential informants and undercover law enforcement personnel. Access to records could interfere with further ongoing investigations and law enforcement activities.

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.

18 U.S.C. §§ 1029, 1030, and 3056 grant the USSS statutory authority to investigate and apprehend subjects involved in financial crimes. Use of sUAS aligns with USSS criminal law enforcement functions to support its law enforcement mission relative to investigating counterfeiting offenses, financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, and electronic funds transfer fraud. sUAS used for investigative purposes will capture high elevation surveillance of individuals

and/or objects as search and arrest warrants are executed and will be used for targeted surveillance to monitor the safety of confidential informant(s) and/or undercover law enforcement personnel. There is also the possibility that footage could reveal additional investigative activity and/or provide additional evidence to support criminal prosecution and identify potential suspects whose information may be shared with law enforcement partners in furtherance of a criminal investigation. =

The DHS/USSS-001 Criminal Investigation Information System of Records Notice applies to the investigative footage kept within a case file associated with an investigation until the file destruction date. Video footage will be archived under an investigative case file number with the respective USSS office.

The current NARA records retention schedule DAA-0087-2014-0001, Item 2, indicates that evidentiary recordings for investigative purposes will be cut off/destroyed at closure of the case or three years after the date of recording, whichever is longer. These recordings will be maintained in the respective USSS office's vault, and/or with the case file.

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 NARA.

USSS seeks to minimize the collection and retention of video, data, and still images to that which is necessary and relevant to carry out its investigative mission. Further, all video, data, and/or still images obtained via sUAS that do not pertain to an investigation will be stored on a secure server at a USSS facility for a period of one year. If there is no suspicion of criminal activity and the video, data, or images are unrelated to a current investigation, they will be automatically overwritten and destroyed at the end of the one-year period. All data and images retained from sUAS and maintained within Secret Service files shall be secured and protected from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction.

Current policy dictates evidentiary recordings will be cut off/destroyed at closure of the case or three years after the date of recording, whichever is longer. Video footage will be archived under an investigative case file number with the respective USSS office. No personal identifiers will be used to locate or retrieve sUAS surveillance footage. Upon case closure, relevant records for investigative purposes can be scheduled for disposal within the case management system. Records maintained outside of the system (e.g., on portable media) and associated with a corresponding case number will be manually disposed based on the disposition date of the case.

Privacy Risk: There is an over-collection risk associated with Secret Service operating sUAS in populated areas.

Mitigation: This risk is partially mitigated. Although the Secret Service will generally use sUAS to monitor targeted surveillance areas, they still may be used in populated areas resulting in incidental collection unrelated to the investigation or mission, if the operation is consistent with the requirements in the "Operation of Small Unmanned Aircraft Systems Over People" Final Rule.[8] This risk is partially mitigated because Secret Service shall retain only information linked to law enforcement operations. It is anticipated that most sUAS flights for investigative missions will be conducted between 200 - 400 feet above ground level whereby cameras that are integrated or mounted on sUAS are limited in optical zoom and infrared zoom, and any recorded video or images are unlikely to be of sufficient quality to permit facial recognition or to determine characters (i.e., letters, numbers, personally identifiable information).

Privacy Risk: There is a risk that recordings will be held beyond the appropriate retention period.

Mitigation: This risk is mitigated. Consistent with proposed draft Records Schedule DAA-0087-2021-0001, Item 1, sUAS evidentiary footage recordings used for investigative purposes will be managed and disposed according to the lifecycle of the corresponding case file (generally, 20 years for judicial cases, and 10 years for non-judicial cases). These recordings will be maintained in the respective USSS office's vault, and/or with the respective case file.

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.

sUAS investigative video footage will be used for airborne surveillance of individuals and/or objects as search and arrest warrants are executed, for example. Any investigative video will be archived under the appropriate investigative case file number and kept within the file until the destruction date. No external sharing will occur unless other criminal acts are captured during recordings, which subsequently shall be disseminated to federal, state, or local law enforcement partners/agencies in furtherance of a criminal investigation or in the interest of public safety. This sharing will be done in accordance with the appropriate System of Records Notice.

Privacy Risk: There is a risk that Secret Service may allow access to video feeds or recordings by individuals without a need-to-know.

[8] *See* 86 Fed. Reg. 4314.

Mitigation: This risk is partially mitigated. Individual access will be limited to specific sUAS's end users, who will only view video via virtual private network (VPN) utilizing two-factor authentication. In most cases, recordings generated under this program are expected to be considered evidentiary recordings. sUAS recordings are kept and maintained in the respective USSS office's vault and/or with the respective case file, and case file numbers are not associated with any personally identifiable information. Further, all Secret Service personnel are required to take annual privacy training and follow policy on the proper use and handling of data entrusted to them.

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.

sUAS will offer an overall "birds-eye view" that will provide high level surveillance to monitor the safety of confidential informant(s) and undercover law enforcement personnel involved in operations and when search and arrest warrants are executed. The sUAS will use an electro optical/infrared camera to capture events that occur during the operation and may capture an individual's physical characteristics but generally not an individual's facial features. sUAS have limited optical zoom and infrared zoom capabilities, and any recorded video or images are unlikely to be of sufficient quality to permit facial recognition. The electro optical/infrared cameras to be used will not be able to identify written personally identifiable information (letters, numbers, other data) on documents that may be in view of the camera(s). Therefore, it is unlikely that personally identifiable information of this sort, if captured in these recordings, can/will be corroborated. Likewise, any such collected PII unrelated to the investigative mission will not be accessed or analyzed.

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.

Video and data obtained through use of sUAS will be transmitted in real time via a closed system with restricted access, subject to access controls and an approval process requiring clearance by Field Support System and/or Field Deployed System administrators to ensure that only authorized users with a need-to-know have access to video feeds. sUAS will only be operated by Secret Service authorized personnel that have been licensed to operate sUAS by the FAA. Additionally, all USSS employees and contractors receive annual privacy training to ensure they understand how to handle and secure personally identifiable information. Recorded evidence will be maintained within a locked container, segregated from other property and/or equipment.

Further, there are technological and physical controls in place to ensure that there is only authorized access to the sUAS and the collected data/images.

Privacy Risk: There is a risk that individual images might be intercepted between the sUAS and the ground control station.

Mitigation: This risk is partially mitigated. Data transmitted from sUAS to a video management system will be encrypted. Further, this transfer occurs near the remote pilot in command, who will subsequently transfer video images to a secure server. sUAS end users can view video via a virtual private network (VPN) utilizing two-factor authentication. In most cases, recordings generated under this program are expected to be considered evidentiary recordings. sUAS recordings are kept and maintained in the respective USSS office's vault, and/or with the case file, and case files numbers are not associated with any personally identifiable information. Further, all Secret Service personnel are required to take annual privacy training and follow policy covering the proper use and handling of data entrusted to them.

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 USSS employees and contractors receive annual privacy and security training to ensure they understand how to handle and secure personally identifiable information. Furthermore, all USSS offices are subject to periodic internal compliance reviews conducted by the USSS Office of Professional Responsibility, Inspection Division. Meanwhile, the status of all FAA licensing and training is maintained by the USSS Aviation Program and the Office of Training. All USSS sUAS operators must be licensed by the FAA to operate sUAS and approved to operate sUAS by program leadership. To further ensure that only authorized personnel access collected data/images, all evidence will be securely stored in each office's evidence vault and access to live video will be controlled through multi-factor authentication that provides technological and physical controls over data retained.

Access to video content related to investigative support will follow the same guidelines and processes as access to any other investigative video ingested into Secret Service field support systems. Video footage is ingested and maintained on a secure server at a USSS facility and physical access to the server is limited through the presence of security personnel located within several controlled access points 24-hours a day. Field Support System and Field Deployed System Administrators have access due to their need for network maintenance and troubleshooting. Moreover, these network administrators allow server access only to those that possess a need-to-know. Video files on the server are further protected by security protocols with designated access confined to authorized Secret Service personnel.

The USSS requires its personnel to follow procedures to ensure that such evidence is not co-mingled with data from other investigations and employees must adhere to guideline procedures to maintain an adequate chain of custody if the information is used as evidence.

Contact Official

Christal Bramson
Privacy Officer
U.S. Secret Service
privacy@usss.dhs.gov

Responsible Official

Michael Eversole
Assistant Division Chief
U.S. Secret Service/Technical Security Division

Approval Signature

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

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717