Privacy Impact Assessment Update

for the

Incident-Driven Video Recording Systems (IDVRS)

DHS Reference No. DHS/CBP/PIA-052(a)

July 10, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is deploying Incident-Driven Video Recording Systems (IDVRS) to document law enforcement incidents and enhance transparency of its law enforcement operations. Following a successful IDVRS field evaluation in 2018, CBP is operationalizing IDVRS at select CBP locations. CBP is publishing this updated Privacy Impact Assessment (PIA) to evaluate the privacy risks associated with CBP's operational deployment of incident-driven video recording technology and changes to the tagging, retention, and storage of the information collected.

Overview

Following a feasibility study in 2014 and field evaluation in 2018, beginning in summer 2021, CBP will equip approximately 3,800 U.S. Border Patrol (USBP) Agents with body-worn cameras connected to a cloud-based digital evidence platform.[1] IDVRS will enhance transparency and accountability with the public, while providing additional documentation during enforcement incidents.

Incident-driven camera technology is an effective tool for providing additional information regarding law enforcement encounters with members of the public. For the field evaluation, CBP deployed IDVRS solutions from multiple commercially available vendors at select operational sites for approximately six months.[2] The evaluation was conducted in multiple land, air, and marine law enforcement operational environments, such as: (1) checkpoint operations, (2) outbound operations at ports of entry (POE), (3) primary inspection lanes at POEs, (4) airports, (5) seaports, (6) marine enforcement operations, and (7) aviation enforcement operations. CBP deployed two types of IDVRS during the evaluation:

- Body-worn cameras (BWC) mounted on the Officer/Agent's chest using manufacturer attachments; and
- Vehicle-mounted cameras (VMC) installed on the front of patrol cars stationed at USBP checkpoints and land ports of entry.

During the evaluation, authorized CBP Officers/Agents uploaded IDVRS data at the end of each shift to an approved, on-site data storage system on the CBP network with appropriate access

[1] For a full description of the privacy risks and mitigations surrounding the field evaluation, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE INCIDENT-DRIVEN VIDEO RECORDING SYSTEMS (IDVRS) EVALUATION, DHS/CBP/PIA-052 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[2] Specifically, CBP procured and evaluated several commercially available systems in order to support CBP's market research. The evaluation was not intended to determine CBP's final selection of camera systems but allowed CBP Officers/Agents to use various IDVRS to assist them in their day-to-day operations.

restrictions.[3] IDVRS recordings were tagged and retained on the IDVRS video management system (VMS) per the following:

- *Non-Evidentiary* – Any recorded data by a CBP Officer/Agent or Supervisor during the normal course of the performance of their duties determined to have no evidentiary value. Accidental recordings are considered Non-Evidentiary. Non-Evidentiary data is retained for 180 days and subsequently destroyed in accordance with the National Archives and Records Administration (NARA)-approved schedule DAA-0568-2015-0002.[4]
- *Evidentiary* – Any recorded data that may have material or probative value, or may have bearing on any criminal, administrative, civil, or other legal proceeding. CBP preserved files determined to have evidentiary value under established rules of evidence with the associated case file. Any IDVRS recording found to be evidentiary is associated with the respective case file and retained in accordance with the retention schedule for the respective CBP system of record.

CBP Officers/Agents were required to complete all necessary training requirements to participate in the evaluation. Training included demonstrating correct procedures for operating an IDVRS device according to manufacturer specified standards; understanding and acknowledging the CBP protocols regarding IDVRS usage; and demonstrating proper uploading, safeguarding, and labeling procedures for recorded IDVRS data.

Field Evaluation Results

CBP evaluated the operational benefits and impacts of the IDVRS with regard to transparency, safety, and evidence collection. The evaluation also examined the expected material and non-material requirements for implementation of the IDVRS program, including camera use and reliability, the existing CBP IT infrastructure, and training of CBP personnel. The evaluation provided insights into the operational environments best suited for deploying IDVRS. The IDVRS Evaluation resulted in the CBP Law Enforcement Safety & Compliance Directorate (LESC) recommending deploying IDVRS at known interdiction points where CBP Officers/Agents encounters with the public are most frequent and gaps in fixed camera surveillance technology have been identified.

[3] Pursuant to CBP Directive No.: 4320-030 Incident-Driven Video Recording Systems (IDVRS), IDVRS recorded data will only be accessed, downloaded, and disclosed by authorized CBP personnel. Any unauthorized access use or release of recorded data, or other violation of confidentiality laws or DHS and CBP policies may result in disciplinary action. Unauthorized use or release of IDVRS recorded data may compromise ongoing criminal investigations and administrative proceedings or violate the privacy and civil rights of those recorded.

[4] The current NARA-approved retention schedule requires CBP to retain recording tagged as Non-Evidentiary for 90 days. CBP is working with the CBP Records Information Management Division and NARA to extend the retention to 180 days in alignment with anticipated statutory requirements.

Additionally, results of the evaluation determined that operational use of IDVRS would increase transparency by providing recordings of CBP law enforcement encounters. These recordings would also increase the footage available for request under the Freedom of Information Act (FOIA). CBP determined that deployment of IDVRS would require upgrades to the existing CBP IT network infrastructure to support the collection and retention of the IDVRS recordings. Prior to implementation, CBP upgraded its existing IT network infrastructure to support the operational deployment of IDVRS.

Reason for the PIA Update

Following the IDVRS Evaluation from 2018, CBP is operationalizing IDVRS at designated CBP locations. CBP is publishing this updated PIA to evaluate the privacy risks associated with (1) CBP's operational deployment of incident-driven video recording technology; (2) creation of a new "Potentially Evidentiary" tag for stored video recordings and a corresponding shorter retention period; and (3) use of a third-party cloud-based storage solution for evidentiary video recordings.

1. Operational Deployment

Beginning in summer 2021, CBP will deploy IDVRS in a targeted, multi-phased approach to areas of operation where the U.S. Border Patrol lacks adequate fixed camera surveillance technology. Initially, CBP will deploy IDVRS at select USBP sectors, including immigration checkpoints.[5]

Operational use will include body worn cameras mounted on the USBP Agent's chest using manufacturer attachments. USBP will deploy body worn cameras only and will not deploy vehicle mounted cameras s at this time. CBP will publish an updated PIA before USBP deploys VMCs in an operational environment. USBP Agents will record IDVRS data in real-time to maintain an audio/video record of the law enforcement encounter. CBP uses this footage, in part, to verify what occurred during the encounter and support evidence gathering and report writing. CBP verifies that PII may be captured in the recording prior to entering it into a separate law enforcement or investigation record. The identity of potential subjects will not rely on IDVRS recordings solely, but may supplement a law enforcement case.

During Phase 1 (anticipated summer 2021), CBP will deploy IDVRS in the Del Rio, Big Bend, and El Paso USBP Sectors. During Phase 2 (anticipated fall 2021), CBP will deploy IDVRS in the Swanton, Yuma, El Centro, and San Diego USBP Sectors. During Phase 3 (anticipated late fall/winter 2021), CBP will deploy IDVRS in the Tucson and Rio Grande Valley USBP Sectors. CBP may adjust specific deployment locations and implementation timeframes as operationally

[5] At this time, the CBP Office of Field Operations (OFO) and Air and Marine Operations (AMO) do not plan to deploy IDVRS. CBP will publish an updated PIA prior to OFO or AMO operational use of IDVRS.

necessary.

To deploy IDVRS in an operational environment, CBP acquired additional hardware, to include cameras and camera accessories such as charging cords and docking stations. In addition to IDVRS equipment, CBP procured handheld throwable ball-like cameras. These types of cameras allow CBP Officers/Agents to get a view inside areas where it may not be safe for the Officer/Agent to enter. CBP is also testing the use of robotic hardware that CBP Officers/Agents can control to get video in places that it is not safe or feasible for Officers/Agents to enter.

The IDVRS program requires each IDVRS-equipped CBP Officer/Agent to have an IDVRS license to access the cloud-based VMS and be equipped with a BWC. The IDVRS license is a software license and will be assigned to each CBP Officer/Agent by their respective IDVRS Coordinator. IDVRS Coordinators are responsible for access control and the issuance of licenses. Each IDVRS license is role-based, subject to audits, and any misuse may lead to the CBP Officer/Agent's removal.

CBP will provide extensive training to Officers/Agents who will be wearing IDVRS, as well as those in leadership positions. Any unauthorized access, use, or release of recorded data or other violation of confidentiality laws or DHS, CBP,[6] and USBP policies, may result in disciplinary action.

2. Potentially Evidentiary Recordings

For CBP's operational deployment, CBP is adding a primary tagging/retention category and changing the default retention period. Other than those two changes, CBP will deploy IDVRS and collect recordings as outlined in the original 2018 PIA. At the end of a shift, or as soon as possible thereafter, the CBP Officer/Agent accessing VMS on a CBP computer workstation will upload the recordings from their assigned BWC. Once uploaded, the CBP Officer/Agent will manually apply a primary retention tag. Previously, the default tag applied to all recordings was the Non-Evidentiary tag which retained the record for 180 days. IDVRS recordings will no longer be assigned a code by default and will be retained until the CBP Officer/Agent applies a primary retention tag. Within 90 days of all recordings, an IDVRS Coordinator[7] will review the primary tag/retention category and may modify the primary tag/retention category if the IDVRS Coordinator determines the original tag to be inappropriate. IDVRS Coordinators will conduct reviews every 90 days to ensure videos maintain proper tagging.

Primary tagging/retention categories will now include Potentially Evidentiary. When applying a primary tag, the CBP Officer/Agent automatically applies one of the following retention

[6] *See* U.S. CUSTOMS AND BORDER PROTECTION STANDARDS OF CONDUCT, 51735-013B, December 9, 2020, *available at* https://www.cbp.gov/sites/default/files/assets/documents/2021-Jan/cbp-standards-conduct-2020_0.pdf.
[7] This would be a Supervisory USBP Agent for IDVRS-equipped USBP Agents.

periods:

- *Non-Evidentiary* – These recordings include any recorded data by a CBP Officer/Agent or Supervisor collected during the normal course of their duties that is determined to have no evidentiary value. Any accidental recording is considered Non-Evidentiary, as well. Audio and video recordings tagged as Non-Evidentiary are automatically deleted 180 days from the recording, per the NARA-approved retention schedule DAA-0568-2015-0002.
- *Potentially Evidentiary* ***[NEW]*** – These recordings consist of audio and video recordings tagged for their potential law enforcement significance during the course of routine surveillance/incident-driven events. Recordings tagged as Potentially Evidentiary will be retained until an approved records schedule is approved by NARA. CBP is working with CBP Records Information Management to update NARA records retention schedule DAA-0568-2015-000 to cover recordings tagged as potentially evidentiary. If approved, IDVRS recordings tagged as Potentially Evidentiary will be retained for three years.
- *Evidentiary* – These recordings include all recorded data that may have material or probative value, or may have bearing on any criminal, administrative, civil, or other legal proceeding. CBP preserves files determined to have evidentiary value under established rules of evidence with the associated case file. Any IDVRS recording found to be evidentiary is associated with the respective case file and retained in accordance with the retention schedule for the responsible CBP system of record. In no case will it be retained beyond 75 years.

Primary Tags and Retention Schedule

Based on the primary tags/retention categories described above, IDVRS intends to use the following retention schedules:

Table 1: IDVRS Primary Tag Retention Schedules

Primary Tag / Retention Category	Retention Schedule
Non-Evidentiary	180 days[8]
Potentially Evidentiary ***[NEW]***	3 years
Evidentiary	See Appendix A of the IDVRS PIA[9]

Secondary Tagging

In addition to primary tags / retention categories, CBP uses secondary tags as needed to

[8] *See supra* note 4.
[9] *See supra* note 6.

provide additional context to the IDVRS recording. In addition to assigning a primary tag/retention category, CBP Officers/Agents must also assign a secondary tag to all video files. CBP Officers/Agents may include as many secondary tags as necessary to provide context and aide in locating the recording.

As discussed in the original PIA, primary tags/retention categories map to the enforcement system of records notices (SORN) referenced in Appendix A of the 2018 PIA.[10] These SORNs control the retention period for the video recording. Secondary tags assist in locating the corresponding recording in the VMS system. In addition, whenever a case file related to IDVRS footage is created, IDVRS Coordinators will be responsible for assigning a case file tag to assist in cross-referencing the recording with the relevant case file. Case file tags will map to the SORNs for the associated case file management system. For example, if Non-Evidentiary IDVRS footage is requested under FOIA prior to its deletion at the end of the 180-day retention period, the IDVRS Coordinator will assign a FOIA tag to the footage. Assignment of the FOIA tag will allow the CBP FOIA Office personnel to access the footage and change the retention period from 180 days to six years, the required retention period for footage requested under FOIA.

Table 2: IDVRS Secondary Tag Retention Schedules

Primary Tag Retention Category	Examples of Secondary Tags	Retention Period
Evidentiary	Deadly Force Incident Fatality Less Lethal Force Incident Pursuit (Vehicle, Vessel, Foot) Prosecution Seizure	75 years
Possible Evidentiary	Vehicle Stop Suspicious Person or Activity Hostile/Possible Complaint	3 years
Non-Evidentiary	Casual Encounter Accidental Activation Training	180 days

3. Third Party Cloud-Based Storage Solution

The third-party cloud-based storage solution, Axon Enterprises Inc., is FedRAMP authorized. The CBP Office of Information and Technology (OIT) is responsible for the integrity of internal databases, encryption of the data in transit and at rest, user access to the environments, and the storage solution's instances within the CBP environment. Access to VMS will be granted to CBP Officers/Agents with BWCs, CBP Supervisors involved in IDVRS, personnel in the CBP FOIA office involved in the redaction and release of footage pursuant to FOIA requests, IDVRS

[10] *See supra* note 6.

Coordinators at CBP stations, and other personnel in the IDVRS Program Management Office with official need to access the system. The storage solution allows different levels of access depending on user type. CBP Officers/Agents will only have access to their own footage, while Supervisors, IDVRS Coordinators, and FOIA personnel will have access to a wider range of footage as necessary to complete duties as assigned. If applicable, video and audio PII will be redacted prior to releasing IDVRS recordings to a requestor.

CBP Officers/Agents are not able to delete or modify footage once it is uploaded to the VMS system. They will be able to apply tags to the footage, with IDVRS Supervisors conducting periodic audits to ensure that footage is properly identified. The VMS system also includes audit logs, which track all actions made in the system and use of the camera (e.g., volume increase/decrease). These audit logs allow CBP personnel to ensure VMS is being used in accordance with policy. Information will be stored in VMS with an identification number and relevant tag(s). As indicated above, the tags will impact the retention period for footage and CBP will audit to ensure that footage with evidentiary tags is transferred to the appropriate law enforcement case management system.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974,[11] as amended, articulates concepts of how the Federal Government should treat individuals and their information, and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). Section 222(2) of the Homeland Security Act,[12] states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected, and applicability to DHS's mission to preserve, protect, and secure the United States.

DHS conducts Privacy Impact Assessments (PIA) on both programs and information technology systems, pursuant to section 208 of the E-Government Act[13] and section 222 of the Homeland Security Act of 2002.[14] Given the technologies involved, and the scope and nature of their use, CBP is conducting this PIA, which examines the privacy impact of the use of IDVRS and the collection of recorded data, as it relates to the FIPPs.

[11] 5 U.S.C. § 552a.
[12] 6 U.S.C. § 101, et seq.
[13] Pub. L. 107-347; 44 U.S.C. § 3501 note.
[14] Pub. L. 107-296; 6 U.S.C. § 142.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

CBP will deploy operational IDVRS consistent with the IDVRS Directive,[15] which requires CBP Officers/Agents to attempt to verbally inform individuals at the beginning of the law enforcement-related encounter that they are being recorded. Accordingly, CBP Officers/Agents are required to position the cameras in obvious/visible locations. However, there may be situations in which providing verbal notice might compromise enforcement operations, is impractical, may interfere with the CBP Officer/Agent and/or a third party's safety, or may inhibit the U.S. Government's ability to enforce federal law and accomplish its border and national security mission. Some law enforcement encounters do not provide the opportunity for CBP Officers/Agents to notify individuals in close proximity to an incident that their facial image or voice will be/has been recorded.

There are no changes to the transparency or notice risks described and mitigated in the original PIA.[16]

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.

CBP law enforcement personnel will use IDVRS to record law enforcement activities involving members of the public. Due to CBP's law enforcement and national security missions, requiring individual consent to CBP's capture of their image or other information in a video recording is not always practical or feasible. Requiring CBP Officers/Agents to obtain an individual's consent prior to the collection, use, dissemination, and maintenance of the video and audio recordings could potentially compromise enforcement operations and prevent CBP from obtaining and utilizing vital evidence for use in prosecutions or investigations.

---

[15] CBP Directive 4320-030, *Incident-Driven Video Recording Systems (IDVRS)*, January 31, 2017, on file with the CBP Privacy and Diversity Office.

[16] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE INCIDENT-DRIVEN VIDEO RECORDING SYSTEMS (IDVRS) EVALUATION, DHS/CBP/PIA-052 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

The system of record notices[17] (s) provided in Appendix A of the original PIA[18] inform the public about the appropriate procedures to obtain access to and correct their record(s), if needed. Due to the law enforcement nature of many of these records, they may be exempt from access under the Privacy Act and be withheld. However, CBP will review requests on a case-by-case basis and release information as appropriate in accordance with the CBP IDVRS Directive and other applicable laws.

There are no changes to individual participation, such as consent or redress, from the original PIA.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which allows for the collection of PII and specifically articulate the purpose or purposes for which the PII is being collected and how it is intended to be used. The purpose specification principle requires DHS to 1) articulate the authority to collect and retain the PII in question; and 2) articulate how DHS will use the PII.

CBP is authorized to collect recorded data from audio and video recordings in support of its border security mission.[19] CBP authorizes the use of IDVRS to collect audio and video recordings of interactions between CBP Officers/Agents and the public under the conditions, and in accordance with the procedures stipulated in the IDVRS Directive. CBP is developing a new directive related to IDVRS. CBP Directive 4320-030A will supersede CBP Directive 4320-030.[20]

Among other purposes, CBP may use IDVRS to record use of force incidents; encounters with the public that are likely to become hostile, adversarial, or confrontational; and other

[17] *See* DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 Fed. Reg. 23361 (April 28, 2014); DHS/CBP-011 U.S. Customs and Border Protection TECS 73 Fed. Reg. 77778 (December 19, 2008); DHS/CBP-013 Seized Assets and Case Tracking System, 73 Fed. Reg. 77764 (December 19, 2008); and DHS/CBP-023 Border Patrol Enforcement Records (BPER), 81 Fed. Reg. 72601 (October 20, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns.

[18] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE INCIDENT-DRIVEN VIDEO RECORDING SYSTEMS (IDVRS) EVALUATION, DHS/CBP/PIA-052 (2018), *available at* https://www.dhs.gov/privacy-documents-us-customs-and-border-protection.

[19] Such authorities include, but are not limited to: 5 U.S.C. § 301; Homeland Security Act of 2002, Pub. L. 107-296; the Tariff Act of 1930, as amended; Title 7, 8, 19 United States Code.

[20] Despite the PIA and other policy updates, operational requirements for the IDVRS program have not changed substantially between the IDVRS Evaluation and in-field deployment. Changes to the Directive include minor changes to standard operating procedures surrounding failure to activate camera, recording encounters, providing additional guidance on labeling and safeguarding recorded footage, including redaction procedures. Additional definitions were included as well as the category Potentially Evidentiary. The updated Directive also addresses the procedure of rapid release of footage including requests from the Commissioner, releases to entities for criminal investigations, and release for cases involving national security risks.

enforcement activities when a recording of an encounter would assist in documenting the incident for law enforcement purposes.[21]

CBP will use IDVRS to record audio and video data in public areas, as well as in or near CBP facilities and ports of entry. CBP will use IDVRS to record official law enforcement encounters between authorized, on-duty, uniformed CBP Officers/Agents and members of the public, except when doing so may jeopardize officer or public safety, such as in extremis situations. Per the IDVRS Directive, Authorized personnel should record enforcement encounters at the start of the event, or as soon as safely possible thereafter.

Beginning in the summer 2021, CBP will deploy IDVRS in a targeted, multi-phased approach to select USBP Sectors where the USBP lacks adequate fixed camera surveillance technology.

CBP has also expanded the primary tags/retention categories and retention period for specific IDVRS recordings. When applying primary retention tags, the CBP Officer/Agent will tag the recording as Evidentiary, Potentially Evidentiary, or Non-Evidentiary. The CBP Officer/Agent will also apply a secondary tag to ensure that the recording is associated with the SORN for the relevant case file management system. Whenever an IDVRS recording becomes associated with a case file, the IDVRS Coordinator will assign a case file tag. The recording will be automatically retained for the retention period required by the applicable SORN.

The IDVRS Coordinator will assign the case file tag of FOIA to any IDVRS recording tagged as Non-Evidentiary and requested under FOIA prior to its deletion at the end of the 180-day retention period. Assignment of the FOIA tag will allow the CBP FOIA Office personnel to access the footage and change the retention period from 180 days to six years (i.e., the required retention period for footage requested under FOIA). The primary tag is viewable to the requestor. The IDVRS software retains all metadata and automatically creates an audit trail with timestamps/video frame regions recorded. The IDVRS software prohibits modification to the original recording. To redact the PII from the original recording, the user must create a copy of the recording and apply redactions to the copy.

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 NARA.

IDVRS recordings with a primary tag/retention category of Non-Evidentiary will be retained for 180 days pursuant to the NARA-approved retention schedule DAA-0568-2015-0002.

[21] IDVRS Directive, Section 8.3.

CBP is working to update NARA records retention schedule DAA-0568-2015-000 to cover recordings tagged as Potentially Evidentiary. If approved, these recordings will be retained for three years, instead of the two years previously reported. Any IDVRS recording found to be Evidentiary is associated with the respective case file and retained in accordance with the retention schedule for the responsible CBP law enforcement system of record (see Appendix A of the original PIA[22]). No recordings will be retained beyond 75 years. CBP follows the NARA-approved retention schedule to ensure the availability of Evidentiary recordings, while preventing the over-collection of Potentially Evidentiary and Non-Evidentiary footage.

During the operational phase, as with the evaluation, CBP acknowledges that there may be situations in which operation of the system is impractical and may be an impediment to public and officer safety. CBP also recognizes human performance limitations during particularly stressful, critical situations, and does not expect the recording devices to run constantly. As such, CBP seeks to limit IDVRS data collection and retention to recordings that are necessary and relevant to carry out CBP's mission and particularly for the purpose of assessing CBP's use of force incidents. CBP policy instructs Officers/Agents to record enforcement encounters at the start of the event, or as soon as safely possible thereafter, and continue recording until the encounter has concluded.

While presumably minimal, per the guidance above, accidental or extraneous recordings not associated with mission-related activity do not become part of a law enforcement record and are deleted after 180 days from the recording. Those images and recordings that become associated with case files would be retained for longer than 180 days based on the retention schedules applicable to the respective case files.

Privacy Risk: There is a risk of over-collection, since IDVRS may retain images of Non-Evidentiary value for longer than necessary while determining whether they should be stored as Evidentiary.

Mitigation: This risk is mitigated. IDVRS recordings with a primary tag/retention category of Non-Evidentiary will be retained for 180 days. If approved, IDVRS recordings with a primary tag/retention category of Potentially Evidentiary will be retained for three years, instead of the two years previously reported. Any IDVRS recording found to be Evidentiary is associated with the respective case file and retained in accordance with the retention schedule for the responsible CBP law enforcement system of record (see Appendix A of the original PIA). No IDVRS recording will be retained beyond 75 years. CBP follows the NARA-approved retention schedule to ensure the availability of Evidentiary recordings, while preventing the over-collection of Potentially Evidentiary and Non-Evidentiary footage.

Further, CBP is planning to conduct a CBP Privacy Evaluation (CPE) on the retention process and data tagging for retention purposes within IDVRS.

[22] *See supra* note 6.

5. Principle of Use Limitation

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

As noted above, CBP will use IDVRS to record official law enforcement encounters[23] between authorized, on-duty, uniformed CBP Officers/Agents[24] and members of the public, except when doing so may jeopardize officer or public safety. CBP may occasionally disclose IDVRS recorded data outside of DHS, including with local, state, tribal, and other federal law enforcement agencies and foreign governments. All disclosures are consistent with the applicable disclosure provisions of the Privacy Act if linked to a law enforcement record. If the IDVRS records unlawful activity, use of force, or officer/agent misconduct, it may be presented as evidence for an investigation or prosecution.

In cases in which CBP would disclose IDVRS recorded data to third-party agencies outside of DHS, the receiving agency is required to use the IDVRS recording only for the purpose for which CBP disclosed the data and must return the data to CBP or destroy all the information after analysis,[25] unless they have independent authority to retain the information. IDVRS recorded data disclosed to other federal, state, local, tribal, and international law enforcement agencies in order to assist in enforcement activities is done so in accordance with published Routine Uses in the applicable SORNs, and with approval from the CBP component and the concurrence of the CBP Privacy Office.

Once the CBP Privacy Office approves the disclosure, CBP documents the disclosure using DHS Form 191 Privacy Act Disclosure Record. CBP may also require its components to seek approval from various CBP stakeholder offices prior to releasing IDVRS recorded data to a third party.

There are no changes to the use limitation risks of IDVRS information as part of the CBP

[23] Enforcement encounters include, but are not limited to: (1) use of force incidents as defined in the CBP Use of Force Policy, Guidelines, and Procedures Handbook, HB 4500-01C, May 2014 (https://www.cbp.gov/document/guidance/final-use-force-policy-handbook); (2) encounters with the public that are likely to become hostile or confrontational; (3) other enforcement activities in which a CBP Officer/Agent believes a video recording would assist the investigation or prosecution of a crime, or when a recording of an encounter would assist in documenting the incident for further law enforcement purposes; and (4) observed suspicious or possible illegal activity.

[24] Authorized CBP Officers/Agents, supervisors, and personnel are persons who are trained and authorized by an Executive Assistant Commissioner, Assistant Commissioner, or equivalent to use IDVRS and manage recorded data.

[25] In cases where IDVRS recorded data is requested for purposes other than to support an investigation or prosecution, CBP provides an authorization memorandum outlining the approved uses of the data, how long it may be retained, and whether additional disclosure is authorized. These memoranda also include a requirement that the recipient of any data provide an attestation statement outlining how and when CBP-provided data was destroyed.

operationalization of this technology.

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.

CBP Officers/Agents are not able to manually delete, modify, or dispose of IDVRS recorded data. Additionally, the video management system tracks all actions taken regarding each piece of footage via an audit log; audit logs are retained indefinitely. CBP Officers/Agents will follow the existing chain of custody and evidence handling procedures for all captured IDVRS recordings and VMS will support the chain of custody requirements.

CBP has entered into an agreement with a third-party vendor to operationalize IDVRS across multiple CBP environments. All vendors must meet the CBP standard for camera equipment and video footage based on market research and best practices.[26] The minimum specification categories included a wide array of specifications: field of view, video, recording, power, battery, recording time and storage, audio or visual indicator, docking station, upload and charging, environmental durability, activation, mounting options, software capabilities, and video management solutions.

CBP's testing of body worn cameras found that the body worn cameras used by CBP provide better image quality than fixed cameras used at the majority of CBP facilities.

There are no changes to the data quality and integrity risks of IDVRS information as part of the CBP operationalization of this technology.

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.

CBP stores IDVRS recordings uploaded by CBP Officers/Agents at the end of each shift using secure storage methodologies (on a cloud-based digital evidence platform accessed through the DHS network) with appropriate role-based access controls within an access-restricted federal facility that meets DHS's physical security requirements pursuant to DHS Sensitive Systems Policy Directive 4300A.[27] Furthermore, the IDVRS security setting is a CBP/OIT-approved and validated operating system using DHS security requirements. Though video and audio files/data

[26] Request for Quote (RFQ) against a GSA Schedule on September 13, 2016; Body Worn Cameras and Vehicle Mounted Camera Systems Request for Information (RFI), April 7, 2016, *available at* https://www.fbo.gov/index?s=opportunity&mode=form&id=a77c3164ffee5a218b1973c8f6d953a4&tab=core&_cview=0.
[27] Available at https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

recorded during the evaluation were stored on physical servers at multiple test locations, the production environment of the deployed IDVRS program will utilize a FedRAMP-authorized, Single Sign On (SSO) enabled, cloud-based software as a service (SaaS) application to store and manage video and audio files/data. Local storage, in the same form it took during the IDVRS Evaluation, will be used as a backup solution to store IDVRS data in the case of network failure.

Access to the audio/video data on the IDVRS cloud application requires a user verification, consisting of IDVRS application-level security. IDVRS-application security is controlled by both the vendor software application and Operating System Level security setting. CBP enhances security by limiting initial access and management of IDVRS recorded data. Accordingly, IDVRS users will not be allowed to delete or modify any uploaded data. IDVRS users will have the ability to upload data, add case log notes, and save the respective files in the system. Viewing, editing, deleting, exporting, and other permissions related to video and metadata rests with the IDVRS application administrator.

CBP prohibits Officers/Agents from (1) tampering with or dismantling an IDVRS, its hardware, or software components; (2) using any other device to intentionally interfere with the capability of the IDVRS; (3) unauthorized access, printing, copying, e-mailing, web-posting, sharing, or reproducing IDVRS recordings; or (4) deleting, modifying, or disposing of IDVRS recordings unless it is in accordance with CBP policies and procedures. CBP takes precautions to prevent IDVRS recorded data alteration or deletion to maintain audio/video data integrity and to protect the recorded data. By policy, CBP prohibits IDVRS recorded data from being uploaded onto public servers or social media websites.

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

Mitigation: This risk is mitigated. CBP mitigates this risk by establishing and developing role-based access controls preventing CBP Officers/Agents from manipulating or deleting the data directly from the camera, or prior to upload at the end of the shift. Data will be securely transferred to secure cloud storage and managed in databases within third-party facilities that comply with DHS security requirements. The CBP Officer/Agent's Supervisor facilitates 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 protocols to prevent manipulation or deletion of audio and video recordings. CBP further mitigates this risk by requiring two-factor authentication via Personal Identify Verification (PIV) card to log into CBP computers. CBP also has appropriate safeguards and audit trails in place to restrict access and viewing of recorded data to those with an official need to know. Such safeguards include automatically logging employee access to a recording, as well as the date, time, and location of access, ensuring that file manipulation is captured in an audit log. Lastly, prior to the issuance of IDVRS, CBP Officers/Agents receive extensive training on the proper use of IDVRS. Training includes correct

procedures for operating IDVRS; understanding and acknowledging protocols regarding usage; and demonstrating proper uploading, safeguarding, and labeling procedures for IDVRS recorded data.

Any unauthorized access, use, release, or removal of recorded data or other violations of confidentiality laws and Department policies may result in disciplinary action and/or criminal or civil sanctions, as applicable. The CBP Office of Professional Responsibility (OPR) is responsible for investigating criminal and administrative allegations and use of force incidents associated with IDVRS users. In addition, every CBP employee has a duty to report any matters that could reflect substantive misconduct or serious mismanagement.

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.

CBP will conduct audits to ensure that all IDVRS recorded data adheres to CBP policy. These audits will ensure that CBP Officers/Agents are using IDVRS for official law enforcement purposes only and in compliance with all CBP policies and Standard Operating Procedures (SOP). CBP Officers/Agents will be properly trained on the use of IDVRS as well as the correct handling of recorded data prior to issuing or being granted access to the IDVRS. All IDVRS equipment shall be accounted for pursuant to CBP Personal Property Management Directives. CBP has established written procedures and designation of responsibilities for viewing IDVRS recordings. In addition, CBP will ensure that all IDVRS recordings are properly stored, categorized, and labeled.

CBP will ensure that any SOPs and technical guidance is updated to reflect changes to IDVRS equipment or existing law, regulations, and policies and that these updates are coordinated with all applicable CBP offices using IDVRS. The VMS system will have appropriate safeguards and audit trails in place to restrict access and viewing of recorded data to those with an official need to know. Such safeguards will automatically log the CBP Officer/Agent accessing the IDVRS recording, as well as the date and time of access.

Only CBP Officers/Agents and personnel with an official need to know will be permitted to access, view, download, disclose, dispose of, or otherwise distribute IDVRS recordings pursuant to CBP policy and based on VMS restrictions. Similar to the process during the 2018 IDVRS Evaluation, CBP will conduct periodic audits of randomly selected IDVRS recordings to ensure that the recordings are being properly categorized and named according to the established SOP and all IDVRS recordings tagged as Evidentiary Value are properly transferred to the appropriate CBP law enforcement system.

Contact Official

Marty P. Chavers
Deputy Executive Director
Policy Directorate
Office of the Commissioner
U.S. Customs and Border Protection

Responsible Official

Debra L. Danisek
Privacy Officer
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection
Privacy_CBP@cbp.dhs.gov

Approval Signature

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

_____

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