Privacy Impact Assessment
for the

Incident-Driven Video Recording Systems (IDVRS) Evaluation

DHS/CBP/PIA-052

April 2, 2018

Contact Point
Marty P. Chavers
Deputy Executive Director
Policy Directorate, Operations Support
U.S. Customs and Border Protection
(202) 325-1395

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) is conducting a field evaluation of Incident-Driven Video Recording Systems (IDVRS) throughout its law enforcement operations. CBP is conducting this study to determine CBP's capability needs and gaps associated with documenting incidents to enhance transparency of operations. The goal of this evaluation is to determine the effectiveness of fixed, vehicle, and body-worn camera technology to provide an accurate representation of law enforcement encounters, while allowing CBP Officers/Agents to safely perform their duties. CBP is publishing this Privacy Impact Assessment (PIA) to evaluate the privacy risks associated with CBP's use of incident-driven video recording technology at and between U.S. ports of entry.

Overview

On December 18, 2014, President Barack Obama signed an Executive Order establishing the President's Task Force on 21st Century Policing.[1] The Task Force's final report (May 18, 2015) identified that implementing body-worn cameras at police departments can improve policing practices and build community trust and legitimacy. The report cautioned that implementing technologies into policing activities must be built on a defined policy framework with its purposes and goals clearly delineated. Implementing new technologies can give police departments an opportunity to fully engage and educate communities in a dialogue about their expectations for transparency, accountability, and privacy.

Camera technology may be an effective tool for providing additional information regarding law enforcement encounters with members of the public. IDVRS technology implementation by police departments around the world has resulted in a variety of outcomes. Based on the outcomes of evaluations by other law enforcement agencies, CBP 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 unavailable.
- Supplementing evidence in criminal cases increasing the likelihood of obtaining successful prosecution for those who have violated the law.

[1] *See* https://obamawhitehouse.archives.gov/the-press-office/2014/12/18/executive-order-establishment-presidents-task-force-21st-century-policin.

- Enhancing training capabilities through utilization of footage as a learning tool.
- Contributing to a "civilizing effect" on law enforcement/civilian interactions by reducing hostilities between officers/agents and citizens.
- Strengthening officer/agent performance and accountability.
- Increasing officer/agent awareness and safety by influencing public behavior.
- Simplifying incident review by enabling the quick and immediate review of footage.

Previous CBP Evaluations

In 2014, the CBP Commissioner, R. Gil Kerlikowske, directed an internal working group to evaluate the feasibility of incorporating Body-Worn Camera (BWC) technologies into CBP law enforcement operations. The BWC feasibility study was conducted as part of CBP's continued emphasis on transparency and accountability. CBP seeks to expand its audio and video recording capability to enhance transparency and accountability with the public through the use of an IDVRS (to include body-worn and vehicle-mounted camera systems).

After testing the equipment in a controlled environment, CBP deployed the equipment in real-life encounters with members of the public from January 2015 through May 2015. CBP discontinued the use of BWCs after this phase of the study and deleted all video content.[2] The working group issued a final report based on the findings of the feasibility study; best practices from federal, state, and local law enforcement jurisdictions; feedback from CBP Officers/Agents that participated in the study; and benefits and concerns voiced by various stakeholders. The final 2015 *BWC Feasibility Study Report*[3] evaluated potential operational benefits of incorporating BWCs into CBP's law enforcement operations. The study supported CBP's overall efforts to increase transparency and accountability associated with law enforcement encounters between CBP Officers/Agents and members of the public. The feasibility study found that while the particular cameras evaluated were not well suited for all CBP environments, camera deployment may benefit the CBP mission by affording additional insight into law enforcement encounters and use of force incidents.

The final *BWC Feasibility Study Report* concluded that BWCs and other types of cameras "may offer benefits in support of the CBP mission," but cautioned that "BWC technology may

[2] CBP discontinued the use of BWCs after this phase of the study and deleted all video content in accordance with the National Archives and Records Administration (NARA) disposition authority DAA-0568-2015-0002. This disposition authority instructs the immediate destruction of associated audio and video footage after the cutoff period which is 90 days from the recording termination date of the event. *See* NARA, Records Schedule: DAA-0568-2015-0002, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0568/daa-0568-2015-0002_sf115.pdf.

[3] *See* Body-Worn Camera Feasibility Study Report (August 2015), *available at* https://www.cbp.gov/sites/default/files/documents/body-worn-camera-20151112.pdf.

also adversely affect CBP's Officers/Agents, operations, and mission." The *BWC Feasibility Study Report* recommended CBP undertake "thoughtful consideration of the advantages and disadvantages of BWC technology, resolution of policy issues, as well as recognition of the diverse individual component operational environments, risk-assessments, and enforcement assignments" to direct its implementation decisions.

CBP IDVRS Policy

On January 31, 2017, CBP issued the agency-wide Directive governing CBP's use of *Incident-Driven Video Recording Systems.*[4] The IDVRS Directive outlines the policies for the use of IDVRS, details responsibilities for parties involved, and lays out procedures related to operation, retention, and training. The IDVRS Directive establishes a number of requirements, including:

- CBP Officers/Agents should record enforcement encounters at the start of the event, or as soon as possible thereafter, and should deactivate their devices once their involvement has concluded.
- CBP Officers/Agents should advise individuals that they are being recorded if it will not interfere with the encounter or officer/agent safety; notice shall be provided whenever possible and practical.
- CBP Officers/Agents should not use IDVRS to record in areas where individuals have a reasonable expectation of privacy, or for the purpose of capturing individuals engaged in activities protected by the First Amendment.
- All recorded data should be stored only on a designated CBP-approved system or media with appropriate safeguards and audit trails, and must be appropriately labeled and categorized.
- CBP Officers/Agents may review footage for preparing reports and investigations for testimony or courtroom presentation, for training, and in preparation of administrative interviews, and all reports shall designate whether IDVRS footage was viewed prior to completion.
- Any release of IDVRS data must be coordinated with the CBP Privacy Office; additional oversight offices must be coordinated with for certain types of requests.

CBP's deployment of IDVRS under this demonstration is bound by the IDVRS Directive and its

[4] The Directive defines IDVRS as "all incident-activated, non-surveillance audio/video recording devices owned by CBP and used by CBP Officers/Agents during the course of their official duties, including, but not limited to: vehicle-mounted, non-integrated vessel-mounted, and body-worn cameras. Cellphones are not included in the definition of IDVRS, and should not be used as a primary means to record enforcement actions."

requirements, which are discussed in more detail in the privacy analysis portion of this document.

2018 IDVRS Field Evaluation

Beginning in April 2018, CBP will deploy IDVRS solutions from multiple commercially available vendors at select operational sites for approximately six months.[5] The evaluation will be 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 ports of entry, (4) airports, (5) seaports, (6) marine enforcement operations, and (7) aviation enforcement operations. The goals of the evaluation include assessing the suitability and effectiveness of various IDVRS devices in CBP operational environments and developing CBP's operational and technical performance requirements for these systems.

CBP will conduct the evaluation in multiple CBP locations nationwide,[6] and it is expected to end approximately six months after commencement. The exact duration and start date of the evaluation are contingent upon field conditions. CBP has identified alternate testing sites should designated locations become unsuitable for the evaluation.

CBP will deploy the following types of IDVRS during the evaluation:

- Body-worn cameras (BWCs), which will be mounted on the officer/agent's chest using manufacturer attachments; and
- Vehicle-mounted cameras (VMC), which will be installed on the front of patrol cars stationed at U.S. Border Patrol (USBP) checkpoints and land ports of entry.

CBP will use IDVRS to record official law enforcement encounters[7] between authorized, on-duty, uniformed CBP Officers/Agents[8] and members of the public, except when doing so may

[5] Specifically, CBP procured and will evaluate several commercially available systems in order to support CBP's market research. The Evaluation is not intended to determine CBP's final selection of camera systems, but will allow CBP Officers/Agents to use various IDVRS to assist them in their day-to-day operations. Systems selected for the CBP operational demonstration and evaluation may or may not be competitive options in CBP future procurement. In addition, CBP does not intend for future procurements to be limited to the exemplar systems selected for this initial operational demonstration.

[6] Operational developments may require CBP to relocate the Evaluation to different locations.

[7] 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), *available at* 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.

[8] 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.

jeopardize officer or public safety.

During the evaluation, authorized CBP Officers/Agents will download IDVRS data at the end of each shift to an approved, on-site data storage system (NetApp storage device)[9] on the CBP network with appropriate access restrictions. Data is downloaded to the content management system once the camera is placed on the docking station. Depending on the camera manufacturer, the data on the camera is either wiped clean at the end of the download or overwritten during recording after download, which minimizes or eliminates concerns regarding duplicate downloads of footage. CBP Officers/Agents will label the recorded data files according to one of the following applicable categories:[10]

a) 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. CBP will retain this data for 90 days[11] and subsequently destroy non-evidentiary data in accordance with the National Archives and Records Administration (NARA)-approved schedule DAA-0568-2015-0002.

b) Evidentiary – Any recorded data that may have material or probative value, or may have bearing on any criminal, administrative, civil, or other legal proceeding. Files determined to have evidentiary value shall be preserved under established rules of evidence with the associated case file.

CBP Officers/Agents who complete all necessary training requirements may participate in the evaluation on a voluntary basis. Training will include: 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 data. CBP will train users on the appropriate recording procedures before providing access to the IDVRS. Failure to comply with the guidelines and requirements of the IDVRS Directive is a violation of CBP's Standards of Conduct[12] and may

[9] The NetApp storage device is the designated information/data storage equipment employed during the IDVRS evaluation. The NetApp storage device is a vetted system and member of the CBP Active Directory (AD) domain network. CBP has obtained an Authority to Test (ATT) that will remain in effect for the duration of the evaluation.
[10] CBP has conducted substantive market analyses and visited various law enforcement departments to better inform the Agency on best practices regarding tagging law enforcement video footage. Specific sub-categories applicable to CBP for tagging video footage will evolve during the evaluation and can be best determined as a result of the assessment of the evaluation period. Each data file must be labeled with the more relevant of the two categories, non-evidentiary or evidentiary, in accordance with the CBP IDVRS Directive.
[11] Footage that is categorized as non-evidentiary and is not requested via the Freedom of Information Act (FOIA) will remain in the local NetApp storage and be automatically deleted after 90 days.
[12] *See* U.S. Customs and Border Protection Directive No. 51735-013A: U.S. Customs and Border Protection Standards of Conduct (March 2013), *available at* https://www.cbp.gov/sites/default/files/documents/std_of_conduct_3.pdf.

subject an employee to disciplinary action, including termination of employment or prosecution.

Retention and Tagging Requirements

CBP personnel are prohibited from deleting, modifying, or disposing of IDVRS recorded data unless it is non-evidentiary and past its 90-day retention period, as permitted by official agency policy. IDVRS users will follow the existing chain of custody and evidence handling procedures for all captured IDVRS evidentiary audio and video recordings.

IDVRS recordings are retained as non-evidentiary by default. At the end of a shift, CBP Officers/Agents must access a dashboard on a computer terminal to upload the recordings from their assigned camera and then manually apply any relevant tags. Recordings that are considered to have material or probative value, or have bearing on any criminal, administrative, civil, or other legal proceeding, are considered "evidentiary" per the IDVRS Directive and CBP Officers/Agents must manually apply the appropriate "tag" referenced in Figure 1 below.

Figure 1 – Mandatory Content Tagging

Primary Tags	**Retention**
Deadly Force Incident	75 years
Fatality	75 years
Less Lethal Force Incident	75 years
Pursuit (Vehicle, Vessel, Foot)	75 years
Arrest/Apprehension	75 years
Seizure	75 years
Vehicle Stop	2 years
Evidentiary/Non-Categorized	5 years
Hostile/Possible Complaint[13]	2 years
Casual Encounter	90 days
Non-Evidentiary/Non-Categorized	90 days
Accidental Activation	90 days
Training	5 days

The primary tags above map to the enforcement system of records notices (SORN) referenced in Appendix A, which control the retention period for the video recording.[14] Secondary tags assist in locating the corresponding recording in the video storage solution(s). CBP Officers/Agents must also include a secondary tag, and include a case number in the corresponding free text field, to match the video recording to the relevant case/event number if evidentiary. CBP Officers/Agents may include as many secondary tags as necessary per the event. Secondary tags for use during the evaluation include:

- TECS;
- E3;

[13] Agents and officers may encounter a complaint when posted at a public location, such as a checkpoint.
[14] Note that this table does not map each evidentiary type to each SORN in Appendix A, because a use of force incident can happen during an enforcement event in each SORN listed.

- Enforcement Action Statistical Analysis and Reporting System (E-Star);
- Joint Integrated Case Management System (JICMS);
- Unified Passenger Targeting (UPAX);
- Significant Incident Report (SIR) Module;
- Other CBP Enforcement Systems;
- Other Agency Systems;[15]
- Freedom of Information Act (FOIA) (records requested through FOIA are retained for 6 years per current CBP FOIA Office protocol);
- Litigation Hold;
- Under Investigation; and
- Notes.

Once appropriately categorized and associated with the corresponding case file, the footage will be transferred from the secure, on-site NetApp storage device/database,[16] via the DHS network, to a Federal Risk and Management Program (FedRAMP)-certified cloud software as a service (SaaS) provider within 90 days of its original upload of the footage. The associated files would be re-labeled as "evidentiary." The designated tagging applies to content regardless of the duration of the incident/encounter (*i.e.*, 5 minutes or several hours). Additionally, per the IDVRS Directive, there will be CBP supervisory oversight into the retention and tagging of video content during the evaluation.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974,[17] 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,[18] 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.

[15] This category will encompass systems that CBP may not realize need to be included as tags in the evaluation. If CBP uses another enforcement system, either external or internal to CBP, CBP will add a new tag for the operational phases of this evaluation.
[16] The NetApp storage device is the designated information/data storage equipment employed during the IDVRS evaluation. The NetApp storage device is a vetted system and member of the CBP Active Directory (AD) domain network. CBP has obtained an Authority to Test (ATT) that will remain in effect for the duration of the evaluation.
[17] 5 U.S.C. § 552a.
[18] 6 U.S.C. § 101, et seq.

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 (PIAs) on both programs and information technology systems, pursuant to section 208 of the E-Government Act[19] and section 222 of the Homeland Security Act of 2002.[20] 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.

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.

During the evaluation, per the IDVRS Directive, CBP Officers/Agents will 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 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 officer 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 even in close proximity to an incident that their facial image or voice will be/has been recorded. To address this gap, CBP is publishing this PIA to provide general notice of its use of IDVRS. In addition, it provides notice of its collection of information related to individuals in the relevant SORNs (see Appendix A).

Generally, although the video and audio recordings clearly identify an individual's facial features and capture any verbal communication, no additional personal information is associated with these images and recordings unless an apprehension or law enforcement action is taken and a case file is created for tracking purposes. However, when CBP Officers/Agents record an individual during a law enforcement action, and the recording is stored in a system of records, the information becomes subject to the requirements of the Privacy Act of 1974. These recordings are

[19] Pub. L. 107-347; 44 U.S.C. § 3501 note.
[20] Pub. L. 107-296; 6 U.S.C. § 142.

maintained in accordance with the retention schedules published in the associated PIAs and SORNs. CBP law enforcement-related systems include: TECS,[21] Seized Assets and Case Tracking System (SEACATS),[22] E3,[23] Enforcement Action Statistical Analysis and Reporting System (E-STAR),[24] and the Joint Integrated Case Management System (JICMS).[25]

For the duration of the evaluation, IDVRS data downloaded on-site and categorized as non-evidentiary will strictly be stored on the NetApp storage device. Non-evidentiary and evidentiary footage will include automatically generated tags for date, time, camera ID, and officer/agent name for ease of retrieval when uploaded on-site. Each officer/agent will be assigned a specific camera for use throughout the IDVRS evaluation increasing accountability, security, and transparency. Officer/agent names will be associated with the individual camera assigned to the officer/agent, respectively. Recordings that have an associated connection with an aforementioned law enforcement-related system, must adhere to the appropriate SORNs detailed in Appendix A.

To ensure retention requirements align with the relevant enforcement record, CBP will transfer all evidentiary data, upon receiving the appropriate tag, to a FedRAMP-certified cloud environment. Non-evidentiary footage requested under the Freedom of Information Act (FOIA) within the 90-day retention period will be reviewed on a case-by-case basis and, if determined appropriate for release in accordance with the CBP IDVRS Directive, will also be transferred to a FedRAMP-certified cloud environment.[26] The cloud storage will have vetted encryption security and appropriate permission restrictions. Should commercial, cloud-based storage systems be used during the evaluation, CBP will ensure that the system vendors are FedRAMP-certified,[27] aligning with National Institutes of Standards and Technology (NIST) Special Publication 800-53 (SP 800-53)[28] and other DHS/CBP security requirements.

In the event that evidentiary recordings are requested for criminal, administrative, civil, or other legal proceedings, the appropriate SORNs will apply. If non-evidentiary or evidentiary

---

[21] *See* DHS/CBP/PIA-021 TECS System: Platform, *available at* https://www.dhs.gov/privacy.
[22] *See* DHS/CBP/PIA-040 Seized Assets and Case Tracking System (SEACATS), *available at* https://www.dhs.gov/privacy.
[23] *See* DHS/CBP/PIA-012 CBP Portal (E3) to ENFORCE/IDENT, *available at* https://www.dhs.gov/privacy.
[24] *See* DHS/CBP/PIA-045 Assaults and Use of Force Reporting System (AUFRS), recently renamed E-STAR, *available at* https://www.dhs.gov/privacy.
[25] *See* DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS), *available at* https://www.dhs.gov/privacy.
[26] Privacy Impact Assessment for Office of Information Policy's Use of FOIAonline: Under NARA's General Records Schedule (GRS) 4.2, agencies may retain FOIA, Privacy Act, and Mandatory Declassification Review records for a maximum of six years after final agency action, and litigation records for a maximum of three years after final adjudication by the courts. Please *see* https://www.justice.gov/FOIAonline/download.
[27] FedRAMP Revision 4 Transition Guide v3.0.
[28] National Institutes of Standards and Technology (NIST) Special Publication 800-53 provides a catalog of security and privacy controls for federal information systems and organizations to protect organizations' operations, assets, individuals, and the Nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks.

materials are requested under FOIA, CBP will review requests on a case-by-case basis and release information as appropriate in accordance with the CBP IDVRS Directive and FOIA requirements.

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 law enforcement encounter, regardless of whether they are directly or indirectly involved.

Mitigation: This risk is partially mitigated. CBP Officers/Agents generally attempt to provide verbal notice during the onset of an encounter when possible. Additionally, BWCs and VMCs are generally positioned or mounted in highly visible locations on the officers'/agents' bodies, or CBP vehicles. However, given the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of CBP personnel or third parties. Therefore, CBP also provides general notice to the public through this PIA.

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 individuals to 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.

During the evaluation, the IDVRS Directive requires CBP Officers/Agents to only use IDVRS to capture law enforcement encounters between authorized on-duty uniformed CBP Officers/Agents and members of the public. CBP Officer/Agent safety, the safety of the public, and the safe operation of government vehicles, not the ability to record, shall always be the primary consideration, even when using an IDVRS CBP will also instruct its officers/agents to continue recording until the law enforcement-related encounter ends, subject to certain specified exceptions.[29] These interactions are often in public areas and may result in the capture of

[29] CBP Officers/Agents are not required to continue to record enforcement encounters if or when the following applies in accordance with the IDVRS Directive, Section 8.6:

individuals besides those who are the focus of the law enforcement encounter. Once a recording becomes associated with a law enforcement encounter case file, the use and retention period of that recording is governed by the record types associated with the case file.

Individuals can look to the SORN(s) provided in Appendix A to determine 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.[30] Individuals seeking notification of, and access to, any record contained in an associated system of record, or seeking to contest its content, may submit a request in writing to: U.S. Customs and Border Protection (CBP), Freedom of Information Act (FOIA) Division, 1300 Pennsylvania Avenue NW, Room 3.3D, Washington, D.C. 20229. Specific FOIA procedures can be found at https://www.cbp.gov/site-policy-notices/foia. Non-evidentiary footage must be requested within 90 days of the incident occurrence, prior to its automated deletion. During the evaluation, CBP will use the primary and secondary tagging capabilities to ensure that records are maintained in accordance with their respective retention schedules.[31]

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

Mitigation: This risk is partially mitigated as CBP will consider individual requests to determine whether or not information may be released. Individuals can contact the CBP Privacy

- They receive a direct order from a supervisor to deactivate the IDVRS. In this case, supervisors who order subordinates to stop recording will document the reason for doing so in a statement or report;
- Continued recording may compromise officer/agent safety;
- In the officer/agent's judgment a recording would interfere with his or her encounter or may be inappropriate because of the victim or witness's physical condition, emotional state, age, or other sensitive circumstances (*e.g.*, victim of domestic or sexual violence);
- A witness is concerned about retaliation if he or she is seen cooperating with CBP Officers/Agents (*e.g.*, material witnesses, sources of information); or
- Recording would risk the safety of a confidential informant or undercover law enforcement officers/agents.

[30] Any release of IDVRS recorded data external to DHS must be coordinated with the CBP Privacy Office and depending on the request, coordinated with, but not limited to: the impacted operation office(s), Office of the Commissioner, Office of Public Affairs, Office of Chief Counsel, Office of Professional Responsibility, Office of Human Resources Management, and Office of Congressional Affairs. The appropriate DHS Headquarters offices must be notified and provided the IDVRS recording prior to any external release.

[31] CBP has conducted substantive, market analyses and visited various law enforcement departments to better inform the Agency on best practices regarding tagging law enforcement video footage. Specific sub-categories applicable to CBP for tagging video footage will evolve during the evaluation and can be best determined as a result of the assessment of the evaluation period. IDVRS data files will have the following associated tags for data standardization and ease of retrieval: date, time, camera ID, and officer/agent name. The camera ID will be specific to the officer or agent (*i.e.*, each officer/agent will be assigned to one camera for the duration of the evaluation).

Officer or CBP FOIA Officer. Additionally, if an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, 245 Murray Drive Southwest, Building 410, STOP-0655, Washington, D.C. 20528. However, there remains some risk to access, given CBP may be authorized to withhold records, the release of which may compromise law enforcement investigations or proceedings.

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

Mitigation: This risk is partially mitigated. CBP developed the two-step process for determining recording retention to ensure that evidentiary recordings are preserved for enforcement, prosecutorial, and access purposes. CBP deliberately defined "evidentiary" as broadly as possible to ensure that CBP retained as many recordings as possible without creating an unmanageable amount of recordings to store, tag, search, and maintain. CBP will retain footage in accordance with the NARA-approved retention schedule.

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 CBP, as their images or voices may be captured without notice or opportunity to opt-out of the collection.

Mitigation: This risk is partially mitigated. In accordance with the IDVRS Directive, CBP Officers/Agents should advise individuals that they are being recorded if it will not interfere with the encounter or officer/agent safety.[32] Any recordings that are extraneous and do not become associated with case files will be labeled non-evidentiary and deleted after 90 days. Under FOIA, faces of officers and any uninvolved bystanders will be blurred. Only the face(s) of the consenting subject(s) is appropriate to release. These actions reduce the risk of individuals in the periphery of situations being unaware of recordings and/or having their images retained by CBP with no business justification to do so.

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: The risk is mitigated. The CBP Law Enforcement Safety and Compliance (LESC) office has determined that the recording devices selected for use during the evaluation can adequately incorporate date, time, camera ID, and officer/agent name tags for video footage metadata. In addition, CBP has customized primary and secondary tags to assist in the storage,

[32] IDVRS Directive, Section 8.4.1

search, and retrieval of evidentiary records. These tags will allow for standardized retrieval of video footage at test site locations for the duration of the evaluation.

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.[33] 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.[34] 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 enforcement activities when a recording of an encounter would assist in documenting the incident for law enforcement purposes.[35]

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. In the same manner that government agencies may install Closed Circuit Television (CCTV) cameras in stationary positions outside of facilities, CBP may use IDVRS in public areas during interactions with the public for mission-related purposes.

As previously discussed, if IDVRS recorded data becomes associated with an individual's investigation or case file, then the data will be retained and governed by the SORN(s) that apply to such investigation or case file (see Appendix A). Any extraneous or incidental IDVRS-recorded data that is captured and not associated with mission-related activity is maintained for 90 days and then deleted. IDVRS recorded data may be disclosed to other federal, state, local, tribal, and international law enforcement agencies in order to assist in enforcement activities 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.

Privacy Risk: There is a risk that CBP Officers/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 investigations. Video cameras can capture individuals entering places or engaging in activities as they relate to their daily lives in populated areas. For example, IDVRS

[33] 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.
[34] IDVRS Directive.
[35] IDVRS Directive, Section 8.3.

may collect video of an individual entering a doctor's office, attending public rallies, social events or meetings, or associating with other individuals.

Mitigation: CBP mitigates this risk by limiting recordings to official law enforcement encounters that support CBP mission and policy, which may include use of force incidents; encounters with the public that are likely to become hostile, adversarial, or confrontational; and other enforcement activities when a recording of an encounter would assist in documenting the incident for law enforcement purposes. While IDVRS may record lawful activities, these recordings, to the extent they do not involve a law enforcement encounter, will be considered "non-evidentiary" and will not be stored beyond 90 days, nor will they be associated with any CBP case files and, therefore, any PII. CBP will copy and retain information from IDVRS only when it is relevant to an active case file for law enforcement or border security purposes. Additionally, CBP will not associate the recorded video or other data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation or other administrative or judicial action.

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 will be used to record official law enforcement encounters except when doing so may jeopardize officer/agent safety. CBP acknowledges that there may be situations in which operation of the system is impractical and may be an impediment to the 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 90 days from the recording. Those images and recordings that become associated with case files, would be retained for longer than 90 days based on the retention schedules applicable to the respective case files.

Privacy Risk: There is a risk of over-collection, since IDVRS 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. CBP limits recordings to official law enforcement encounters that support the CBP mission and policy. While IDVRS will record lawful activities, any such recordings that do not involve a law enforcement encounter are considered "non-evidentiary" and not stored beyond 90 days from the end of the recording date, nor are they associated with a case file and, therefore, any PII. Deleting these non-evidentiary files reduces the risk of retaining data that is not germane to a law enforcement encounter.

CBP copies and retains information from IDVRS only when it is relevant to an active case file for law enforcement or border security purposes. However, it is possible that CBP may retain images of individuals who are near the scene of an enforcement incident. If these individuals are not involved in the law enforcement encounter, their images will be saved as part of the evidentiary file but will not linked or tagged for search. These images will be blurred or redacted prior to release under FOIA, even when part of an evidentiary record.

Privacy Risk: There is a risk that CBP may retain footage or PII for longer than necessary to meet CBP's border security mission.

Mitigation: This risk is mitigated. CBP automatically deletes recordings not associated with mission-related activity that do not become part of a law enforcement record or case file after 90 days. Those images and recordings associated with case files or other law enforcement records are retained in accordance with the established retention schedules and procedures for the respective case files or records. Additionally, CBP Privacy will conduct a CBP Privacy Evaluation (CPE) on the retention process and data tagging for retention purposes within IDVRS at the end of the evaluation period. Following the CPE, CBP Privacy will make recommendations regarding changing or modifying the tagging process to better align with CBP operational needs. The results of the CPE will be shared with the DHS Privacy Office.

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.

CBP restricts its use of IDVRS footage captured during the evaluation to the following purposes:

- To further evaluate if universal BWC assumptions hold true in CBP's operational environments;
- To assist in drafting a report or any other paperwork required in association with an incident;
- For evidence in association with a law enforcement action or investigation; and
- To review CBP Officer/Agent actions in relation to an incident tagged as evidentiary.

CBP Officers/Agents are trained to record enforcement encounters at the start of the event, or as soon as safely possible thereafter. In addition, the IDVRS Directive prohibits the use of IDVRS in the following circumstances:

- For the sole purpose of conducting or supporting a personnel investigation or disciplinary action;
- For employee assessments, except for use in the training environment as part of student/instructor feedback process;
- For recording CBP personnel during non-enforcement activities;
- For privileged communication between CBP personnel and their attorney or Union representative;
- In places or areas where persons have a reasonable expectation of privacy, such as locker rooms, dressing rooms, or restrooms, unless related to official duties;
- In hospitals or to record patients during medical or psychological evaluations, or during treatment, unless related to official duties;
- In non-CBP detention facilities, jail facilities, or other law enforcement facilities that prohibit the use of recording equipment; or
- For the purpose of capturing individuals who are engaged in activity protected by the First Amendment.

CBP may occasionally disclose IDVRS recorded data outside of DHS consistent with the applicable disclosure provisions of the Privacy Act if linked to an enforcement record. If the encounter 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, unless they have independent authority to retain the information.

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.

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

Mitigation: In accordance with the IDVRS Directive, Section 8.2, CBP mitigates this risk by prohibiting the use of CBP-owned IDVRS for personal use, and prohibiting 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 incidents pertaining to those locations. CBP restricts officers/agents from recording events that are not law enforcement encounters, including actions and conversations of co-workers and management that are not part of the law enforcement incident. In addition, supervisors or other personnel may not routinely or randomly view recorded data for the sole purpose of identifying policy violations, conducting or supporting personnel investigations, or disciplining the responsible CBP Officer/Agent. CBP will not record CBP briefings, meetings, or roll calls; employee performance assessments; places where individuals have a reasonable expectation of privacy, such as medical doctor or psychiatrist's offices unless it is related to official duties; non-CBP law enforcement facilities that prohibit recording equipment; and individuals who are engaged in non-confrontational and/or non-adversarial activity protected by the First Amendment of the U.S. Constitution.

Since unauthorized use or release of IDVRS recorded data may compromise ongoing criminal investigations and administrative proceedings, or violate the privacy rights of recorded individuals, any unauthorized access, use, or release of recorded data or other violation of confidentiality laws and Department policies may result in disciplinary action. CBP specifically limits IDVRS use to law enforcement activities.

Additionally, CBP prohibits officers/agents from (1) tampering with or dismantling an IDVRS, including 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.

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: Data requests for IDVRS recorded information are subject to all applicable laws, regulations, collective bargaining agreements, memoranda of understanding (MOU), CBP policies, and governing SORNs. CBP requires its components to seek approval from CBP stakeholder offices prior to releasing IDVRS recorded data to a third-party. Specifically, the CBP

Privacy Office requires all components to complete a DHS Privacy Act Disclosure Record (DHS Form 191) upon sharing personal information outside of DHS. The receiving agency is required to use the IDVRS recording only for the purpose(s) for which CBP disclosed the data, and must return the data to CBP or destroy all the information after analysis, unless they have separate statutory authority to retain the recordings.

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

Mitigation: CBP mitigates this risk by determining whether or not the recording has evidentiary value. Recordings determined to have non-evidentiary value are deleted after 90 days. Additionally, IDVRS recorded data is only disclosed for official purposes in accordance with applicable DHS/CBP policies, including FOIA and Privacy Act request procedures listed in Section 2 of this document.

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 captures IDVRS recorded data in real-time to maintain an audio/video record of law enforcement encounters. CBP uses this footage, in part, to verify what occurred during the encounter. Although the collection of IDVRS footage does not generally involve the collection of PII, CBP verifies any PII that may be captured in the audio or video footage prior to entering it into a separate enforcement or investigation record. In addition, audio and video recordings of law enforcement encounters would not be the sole source to identify potential subjects in cases or investigations. These recordings would supplement existing processes in building law enforcement cases.

CBP outlined a standard for camera equipment and video footage based on market research and best practices.[36] 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. Only technology that has been vetted through the indicated standards will be utilized during the IDVRS evaluation period. The standards for camera equipment and video footage are as follows:

[36] 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.

- Shall have a minimum video resolution of 480p (standard definition);
- Shall be configurable to 720p (high definition);
- Shall have video compression of at least H.264. Use the lowest possible amount of compression in order to maximize the amount of information available;
- Shall have a frame rate of at least 30 frames per second; and
- Shall have audio compression sufficient to capture high speech quality.

Each vendor's video management system (VMS) automatically tags the time, date, camera ID, and officer/agent name of recorded footage to standardize metadata and assist in footage retrieval and ensure the availability of the footage. Additionally, the vendor's VMS allows for manual tagging of uploaded footage by each officer/agent based on the event or type of encounter. Finally, CBP follows the NARA-approved retention schedule to ensure the availability of evidentiary footage, while preventing the over-collection of non-evidentiary footage.

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

Mitigation: This risk is mitigated by the fact that CBP Officers/Agents use a variety of evidence prior to taking action, and would use IDVRS footage to supplement information obtained via other investigative techniques.

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 (typically on stand-alone servers connected to 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.[37] Furthermore, the IDVRS security setting is a CBP/Office of Information Technology (OIT)-approved and validated operating system using DHS security standards. Though video and audio files/data recorded during the evaluation will be stored at multiple test locations, the IDVRS application is set up on a server that is connected to an on-site, NetApp storage device on the CBP network. The IDVRS server and NetApp storage devices are both

[37] *See* DHS 4300A, *available at* https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive%20Systems%20Policy%20v11%200.pdf.

members of the CBP Active Directory (AD) domain network. The data will also be transferred to the FedRAMP-certified cloud environment.

Access to the audio/video data on the CBP storage database requires a user verification, consisting of two levels of security at each evaluation site: Local Area Network (LAN)/Operating System (OS) Level security and IDVRS-application Level security. LAN/OS Level security is controlled by active directory security grouping and user accounts formulated by NIST 800-53 standards. Sites will determine key individuals with OS Level security access. IDVRS-application security is controlled by both the vendor software application and OS 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 dealing with 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. All CBP Officers/Agents must download all IDVRS recorded data to the local storage database at the end of each shift, unless otherwise specified by their respective offices. The downloaded data will be stored locally for 90 days. Any evidentiary data will be moved to a central storage location "by replication" while the remaining data on the local database is destroyed. Officers/agents and their supervisors will label the respective videos and recordings appropriately.

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

Mitigation: CBP will mitigate 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 storage databases within facilities that comply with DHS security requirements. The CBP Officer/Agent's Supervisor also 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 in 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.[38] 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.

Records maintained by CBP may only be disclosed to authorized individuals with a work-related need for the information and only for uses that are consistent with the intended purposes of the program. All information stored in CBP systems is secured in accordance with DHS system security requirements and standards. Users of these systems must complete annual security and privacy awareness training and be provisioned in the system to view the records based on their official need to know. User access and activities are audited, with audit logs that capture the date, time, and search terms, and misuse may subject the user to disciplinary consequences in accordance with DHS policy, as well as criminal and civil penalties.

CBP will ensure that video is properly stored, categorized, and labeled; and that standard operating procedures (SOPs) and technical guidance are updated to reflect changes to equipment or existing laws, regulations, and policies. These updates will be coordinated with all applicable offices. CBP will also monitor system deployment to ensure that CBP Officers/Agents are utilizing IDVRS correctly. The ability to audit the footage is necessary once the evaluation is complete and CBP has determined how to move forward with camera technology at the enterprise level based

[38] IDVRS Directive, Section 8.9.

on the assessment of the evaluation. These documented audits will be completed by selecting recorded data at random to ensure it is properly categorized and named according to established SOPs, and ensuring that all recorded data determined to be of evidentiary value or requested under FOIA is properly transferred to CBP law enforcement systems.

Responsible Officials

Marty P. Chavers
Senior Policy Advisor
Policy Directorate | Operations Support
Office of the Commissioner
U.S. Customs and Border Protection

Debra L. Danisek
Privacy Officer
Privacy and Diversity Office
Office of the Commissioner
U.S. Customs and Border Protection

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security

Appendix A
Records Retention and SORN Coverage

Record retention and System of Record Notice (SORN) coverage outline the categories of records retained, the purpose of retaining these records, and the retention schedules pertinent to information collected under this effort. CBP handles various types of data and addresses the security issues through multiple SORNs. The following list is not exhaustive but highlights the major types of records associated with the IDVRS evaluation and the corresponding SORNs.

There are five categories in which records are retained: 1) Border Patrol Enforcement Records; 2) CBP Assaults, Uses of Force, and Vehicle Pursuit Records; 3) Internal Affairs Records; 4) Law Enforcement Records; and 5) and Seized Asset Records. The purpose of a SORN is to protect the integrity of departmental operations, and to ensure compliance with applicable laws, regulations, and policies. The retention schedule lays out the procedures and duration for retaining, maintaining, and the using these records.

	Basic Record Category	**SORN/Purpose**	**Retention Schedule**
1	Border Patrol Enforcement Records and CBP Assaults, Uses of Force, and Vehicle Pursuit Records	DHS/CBP-023 Border Patrol Enforcement Records: The purposes of this system of records is are to (1) Prevent the entry of inadmissible aliens into the United States; (2) Record the detection, location, encounter, identification, apprehension, and/or detention of individuals who commit violations of U.S. laws enforced by CBP or DHS between the POE; (3) Support the identification and arrest of individuals (both citizens and non-citizens) who commit violations of federal criminal laws enforced by DHS; (4) Support the grant, denial, and tracking of individuals who seek or receive parole into the United States; (5) Provide criminal and	CBP is in the process of drafting a proposed record retention schedule for the information maintained in the BPER SORN. CBP anticipates retaining records of arrests, detentions, and removals for seventy-five (75) years. Investigative information that does not result in an individual's arrest, detention, or removal, is stored for twenty (20) years after the investigation is closed, consistent with the N1-563-08-4-2. User account management records for ten (10) years following an individual's separation of employment from federal service; statistical records for ten (10) years; audit files for fifteen (15) years; and backup files for up to one (1) month. Records replicated on other DHS or CBP

		immigration history information during DHS enforcement encounters, and background checks on applicants for DHS immigration benefits (*e.g.*, employment authorization and petitions); and (6) Identify potential terrorist and criminal activity, immigration violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.	unclassified and classified systems and networks will follow the same retention schedule.
2	Internal Affairs Records	DHS/ALL-020 Department of Homeland Security Internal Affairs: The purpose of this system is to collect and maintain records concerning internal affairs matters, specifically internal integrity or disciplinary inquiries, as well as internal reviews, inspections, or investigations conducted by DHS Headquarters or its components, except those conducted by the Office of Inspector General (OIG). This SORN is intended to support and protect the integrity of Departmental operations; to ensure compliance with applicable laws, regulations, and policies; and to ensure the integrity of DHS employees' conduct and those acting on behalf of DHS.	DHS retains investigative, inspection, and allegation-related files for five years after the related case is closed. Records would then be transferred to the Federal Records Center (FRC) and destroyed 25 years after the date of closure for investigative files and ten years after the date of closure for inspection and allegation-related files. Review files will be maintained for ten years after the related case is closed. Records would then be transferred to the FRC and retained permanently. Sexual abuse and assault files and reports would be maintained in a secure location for ten years after the end of the fiscal year in which the related case is closed. Records then would be transferred to the FRC and destroyed 20 years after the end of the fiscal year in which the case was closed.

3	Law Enforcement Records	CBP-011 U.S. Customs and Border Protection TECS: The purpose of this system is to track individuals who have violated or are suspected of violating a law or regulation that is enforced or administered by CBP, to provide a record of any inspections conducted at the border by CBP, to determine admissibility into the United States, and to record information regarding individuals, firms, and organizations to whom CBP has issued detentions and warnings. Additionally, this system of records covers individuals who have been given access to TECS for authorized purposes.	The majority of information collected in TECS is used for law enforcement and counterterrorism purposes. Records in the system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration. The retention period for information maintained in TECS is seventy-five (75) years from the date of the collection of the information for the life of the law enforcement matter to support that activity and other enforcement activities that may become related. TECS collects information directly from authorized users.
4	Seized Assets Records	CBP-013 Seized Assets and Case Tracking System (SEACATS): The purpose of this system is to document individuals and businesses who violated, or are alleged to have violated, Custom, immigration, agriculture and other laws and regulations enforced or administered by CBP; collect and maintain records on fines, penalties, and forfeitures; and collect and maintain records of individuals who have provided assistance with respect to identifying or locating individuals who have or are alleged to have violated Customs, immigration, agriculture and other laws and	Records related to a law enforcement action; or that are linked to an alleged violation of law or regulation, or are matches or suspected matches to enforcement activities, investigations or cases (*i.e.*, administrative penalty actions or criminal prosecutions), will remain accessible until the conclusion of the law enforcement matter and any other enforcement matters or related investigative, administrative, or judicial action to which it becomes associated plus five years. Records associated with a law enforcement matter, where all applicable statutes of limitation have expired prior to the conclusion of the matter, will be retained for two years following the expiration

		regulations enforced or administered by CBP.	of the applicable statute of limitations.