Privacy Impact Assessment

for the

USSS Incident Driven Video Recording System (IDVRS)

DHS Reference No. DHS/USSS/PIA-031

July 21, 2023

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Secret Service (Secret Service or USSS) is deploying Incident Driven Video Recording System (IDVRS) technology that provides enhanced transparency during recorded interactions between officers, special agents, and the public. In conformity with the Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, and to ensure the smooth implementation of a full IDVRS program across the agency, the Secret Service proposes to develop and deploy IDVRS technology amongst its diverse workforce of Uniformed Division personnel, Special Agents, and Technical Law Enforcement personnel through a multi-year phased plan. IDVRS further allows personnel to safely perform their duties during encounters with the public, while also assisting in the collection of evidence for use in prosecutions. The Secret Service is publishing this Privacy Impact Assessment (PIA) to assess the privacy risks associated with operational use of incident driven recording technology used during law enforcement interactions with the public, while also outlining the Agency's intentions regarding footage retention and storage of information collected. This Privacy Impact Assessment discusses testing and evaluation, pending funding and future deployment, and will be updated prior to formal and final deployment.

Introduction

On May 25, 2022, President Biden signed an Executive Order establishing Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety[1] that identified implementing body worn cameras (BWC) as one of the variety of mechanisms in the fulfillment of new practices within law enforcement that will improve oversight and accountability to enhance policing practices and build community trust and legitimacy. Incident driven camera technology has been proven to be an effective tool for providing additional information regarding law enforcement encounters with members of the public, enhancing an agency's transparency and accountability.

Based on the outcomes of evaluations by other law enforcement agencies, the Secret Service could potentially experience the following benefits from using IDVRS technology:

- Reducing allegations and complaints, deterring frivolous complaints, and lowering the likelihood of use of force incidents.
- Affording insights into law enforcement encounters that have traditionally been

[1] *See* 87 Fed Reg. 32945 (May 21, 2022), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/.

unavailable.

- Supplementing evidence in criminal cases, increasing the likelihood of obtaining successful prosecution for those who have violated the law.
- Enhancing training capabilities through use of recorded footage as a learning tool.
- Improving law enforcement/civilian interactions by reducing hostilities between officers/agents and citizens.
- Strengthening officer/agent performance and accountability.
- Increasing officer/agent awareness and safety through increased accountability. Simplifying incident review by enabling the quick and immediate review of footage.

An operational IDVRS system incorporates three primary elements:

- Camera Hardware – including cameras, mounts, vehicle camera systems, and charging hardware.
- Digital Evidence Management System (DEMS) – This software allows for the storage, categorization, retention, and management of digital evidence (videos). IDVRS requires licenses for all personnel accessing the system to the vendor Digital Evidence Management System.
- Information Technology (IT) Infrastructure and Cloud Storage – The Secret Service's requirements include the information technology infrastructure needed to transport and store video on a FedRAMP High authorized cloud storage system.

If the Secret Service discloses IDVRS recorded data to an agency outside of DHS, prior to doing so, there shall be an established Memorandum of Understanding (MOU) between the Secret Service and the receiving agency stipulating within the Memorandum of Understanding that the receiving agency is required to use the IDVRS recording solely for the purposes for which the Secret Service disclosed the data and must return it to the Secret Service or destroy all information after review of the released materials is completed. Any data sharing of footage between components within DHS, other Federal Law Enforcement Agencies, and State or Local agencies, shall be requested in writing through appropriate channels.

Release of Body Worn Camera recordings external to DHS partners must be coordinated with the Secret Service Office of the Chief Counsel. Releases must also be coordinated with other impacted operational office(s), such as, DHS Headquarters offices, including, but not limited to DHS Office of the General Counsel (OGC), DHS Office for Civil Rights and Civil Liberties (CRCL), the DHS Privacy Office (PRIV), and for the release of recordings to members of the media, the DHS Office of Public Affairs (OPA), who will be notified prior to any external release of Body Worn Camera recordings.

USSS IDVRS Policy

On September 16, 2022, the Secret Service issued an agency wide policy governing the use of Body Worn Cameras by agency personnel.[2] Through this policy, the Secret Service authorizes the use of Body Worn Cameras to collect audio and video recordings of interactions between Secret Service personnel who are authorized to carry firearms and the public according to the requirements established in the policy. The policy applies to Secret Service personnel and task force officers assigned to Secret Service-led task forces who operate Body Worn Cameras or handle recorded data.

The Secret Service acknowledges that there may be situations in which Body Worn Camera operation is impractical and may be an impediment to public and officer/agent safety. Additionally, the Secret Service recognizes human performance limitations during particularly stressful, critical situations. However, absent extenuating circumstances that implicate public or officer/agent safety, Secret Service personnel are required to activate their Body Worn Camera in accordance with this policy. If the device is not activated, however, there may be options to record video off the device in the future. This Privacy Impact Assessment will be updated when the internal policies governing video recovery options for Body Worn Cameras that are not activated are complete.

Implementation of the Body Worn Camera policy, as well as the development and implementation of related internal operating procedures, is contingent on the availability of funding to acquire the requisite equipment and supporting information technology infrastructure, personnel to support equipment operations and maintenance, personnel who will review and redact captured video/audio recordings for Freedom of Information Act (FOIA) and other authorized release requests, the distribution of Body Worn Camera equipment to Secret Service personnel, and the completion of related training.

The USSS policy establishes many requirements, including:

- Body Worn Cameras will be used to record law enforcement encounters by Secret Service personnel who are authorized to carry firearms when they are performing the following law enforcement duties except as otherwise prohibited by the policy or when doing so may jeopardize the safety of Secret Service personnel, other law enforcement agency personnel, or the public:
    - Uniformed Division (UND) personnel who are authorized to carry firearms are required to wear a Body Worn Camera and activate it during law enforcement encounters when they are conducting patrol or are otherwise engaged with the public in response to emergency calls.

[2] *See* https://www.secretservice.gov/sites/default/files/reports/2022-10/dep-01.pdf.

  - All Secret Service personnel who are authorized to carry a firearm are required to wear and activate a Body Worn Camera during a pre-planned attempt to serve an arrest warrant or other pre-planned arrest, or during the execution of a search or seizure warrant or order.

- At the direction of the Special Agent in Charge (SAIC) or Deputy Chief, Secret Service personnel may wear and activate Body Worn Cameras in other situations beyond the scope of the requirements above, if such wearing and activation of Body Worn Cameras does not otherwise conflict with the exceptions and prohibitions defined in agency policy.
- When equipped with a Body Worn Camera, Secret Service personnel will activate their Body Worn Camera (i.e., record law enforcement encounters that fall within the scope of the policy at the start of an event or as soon as safely possible thereafter) and continue recording until involvement in an event has concluded.
- Secret Service personnel shall deactivate their Body Worn Cameras when their role in an event has concluded (e.g., they are leaving the scene of an encounter or have completed their interaction with the subject or subjects involved in an encounter).
- When conducting a pre-planned attempt to serve an arrest warrant or other pre-planned arrest, or during the execution of a search or seizure warrant or order, Secret Service personnel will deactivate their Body Worn Cameras when the scene is secured as determined by the Secret Service supervisor on the scene. Under the policy, the term "secured" means that the scene is safe and under law enforcement control.
- If Body Worn Camera-equipped Secret Service personnel fail or are otherwise unable to activate their camera, they may be required to provide a statement indicating the reason why they failed or were otherwise unable to activate their camera. This Privacy Impact Assessment will be updated when the applicable policies regarding unactive Body Worn Cameras is complete.
- Secret Service personnel will not activate their Body Worn Cameras in a hospital or medical facility unless they are engaged in a law enforcement encounter as defined in agency policy.
- Secret Service personnel will not activate their Body Worn Cameras in any location where there is a reasonable expectation of privacy (e.g., restroom, locker room, dressing room, break room), unless they are engaged in a law enforcement encounter as defined in the policy.
- Body Worn Cameras will not be used to record a particular person based solely on the person's race, color, religion, national origin, sex, age, disability, sexual orientation,

marital status, parental status, personal appearance, gender identity or expression, or political affiliation.

- Body Worn Cameras will not be used for the purpose of recording individuals who are engaged in activity protected by the First Amendment (e.g., people who are lawfully exercising their freedom of speech, press, association, assembly, religion, or the right to petition the government for redress of grievances), unless the situation has become violent, dangerous, or otherwise unlawful, as determined by the officers' training, experience, and discretion. This prohibition includes any conversations that Body Worn Camera-equipped personnel have with individuals engaged in activities protected by the First Amendment unless those conversations are clearly related to criminal activity.
- Body Worn Camera-recorded data may not be accessed, used, downloaded, printed, copied, emailed, posted, shared, reproduced, or otherwise distributed in any manner, unless for official use and in accordance with agency policy and directorate, division, branch, and/or office internal operating procedures.
- Unauthorized use or release of Body Worn Camera-recorded data may compromise ongoing criminal investigations and administrative proceedings or violate the privacy or civil rights of those recorded. Any unauthorized access, use, deletion, modification, or release of Body Worn Camera-recorded data, or other violations of records management or privacy laws or DHS or Secret Service policies may result in disciplinary action.

Subject to the exceptions set forth below, Secret Service personnel may not review their Body Worn Camera recordings or Body Worn Camera recordings of other Body Worn Camera-equipped personnel that have been shared with them prior to writing initial incident reports. After completing initial incident reports, Secret Service personnel may, but are not required to, review all available Body Worn Camera recordings provided that any amendments they make to their initial incident reports include a statement that the incident report has been amended after reviewing Body Worn Camera footage. Such amendments must specify what aspects of the incident report have changed after Body Worn Camera recordings were reviewed.

Deployment of IDVRS

Upon successful completion of testing and evaluation of the IDVRS equipment in a closed (training) environment, which includes finalizing all internal policies and procedures and updating this Privacy Impact Assessment, the Secret Service will deploy the equipment amongst the different directorates within the Agency to ensure operational inclusion of the IDVRS technology to meet the requirements of the Executive Order. IDVRS equipment shall be deployed at the scene of a law enforcement encounter, such as Officers patrolling areas around protective venues, police/citizen contacts throughout the District of Columbia, while making arrests, pre-planned

attempts to serve an arrest warrant or other pre-planned arrests, or during the execution of a search or seizure warrant or order.

Operational uses of IDVRS devices predominately include the use of Body Worn Cameras, and will include a limited number of in-vehicle video recording systems which will be focused on the Agency's fleet of Prisoner Transport Vehicles (internal and external cameras will be mounted in the transport vehicles). Any expansion of the in-vehicle camera systems will be published and updated in future Privacy Impact Assessments.

Recording Notice

Secret Service personnel must orally advise subjects during the law enforcement interaction that they are being recorded if doing so does not interfere with the planned, overt enforcement activity or otherwise risk the officer's or the public's safety. Otherwise, verbal notice will be provided as soon as practicable for the overt enforcement activity. Cameras will be positioned conspicuously on Secret Service personnel, such as outerwear or visibly worn on the chest, that allows the subject to ascertain that Secret Service personnel are using a camera.

IDVRS-equipped Secret Service personnel should advise other Secret Service personnel and other agency law enforcement personnel that they are being recorded if doing so will not interfere with the encounter or officer/agent safety. This will provide other law enforcement officers with situational awareness and allow them to include related information in any written report.

Further, individual requests for Body Worn Camera-recorded data are subject to all applicable laws, regulations, and DHS and Secret Service policies, including but not limited to the Freedom of Information Act, as amended, 5 U.S.C. § 552, and the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

Employee IDVRS Training

Secret Service directorates, divisions, branches, and/or offices will ensure that Secret Service personnel who operate IDVRS devices or handle recorded data are trained in the use of Body Worn Cameras, relevant IDVRS policies and procedures, and have completed all applicable refresher training prior to their authorization to use IDVRS devices or access recorded data. Training must include the following:

- Body Worn Camera operation, maintenance, and care.
- Correct handling, storage, use, and dissemination of Body Worn Camera recorded data.
- Privacy compliance and proper privacy and FOIA procedures for applying exemptions (i.e., redacting), sharing, and disclosing Body Worn Camera data.
- Required, judgmental, and non-permissible uses of Body Worn Cameras.

- Officer/agent and public safety considerations when wearing/operating Body Worn Cameras.
- Training on any significant changes to the laws, regulations, or policies governing the use of Body Worn Cameras.
- Civil rights and civil liberties considerations (in consultation with CRCL).

Recorded data captured using Body Worn Cameras in the training environment will be used only as a part of the student instructor feedback process. Only authorized Secret Service instructors will use the recorded data for feedback purposes.

IDVRS Equipment and Data Upload

Footage Capture and Sync Process

When equipped with a IDVRS device, Secret Service personnel will activate their Body Worn Camera (i.e., record law enforcement encounters that fall within the scope of the policy at the start of an event or as soon as safely possible thereafter) and continue recording until involvement in an event has concluded.

Secret Service personnel must deactivate their Body Worn Cameras when their role in an event has concluded or the situation no longer permits use of Body Worn Cameras (e.g., they are leaving the scene of an encounter or have completed their interaction with the subject or subjects involved in an encounter or activity protected by the First Amendment is no longer violent, dangerous, or otherwise unlawful). When conducting a pre-planned attempt to serve an arrest warrant or other pre-planned arrest, or during the execution of a search or seizure warrant or order, Secret Service personnel will deactivate their Body Worn Cameras when the scene is secured as determined by the Secret Service supervisor on the scene. For purposes of the IDVRS policy, the term "secured" means that the scene is safe and under law enforcement control, however; the Secret Service is still developing internal policies and procedures which will govern how appropriate Secret Service personnel determine when a scene is secured. This Privacy Impact Assessment will be updated when additional policies and procedures are finalized and prior to deployment of IDVRS.

The IDVRS camera device will be able to capture what the eye can see in a reduced light environment, possess battery life with an average Secret Service workday (8-12 hours), have sufficient encrypted storage capacity for extended situations, and have capability to force critical video uploads to the cloud-based storage via LTE cellular data if required. Future capabilities will include mobile upload docks/kits which will be connected to LTE cellular service to perform emergency in-the-field data transfers to preserve the recorded data.

Secret Service Body Worn Cameras will be configured with no less than a 30-second pre-event video recording buffer (i.e., the duration of time and scope of the Body Worn Camera footage

preserved prior to its activation). When IDVRS devices are activated, the preceding 30 seconds of video (no audio) will be captured and become part of the event recording. The audio recording on the device will begin at the time the Body Worn Camera is activated. This 30-second buffer period will constantly be overwritten until the camera device is activated by the user manually or the weapon holster sensor. The IDVRS camera device will not record when the camera is powered off.

A typical IDVRS device workflow for the Secret Service is as follows:

- At the beginning of the shift, the body worn camera device is powered "on."
- If the device is activated (via holster sensors, Taser powered on or manually turned on by the user), the 30-second buffer recording has been saved (no audio) and now video and audio are being recorded by the authorized user's encrypted device.
- At the conclusion of an encounter the device is manually deactivated by the user, the data recorded is saved on the encrypted device secure storage drive, and the user tags or labels the encounter via their government-issued cellular device for future retention or attachment to an ongoing case.
- At the conclusion of the user's assigned shift, the IDVRS device will be docked in the assigned operational branch or office, where the device will have a pre-determined time to upload the recorded data to the secure FedRAMP-certified Digital Evidence Management System cloud-based servers (secure end-to-end encryption data transfer) for additional tagging or labelling.
- While the recorded data files are being uploaded to the cloud, the Digital Evidence Management System confirms the integrity of the files. Once verified, the file will be wiped from the local device secure storage drive and only then reside in the secure cloud-based storage servers.
- While docked, the IDVRS devices will be checked by pre-set vendor determined settings to ensure the loaded firmware is performing as expected and the battery is operational within established performance parameters. Any issues with programing or batteries will be flagged by the vendor's system and a property management custodian will cycle the defective equipment out for service. Affected personnel will be assigned a new device.

The Evidence Management System

The vendor-based Digital Evidence Management System, Evidence.com, will allow for Secret Service personnel to directly upload their video/audio files; tag and label an event file, and allow for direct sharing of videos with appropriate law enforcement authorities, to include the U.S.

Attorney's Office and D.C. Courts, to be used in case development while maintaining the full chain of custody of the recorded data.

Within the Secret Service IDVRS program, data, including USSS employee Personally Identifiable Information (PII), will be stored as user account information in the Digital Evidence Management System software product, which will be housed on the vendor cloud. Additionally, if related to an incident or arrest by a member of the Secret Service, personally identifiable information of members of the public (citizens and non-citizens), other government employees, and contractors, will be collected, maintained, and used within the Digital Evidence Management System.

The system is designed to be used daily in the agency's protective and investigative duties, capturing video and audio from law enforcement encounters with the public, incidents, or planned police actions. The IDVRS system will capture video footage that will include faces and images of Secret Service personnel and the public, as well as audio. The IDVRS system may not be used to collect any data on sensitive or protected populations not involved in law enforcement encounters, incidents, or planned police actions.

USSS personnel, vendor representatives, and other USSS mission support staff will have access to the IDVRS system. Users will at a minimum utilize a Single Sign-On (SSO) capability in conjunction with PIV credential validation for dual authentication to access the system via agency active directory permissions and policies. Each system user is assigned a level of access based on their responsibilities within the system using principles of Role Based Access Control, which will limit their access to information in the Digital Evidence Management System on a need-to-know basis. The system will have the appropriate safeguards and audit trails in place to restrict access and viewing of recorded IDVRS data files.

The Digital Evidence Management System vendor will not have access to the saved video/audio files contained within the Digital Evidence Management System cloud-based servers unless the Secret Service grants access for system support purposes at the time of need. Safeguards will include logging who accesses a file, date, time, and location accessed, as well as an agency defined appropriate retention schedule enforced on saved data in the cloud.

The IDVRS system is not designed to disseminate any personally identifiable information or other sensitive information. It is a secure, FedRAMP-certified cloud-based system, used to retain relevant video files related to open/closed investigations, incidents and/or ongoing criminal cases. The Digital Evidence Management System will be accessed by the U.S Attorney's Office and Washington D.C. Metropolitan Police Department in prosecutions of active agency investigations.

USSS IDVRS Records Retention Schedule

Data is retrievable by date, time, user, and the specific camera that captured the data. An automated purge, followed by a manual audit, will ensure all data containing personally identifiable information is disposed of properly, as outlined in the approved National Archives and Records Administration (NARA) retention schedule published September 28, 2022 (Records Schedule Number: DAA-0087-2022-0001). The approved Records Retention policy issued by the National Archives and Records Administration is outlined below.

- The approved records retention schedule covers captured video and audio from law enforcement encounters with the public, incidents, or planned police actions by USSS personnel, using recording devices (including, but not limited to, body worn, mobile, and vehicle/vessel-mounted cameras) during their official duties. Each recording results in the creation of a media file. Media files may be determined to have evidentiary or non-evidentiary value.
- For use in approved retention schedule, "media" refers to audio, visual, or a combination of the two, recorded through analog or digital means. It can contain raw or uncompressed data, compressed data, excerpts of the data, and associated metadata. "Media" also refers to either clips or full-length recordings, without distinction.
- When a recording device fails to capture some or all of the audio or video of an incident due to malfunction, displacement of camera, or any other cause, any other related audio or video footage[3] that is captured regarding the incident shall be treated the same as body worn or vehicle camera audio or video footage under this approved retention schedule.

Upon determination that IDVRS footage is evidence (or has a high likelihood or potential to become evidence) in a criminal, civil, or administrative proceeding, the footage will be managed according to applicable rules of evidence until the conclusion of that proceeding and then dispositioned according to the relevant provisions of the retention schedule. However, any copies or portions thereof which are included in a case file will be dispositioned according to the corresponding retention schedule for case files:

1. NON-EVIDENTIARY RECORDINGS THAT HAVE NO FURTHER BUSINESS USE

   Disposition Authority Number: DAA-0087-2022-0001-0001

   Media files/data recorded by law enforcement personnel during the performance of their duties that are not determined to have potential evidentiary or exculpatory value and which are not otherwise required to meet legal obligations, nor to initiate, sustain, evaluate, or provide documentation of agency actions will be purged from the Digital Evidence Management System within 90 days from the date of recording.

[3] For example, this could include video captured from stationary Secret Service cameras in the vicinity of the incident or recorded radio traffic that includes audio of the events happening in the background.

2. RECORDINGS VOLUNTARILY REQUESTED FOR LONGER RETENTION

Disposition Authority Number: DAA-0087-2022-0001-0002

Within 90 days of creation, certain members of the public may request that media files/data be retained for extended retention. The requester must be: a) any member of the public who is a subject of the video footage; b) any parent or legal guardian of a minor who is a subject of the video footage; and/or c) a deceased subject's spouse, next of kin, or legally authorized designee. If such a request is made, the media/data files will be destroyed three (3) years after the date the specific event or occurrence was first recorded.

3. RECORDINGS ASSERTED TO HAVE POTENTIAL EVIDENTIARY OR EXCULPATORY VALUE AND WHICH ARE REQUESTED FOR EXTENDED RETENTION

Disposition Authority Number: DAA-0087-2022-0001-0003

Media files/data asserted to have potential evidentiary or exculpatory value in an ongoing investigation, which are voluntarily requested for extended retention within the initial 90 days of their creation, by a) the Secret Service law enforcement personnel whose body camera recorded the video footage; b) any Secret Service law enforcement officer who is a subject of the video footage; and/or c) any superior officer of a Secret Service law enforcement officer whose body camera recorded the video footage or who is a subject of the video footage will be destroyed three (3) years after the date the specific event or occurrence was first recorded, or when use in agency mission/business operations ceases, or when the related case file(s) are closed, whichever is later.

4. RECORDINGS RELATED TO A USE OF FORCE

Disposition Authority Number: DAA-0087-2022-0001-0004

Any media files/data capturing an interaction or event involving a Secret Service law enforcement officer's use of force will be destroyed three (3) years after the date the specific event or occurrence was first recorded, or when use in agency mission/business operations ceases, or when the related case file(s) are closed, whichever is later.

5. RECORDINGS RELATED TO A COMPLAINT REGISTERED BY A SUBJECT OF THE VIDEO FOOTAGE

Disposition Authority Number: DAA-0087-2022-0001-0005

Any media files/data capturing an interaction or event about which a complaint has been registered, within the initial 90 days of its creation, by a subject of the video footage will be destroyed three (3) years after the date the specific event or occurrence was first recorded; or when use in agency mission/business operations ceases; or when the related case file(s) are closed, whichever is later.

6. RECORDINGS RELEVANT TO OTHER AUTHORIZED LAW ENFORCEMENT PURPOSES

Disposition Authority Number: DAA-0087-2022-0001-0006

Media files/data recorded by Secret Service law enforcement personnel during the performance of their duties requested and approved by a supervisor as needed for prescribed law enforcement purposes (e.g., after action analysis, training), and/or in support of any other authorized investigative inquiry not covered above will be destroyed three (3) years after the date the specific event or occurrence was first recorded; or when use in agency mission/business operations ceases; or when the related case/project file(s) are closed, whichever is later.

USSS IDVRS Evaluation

The Secret Service plans to conduct IDVRS testing and evaluation in a controlled environment, at the Agency's training center in Beltsville, Maryland, once funding is received to procure the necessary IDVRS equipment and support. The planned evaluation of the IDVRS program is tentatively scheduled to last three (3) to six (6) months, allowing for a full evaluation of the system and the IDVRS equipment. Testing and evaluation will be conducted in a controlled (training) environment at Secret Service Rowley Training Center, utilizing Secret Service personnel and contractors. Approved training scenarios will be utilized, allowing for testing the full capabilities of the IDVRS technology in all possible operating environments, while conducting investigations and/or protection related activities. The goal of this evaluation is to assess the effectiveness of the IDVRS program while operating in the Secret Service's daily operational environment, and develop the operational performance requirements. A successful evaluation will confirm that the technology works as intended including cloud storage and media/data age offs, training is effective, and all other privacy safeguards articulated in this privacy impact assessment function as described herein. To fulfill the Authority to Operate (ATO) requirement, IDVRS must require approval by the Component Acquisition Executive (CAE), functioning as the acquisition oversight authority.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[4] 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

[4] 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.[5]

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.[6] 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[7] and the Homeland Security Act of 2002, Section 222.[8] This Privacy Impact Assessment examines the privacy impact of the IDVRS program as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a System of Records Notice and Privacy Impact Assessment, as appropriate.

Per Secret Service policy, Body Worn Camera equipped personnel will advise individuals that they are being recorded if doing so will not interfere with the encounter or officer/agent/public safety. Otherwise, this notice must be given as soon as possible and practical. Body Worn Camera-equipped Secret Service personnel must advise other Secret Service personnel and other agency law enforcement personnel that they are being recorded if doing so will not interfere with the encounter or officer/agent/public safety. This will provide other law enforcement officers with situational awareness and allow them to include related information in any written report.

Privacy Risk: There is a risk that individuals may not receive adequate notice that their images and voice communications may be recorded when they are in close proximity to a Secret Service law enforcement encounter, regardless of whether they are directly or indirectly involved.

Mitigation: This risk is partially mitigated. There may be situations in which providing oral notice might compromise the safety of a scene or an individual, is impracticable, or may interfere with an ongoing investigation. There may be instances when Secret Service personnel will not be able to advise individuals located in and around an ongoing scene/incident that their facial image(s) or voice(s) might be captured on an IDVRS piece of equipment. To address this

[5] 6 U.S.C. § 142(a)(2).
[6] 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.
[7] 44 U.S.C. § 3501 note.
[8] 6 U.S.C. § 142.

possible gap, the Secret Service is publishing this Privacy Impact Assessment to provide general notice of its use of IDVRS.

Even though captured video and audio recordings from an IDVRS device clearly identify an individual's face or verbal communications, these recordings will not be linked to any personally identifiable information unless the individual is stopped, detained, arrested, or involved with a law enforcement action. In such instances, the associated personally identifiable information would be contained in an agency case file.

Further, Secret Service policy directs officers and agents to generally attempt to provide oral notice at the onset of a citizen/police encounter whenever possible. Per agency policy, IDVRS devices will be positioned or mounted in highly visible locations on the officers'/agents' bodies or USSS vehicles. Because of the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impracticable, impossible, or may jeopardize the safety of personnel on/in or around a scene. Therefore, the Secret Service is providing this Privacy Impact Assessment as notice to the public.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using personally identifiable information. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of personally identifiable information and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of personally identifiable information.

Secret Service law enforcement personnel will use the IDVRS program to record law enforcement activities involving members of the public. Due to the nature of the Secret Service's law enforcement mission, requiring individuals to consent to USSS's capture of their image or other information in a video recording is not always practical or feasible. Requiring the Secret Service to obtain an individual's consent prior to the collection, use, dissemination, and maintenance of the video and audio recording could potentially compromise the agency's law enforcement operations and prevent the Secret Service from obtaining and using evidence in ongoing investigations or prosecutions.

Most law enforcement interactions by the Secret Service are in public areas and may result in the capture of individuals in addition to those who are the focus of the law enforcement encounter. Once an IDVRS recording is associated with an established case file, the use and retention period of that recording is governed by the approved National Archives and Records Administration retention schedule as listed in this Privacy Impact Assessment.

Individuals who may have been recorded on an IDVRS device must follow the appropriate procedures for obtaining access to the possible recording. Due to the law enforcement nature of many of these recordings, they may be exempt from access under the Privacy Act and be withheld.

The Secret Service will review requests on a case-by-case basis and release information as appropriate in accordance with Secret Service policy and applicable laws. Individuals seeking notification of and access to any recording contained in an associated system of record, or seeking to contest its content, may submit a request in writing to:

U.S. Secret Service FOIA/PA Program
Attn: FOIA Officer
245 Murray Lane, SW, Building #T-5
Washington, D.C. 20223
or via email at: FOIA@usss.dhs.gov

Privacy Risk: There is a risk that members of the public may not be able to access or modify their records because of the law enforcement nature of the activities captured in the audio and visual recordings.

Mitigation: This risk is partially mitigated. While the Secret Service may be authorized to withhold records for which release may compromise ongoing law enforcement investigations and/or prosecutions, individuals may contact the Secret Service Privacy or FOIA Officers to request review, and the Secret Service will consider individual requests and determine whether information may be released. Individuals who believe more than one DHS component maintains Privacy Act records concerning them, may submit a request to:

Chief Privacy Officer and Chief FOIA Officer
Department of Homeland Security
245 Murray Drive, SW, Building 410, STOP–0655
Washington, D.C. 20528

Privacy Risk: There is a risk that members of the public may request access to footage captured by IDVRS, however may not access the relevant non-evidentiary footage prior to the 90-day deletion.

Mitigation: This risk is mitigated. The Secret Service developed a detailed retention schedule to ensure recordings are preserved for ongoing investigations, prosecutions, and agency case files balanced against the privacy interests of individuals who are not subject to investigations or protections. The Secret Service will retain footage in accordance with the approved National Archives and Records Administration retention schedule as listed in this Privacy Impact Assessment.

Privacy Risk: There is a privacy risk to individuals who are in the range of the recording device but not direct participants in interactions with the Secret Service and their images or voices may be captured without notice or opportunity to opt-out of the collection.

Mitigation: This risk is partially mitigated. Per Secret Service IDVRS policy, Officers/Agents should advise individuals that they are being recorded if it will not interfere with

the law enforcement encounter or safety of those at the scene. Any IDVRS recordings that are not associated with any listed event in the approved National Archives and Records Administration retention schedule will be deleted after 90 days. The Secret Service will process responsive records and apply any applicable FOIA exemption or exception to protect privacy of individuals captured in the video consistent with the law.

Privacy Risk: There is a risk that video footage requested by an external entity through FOIA or by another means may be difficult to retrieve if optimal data-tagging practices are not incorporated.

Mitigation: This risk is mitigated. Through other components, it has been determined that the selected IDVRS recording devices for use can adequately incorporate date, time, camera ID, and officer/agent name tags for video footage metadata. The Secret Service will also incorporate custom primary and secondary tags to assist with storage, search, and retrieval of retained records. These tags will allow for standardized retrieval of video footage contained in the IDVRS Digital Evidence Management System platform.

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 Secret Service will use the IDVRS program to collect audio and video recordings of interactions between Officers/Agents and the public under the conditions, and in accordance with, the procedures stipulated in the Secret Service Body Worn Camera policy. Specifically, Uniformed Division personnel who are authorized to carry firearms are required to wear a Body Worn Camera and activate it during law enforcement encounters when they are conducting patrol or are otherwise engaged with the public in response to emergency calls. Law enforcement encounters may include but are not limited to the following: use of force incidents; other law enforcement activities (e.g., during an arrest), in which a video recording would assist the investigation or prosecution of a crime or when a recording could assist in documenting the incident for further law enforcement purposes; and suspicious or possible illegal activity when observed by Body Worn Camera-equipped Secret Service personnel. Additionally, the Secret Service will use Body Worn Cameras to record pre-planned attempts to serve arrest warrants or other pre-planned arrests, and during the execution of search or seizure warrants or orders. The Secret Service will use IDVRS to record audio and video data in public areas, as well as in or near Secret Service facilities and/or protected locations consistent with the policy.

As stated previously, if IDVRS recorded data becomes associated with an individual's investigation or agency case file, then the data will be retained and governed by the associated National Archives and Records Administration retention schedule. Any video recordings not

attached to a specific classification as listed in the approved National Archives and Records Administration retention schedule, will be deleted after 90 days.

IDVRS recorded data may be disclosed to other federal, state, or local law enforcement agencies, in accordance with approved Secret Service policies and procedures and System of Records Notices,[9] as appropriate.

Privacy Risk: There is a risk that Secret Service Officers/Special Agents may record facial and video images outside the scope of a "law enforcement encounter" or use the captured images for purposes other than law enforcement purposes. Video cameras can capture individuals entering places or engaging in activities as they relate to their daily lives in populated areas. For example, IDVRS may collect video of an individual entering a doctor's office, attending public rallies, social events, or meetings, or associating with other individuals.

Mitigation: This risk is partially mitigated. The Secret Service mitigates this risk by limiting recordings to official law enforcement encounters that support the agency's integrated mission: protection and financial investigations to ensure the safety and security of our protectees, key locations, and events of national significance. These encounters may include but are not limited to use of force incidents, other law enforcement activities (e.g., during an arrest), in which a video recording would assist the investigation or prosecution of a crime or when a recording could assist in documenting the incident for further law enforcement purposes; and suspicious or possible illegal activity when observed by Body Worn Camera-equipped Secret Service personnel.

While an IDVRS device may record lawful activities, these recordings, to the extent they do not involve a law enforcement encounter, will be deleted after 90 days pursuant to the approved National Archives and Records Administration retention schedule. The Secret Service will copy and retain information from the IDVRS program to the approved Digital Evidence Management System only when it is relevant to an active case file for law enforcement investigations and/or prosecutions.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The Secret Service IDVRS program will be used to record official law enforcement activities/encounters by Secret Service officers, except when doing so may jeopardize officer/agent/public safety. The Secret Service acknowledges that there may be situations in which

[9] *See* DHS/USSS-001 Criminal Investigation Information, 85 Fed. Reg. 64523 (October 13, 2020); DHS/USSS-004 Protection Information, 85 Fed. Reg. 64519 (October 13, 2020).

operation of the IDVRS system is impracticable and may impede the safety of the public or officer/agent.

The Secret Service IDVRS Body Worn Camera policy states that officers/agents are required to record an event at the start of the incident/encounter, or as soon as practicable, and continue to record until the conclusion of the event.

Due to the expected use of IDVRS within the Secret Service to be enterprise wide, encompassing both officers and special agents, there is expected to be minimal, accidental recordings not associated with mission related activities, which will not become part of the Digital Evidence Management System record and will be deleted after the 90-day retention schedule from the time of the recording. Any recordings captured that have become associated with a respective retention tag will be retained in accordance with the approved National Archives and Records Administration retention schedule.

Privacy Risk: There is a risk of over-collection because IDVRS devices may capture images of individuals recorded in the proximity of an incident that are irrelevant to the interaction or encounter.

Mitigation: This risk is partially mitigated. The Secret Service will limit the IDVRS recordings to official law enforcement encounters that have occurred in support of the agency's integrated mission. While the IDVRS program will record lawful activities, any such recordings that are not associated with a Secret Service incident or case management file, will be deleted after the 90-day National Archives and Records Administration retention schedule. Deleting these types of IDVRS files will reduce the risk of retaining data that is unrelated to the agency's law enforcement mission.

The Secret Service will keep copies of IDVRS recordings and retain associated data only when it is relevant to an active investigation, prosecution, or case file. The recordings will be subject to the National Archives and Records Administration approved retention schedule.

As previously mentioned, per Secret Service IDVRS policy, Officers/Agents must advise individuals that they are being recorded if doing so will not interfere with the law enforcement encounter or impact the safety of those at the scene. Any IDVRS recordings that are not associated with any listed event in the approved National Archives and Records Administration retention schedule will be deleted after 90 days. The Secret Service will process responsive records and apply any applicable FOIA exemption or exception to protect privacy of individuals captured in the video consistent with the law.

Privacy Risk: There is a risk that the Secret Service may retain footage or personally identifiable information for longer than necessary to meet its law enforcement mission.

Mitigation: This risk is mitigated. The Secret Service automatically deletes recordings not associated with a mission-related event/encounter that has not been attached to an active investigation, prosecution, or case file, after 90-days as approved by the National Archives and Records Administration. Images and recordings associated with active case files, investigations, and/or prosecutions, will be maintained in accordance with the approved National Archives and Records Administration retention schedule.

Periodic reviews will be conducted by the agency to monitor the retention tagging of recorded audio and video files within the IDVRS Digital Evidence Management System, ensuring all proper schedules are being maintained.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

As stated previously, the Secret Service will use the IDVRS program to record official law enforcement encounters between officers/agents and members of the public, except when doing so may jeopardize the officer/agent or public safety.

The Secret Service may occasionally disclose IDVRS recorded data outside of DHS, to include other federal law enforcement, state law enforcement, or local agencies as allowed per established policies and procedures. All disclosures are consistent with the applicable disclosure provisions of the Privacy Act, if linked to a law enforcement file, and consistent with the original purpose for which the data was collected.

If the Secret Service discloses IDVRS recorded data outside of DHS, prior to doing so, there must be an established Memorandum of Understanding between the Secret Service and the receiving agency stipulating within the agreement that the receiving agency is required to use the IDVRS recording solely for the purposes for which the Secret Service disclosed the data and must return it to the Secret Service or destroy all information after review of the released materials is completed.

Privacy Risk: Due to the portable nature of IDVRS devices and their compactness, there is a risk that the cameras may be used in restricted private locations, such as locker rooms or restrooms.

Mitigation: This risk is mitigated. In accordance with Secret Service IDVRS Policy, USSS mitigates this risk by prohibiting the use of IDVRS devices for personal use and prohibits IDVRS recordings in places or areas where persons have a reasonable expectation of privacy, such as locker rooms, dressing rooms, and restrooms, unless related to official duties or incident response in those areas.

The Secret Service IDVRS Policy prohibits officers/agents from recording events that are not law enforcement encounters, including conversations of co-workers and management that are not part of an incident or event. IDVRS recordings will not be used for the sole purpose of conducting or supporting a personnel investigation, disciplinary action, or employee performance assessment unless such assessment is used in a IDVRS training environment in support of student-instructor feedback.

The Secret Service IDVRS policy prohibits IDVRS recordings to be used for recording individuals who are engaged in activity protected by the First Amendment (e.g., people who are lawfully exercising their freedom of speech, press, association, assembly, religion, or the right to petition the government for redress of grievances), unless the situation becomes violent, dangerous, or otherwise unlawful. This prohibition includes any conversations that IDVRS equipped personnel have with individuals engaged in activities protected by the First Amendment unless those conversations are clearly related to criminal activity.

Unauthorized use or release of IDVRS recorded data may compromise ongoing criminal investigations and administrative proceedings or violate the privacy or civil rights of those recorded. Any unauthorized access, use, deletion, modification, or release of IDVRS recorded data, or other violations of records management or privacy laws or Department of Homeland Security or Secret Service policies may result in disciplinary action.

Privacy Risk: There is a risk that recordings may be shared with third parties for purposes other than the purpose for which the recordings were made.

Mitigation: This risk is mitigated. Requests for IDVRS recorded data are subject to all applicable laws, regulations, and DHS and Secret Service policies, including but not limited to the Freedom of Information Act, as amended, 5 U.S.C. § 552, and the Privacy Act of 1974, as amended, 5 U.S.C. § 552a. These requests will be processed through appropriate offices (e.g., legal, privacy, FOIA).

Privacy Risk: There is a risk that recordings of "non-evidentiary value" may be shared with third parties.

Mitigation: This risk is mitigated. The Secret Service mitigates this risk by determining through the approved National Archives and Records Administration retention schedule how recordings will be filed, based on their relevance to a law enforcement encounter. All recorded data captured using a Secret Service Body Worn Camera is considered an official Secret Service record and, as such, must be handled consistent with National Archives and Records Administration approved records schedule DAA-0087-2022-0001 and applicable Secret Service Record Programs Management Manual policies when it is moved to storage.

When recorded data is placed in Digital Evidence Management System storage, it is maintained for an initial period of 90 days. By the end of this 90-day time period (or sooner, if its

attributes are readily apparent), each IDVRS data file must be labeled with the more relevant categories contained in the approved National Archives and Records Administration retention schedule. If a file is not attached to an ongoing event, investigation, prosecution, or case file, it will be deleted after the 90-day holding period.

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.

Once funded and deployed, the Secret Service IDVRS program will record in real-time to maintain an audio/video record of law enforcement encounters between Secret Service officers/agents and the public. The Secret Service will use the recorded data, in part, to verify what occurred during an encounter. Although the IDVRS devices are not generally involved in the collection of personally identifiable information, it is possible that personally identifiable information may be recorded in audio or video recordings while a law enforcement encounter occurs. Any personally identifiable information recorded on an IDVRS device would not be the sole source to identify potential subjects in an investigation or case. The IDVRS recordings would supplement existing processes in building a law enforcement investigation.

The Secret Service has outlined a standard for camera equipment and video recording devices based on market research and best practices. The minimum specifications for an IDVRS device included a wide array of requirements: field of view, video quality, recording capacity, battery life, recording time and storage limits, audio or visual indicators on a device, available docking stations, data upload options and battery charging times, environmental durability of the devices, activation of devices, mounting options, software capabilities, and video management solutions. Only technology that has been vetted through the pre-determined requirements will be used in the Secret Service IDVRS program.

The vendor-specific Digital Evidence Management System will automatically tag the time, date, and camera ID to standardize the metadata, assisting in retrieval of the recordings, while ensuring the availability of all files located in the Digital Evidence Management System. All recorded data captured using a Secret Service Body Worn Camera is considered an official Secret Service record and, as such, must be handled consistent with National Archives and Records Administration approved records schedule DAA-0087-2022-0001 and applicable Secret Service Record Programs Management Manual policies when it is moved to storage.

Privacy Risk: There is a risk that the Secret Service will identify and take enforcement action against an individual based solely on IDVRS footage.

Mitigation: This risk is mitigated. Secret Service officers/agents use a variety of techniques prior to taking enforcement action and may only use IDVRS recorded footage to

supplement and/or corroborate information obtained via other investigative techniques during the course of their law enforcement encounter. Such techniques include but are not limited to officer/agent reports; interviews of victims, subjects, and witnesses; and the collection and analysis of available evidence.

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.

In concept, the Secret Service IDVRS recordings will be uploaded by agency personnel at the end of each shift utilizing vendor supplied docking stations, using the FedRAMP-certified Digital Evidence Management System software and cloud-based storage to properly secure the recorded data. The docking stations will be connected via a Secret Service virtual network connection for device isolation.

Upon placement of the IDVRS device into the supplied docking station, it will immediately begin to synchronize recorded video data on the devices to the cloud-based Digital Evidence Management System. Once the video transfer/upload has been confirmed/validated by the server, the data on the IDVRS device will then be deleted from the memory of the IDVRS device.

The Digital Evidence Management System will be a FedRAMP-certified operating system, utilizing Single Sign-On enabled, cloud-based Software as a Service (SaaS) application which will store and manage all video and audio files uploaded to the servers from the deployed operational IDVRS devices/equipment.

Access to the IDVRS recordings in the cloud-based storage system will be controlled by agency security protocols as well as FedRAMP security protocols on the vendor-specific Digital Evidence Management System platform. The Secret Service also enhances security by adding layers of "customer provided" encryption keys where configurable in the Digital Evidence Management System platform, as well as configuring accounts to limit access and management of IDVRS recorded data based on a "need-to-know." IDVRS users will not be allowed to delete or modify any uploaded data in the Digital Evidence Management System cloud-based storage. IDVRS users will only be allowed to upload data, add case notes, place tags on recorded files, and save files into the proper investigation retention categories. Viewing, editing, deleting, exporting, and other permissions dealing with IDVRS metadata rests with the overall program administrator/manager.

Per Secret Service IDVRS Policy, officers/agents are prohibited from:

- Tampering with or dismantling an IDVRS device, its hardware, or software components;
- Using any other device to intentionally interfere with the capability of the IDVRS device;

- Unauthorized access, printing, copying, emailing, web-posting, sharing, or reproducing IDVRS recordings; or
- Deleting, modifying, or disposing of IDVRS recordings unless it is in accordance with Secret Service policies and procedures.

Privacy Risk: There is a risk of unauthorized access, use, disclosure, or removal of audio or video recordings.

Mitigation: This risk is partially mitigated. The Secret Service mitigates this risk by ensuring that audio/visual capabilities within IDVRS are successfully tested and evaluated during the authority to operate process. The testing and evaluation process includes establishing and developing role-based assess controls, preventing officers/agents from manipulating or deleting the IDVRS data directly from the device (camera), or prior to upload at the end of each officer/agent's shift. Though the testing and evaluation process has not begun, the Secret Service anticipates this risk being fully mitigated once testing is finalized. This Privacy Impact Assessment will be updated when the testing phase is complete and before IDVRS is deployed. Data will be securely transferred via "end to end" encryption, provided by the vendor approved DHS FedRAMP-compliant software/hardware. Secret Service supervisors also facilitate additional access to the chain of command that has a "need to view" the information in the performance of official duties.

IDVRS manufactured software is designed with security protocols in place to prevent manipulation or deletion of audio and video recordings. Once deployed, the Secret Service will further mitigate this risk by requiring two-factor authentication via Personal Identify Verification (PIV) cards issued to each officer/agent. The Secret Service also will employ additional layers of security, placing layers of protocols restricting access to and viewing recorded IDVRS data to only those personnel having a "need" to view. Additional safeguards include: automatically logging employee access to files, as well as the date, time, and location of access, ensuring that any file manipulation is captured in an audit log.

Prior to issuance of an IDVRS device to an officer/agent, the Secret Service will provide extensive training in the proper use of the IDVRS system. Training to the workforce includes correct procedures for operating the IDVRS devices (Cameras, Docking Stations), understanding and acknowledging protocols regarding of the use of the IDVRS system, demonstrating the proper uploading of recorded data on a IDVRS device, safeguarding equipment and recordings, and properly labelling recorded data to ensure the approved retention schedules are placed on the captured files.

Unauthorized use or release of Body Worn Camera recorded data may compromise ongoing criminal investigations and administrative proceedings and violates the privacy and/or civil rights of those recorded. Any unauthorized access, use, deletion, modification, and/or release

of Body Worn Camera recorded data, or other violations of records management and data privacy governed by federal, DHS, and/or Secret Service policies may result in disciplinary action.

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.

IDVRS recorded data will be secured in accordance with DHS system security requirements and standards. Secret Service network users must complete annual security and privacy awareness training and must have an active directory profile to access the system via their issued PIV card. Secret Service personnel will be properly trained on the use of the IDVRS system and all its components, as well as the correct procedures for handling recorded data prior to being granted IDVRS access.

Secret Service will utilize auditing procedures to ensure compliance with Secret Service policy and the standards established in this Privacy Impact Assessment. The Digital Evidence Management System will incorporate audit logs for all actions taken with respect to recorded IDVRS data from the moment recorded data is captured up until the point in time when it is deleted. Additionally, the Digital Evidence Management System will have established safeguards to restrict access to and viewing of IDVRS recorded data to only those personnel who have a need-to-know. Any attempt to view, delete, tag, download, or manipulate recorded data will be captured in the audit logs.

Secret Service will review IDVRS audit logs on a periodic basis, no less than quarterly, and more frequently as necessary. Audit logs will be reviewed for all recorded IDVRS data captured from use of force incidents. Misuse of any aspect of the IDVRS program may subject the user to disciplinary actions in accordance with Secret Service and DHS policy, as well as criminal and civil penalties. This auding capability will ensure officers/agents are using the IDVRS program for official law enforcement purposes and in compliance with all DHS and Secret Service policies and procedures. All IDVRS equipment will be accounted for pursuant to Secret Service policy.

The Secret Service has established written policies and procedures for viewing IDVRS recordings. All IDVRS recordings will be properly stored, categorized, and labelled, as outlined in the Secret Service policies and procedures. The approved National Archives and Records Administration retention schedule will be followed to ensure proper records keeping. Records maintained by the Secret Service may only be disclosed to authorized individuals with a work-related need for the information and only for the uses that are consistent with the intended purposes of the IDVRS program.

Contact Official

James McGill
Inspector
Uniformed Division, Office of the Chief
United States Secret Service
U.S. Department of Homeland Security

Responsible Official

Christal Bramson
Privacy Officer
United States Secret Service
U.S. Department of Homeland Security

Approval Signature

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

_____

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