U.S. CUSTOMS AND BORDER PROTECTION DIRECTIVE

CBP DIRECTIVE NO.: 4320-030B **DATE:** AUG 06 2021
ORIGINATING OFFICE: U.S. Border Patrol/Law Enforcement Operations Directorate
SUPERSEDES: 4320-030 dated January 31, 2017
REVIEW DATE:

INCIDENT-DRIVEN VIDEO RECORDING SYSTEMS

1 PURPOSE. This directive establishes the responsibilities and procedures for the use of Incident-Driven Video Recording Systems (IDVRS), including vehicle, non-integrated vessel, and body-worn camera systems by U.S. Customs and Border Protection (CBP) personnel, in accordance with all applicable laws, regulations, policies, and procedures.

2 POLICY.

2.1 CBP authorizes the use of IDVRS to collect audio and video recordings of interactions between CBP Officers (CBPOs)/Border Patrol Agents (BPAs)/Air and Marine Agents (AMAs) and the public under the conditions and according to procedures stipulated in this directive, contingent upon critical operational priorities, and the availability of resources.

2.2 As stated in Section 8.3, IDVRS will be used to record official law enforcement encounters, except when doing so may jeopardize CBPOs/BPAs/AMAs or public safety.[1] CBP acknowledges that there may be situations in which system operation is impractical and may be an impediment to the public and officer safety. Additionally, the Agency recognizes human performance limitations during particularly stressful, critical situations.

2.3 When equipped with IDVRS, CBPOs/BPAs/AMAs should record enforcement encounters at the start of the event or as soon as safely possible thereafter and continue recording until the CBPOs/BPAs/AMAs involvement in the encounter has concluded.[2]

2.4 IDVRS recorded data will only be accessed, downloaded, and disclosed by authorized CBP personnel.

2.5 Accessing, viewing, copying, forwarding, or releasing any IDVRS recorded data other than for official use is strictly prohibited. CBPOs/BPAs/AMAs may review IDVRS recorded data prior to submitting reports.

---

[1] See Section 6.4 for definition of enforcement encounter.

[2] CBPOs/BPAs/AMAs shall deactivate their IDVRS when their role in the encounter has concluded (i.e., they are leaving the scene or have completed their interaction with the subject).

2.6 Any unauthorized access, use or release of recorded data, or other violations of confidentiality laws or Department of Homeland Security (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.

2.7 IDVRS shall not be used to record actions and conversations of coworkers when not actively engaged in resolving a law enforcement encounter. If applicable, refer to office policies regarding recording devices.

3 AUTHORITY.

lmmigration and Nationality Act (lNA); Title 7 USC; Title 8 USC; Title 9 USC; Title 12 USC; Title 15 USC; Title 16 USC; Title 17 USC; Title 18 USC; Title 19 USC; Title 21 USC; Title 22 USC; Title 26 USC; Title 27 USC; Title 31 USC; Title 42 USC; Title 47 USC; Title 48 USC; Title 49 USC; Title 50 USC; *Personal Search Handbook, HB 3300-04B; U.S. Customs and Border Protection, National Standards on Transport, Escort, Detention, and Search, October 2015; Land Border Inspectional Safety Policy, Directive 5290-007A; Physical Control of Suspects, Directive 3340-028; Non-Intrusive Inspection (NII) Technology, Directive 3340-036; Passenger Programs Handbook, CIS HB 3300-02A; Use of Force Policy, Guidelines and Procedures Handbook, HB 4500-01C; Personal Property Management, Directive 5230- 032A; Accounting for Personal Property, Directive 5230-027D; Privacy Policy, Compliance, and Implementation, Directive 2120-010; Freedom of Information Act Compliance Requirements Directive 2120-009B; Information Systems Security Policies and Procedures Handbook, HB l400-05D; DHS 4300A Sensitive Systems Handbook; U.S. Customs and Border Protection Standards of Conduct, Directive 51735-013A; and Table of Offenses and Penalties.*

4 SCOPE.

4.1 This directive establishes the authorities, responsibilities, and procedures for the use of IDVRS and recorded data by CBP personnel in Air and Marine Operations (AMO), Office of Field Operations (OFO), U.S. Border Patrol (USBP), and CBP personnel in other offices. This Directive applies to personnel who operate IDVRS or handle recorded data when required by duty location, leadership, other government agencies, or as required.

4.2 This directive sets forth overarching IDVRS guidance and does not replace the need for CBP office level Standard Operating Procedures (SOPs) and issuing manufacturer's operational guidelines and technical guidance. Offices will issue SOPs to facilitate the use of the specific types of IDVRS before deployment.

4.3 This directive does not apply to recording statements during criminal investigations, The Office of Professional Responsibility (OPR) official investigations or CBP administrative proceedings and does prohibit using IDVRS for those purposes.

5 BACKGROUND.

5.1 In a time when camera technology has become readily available, highly portable, and of broad application by the average citizen, law enforcement agencies have begun to discover the numerous benefits which camera technology can offer. IDVRS has demonstrated that such systems can be a valuable tool to establish facts surrounding a law enforcement encounter with the public, can provide evidence of criminal activity, and, in many cases, have documented excellent professional performance by law enforcement officers, which distinguishes them and their organizations. Therefore, CBP recognizes that

when used properly, camera technology can be a valuable tool in carrying out its mission. IDVRS recorded data may provide only a limited perspective of an enforcement encounter, therefore, it must be considered alongside all other available evidence when evaluating subject and law enforcement actions, including applicable witness statements, CBPOs/BPAs/AMAs interviews and statements, forensic analysis, and documentary evidence.

5.2 Camera technology may enhance CBP's ability to document and review statements and actions for field report purposes or courtroom preparation and provide audio and video footage of encounters and incidents to assist in addressing allegations of misconduct or personnel complaints. The technology may also clear CBPOs/BPAs/AMAs of unfounded accusations, provide evidence in support of criminal prosecutions, and safeguard the rights of members of the public and CBPOs/BPAs/AMAs

6 DEFINITIONS.

6.1 Agent means any class of CBP employees designated by the Commissioner to perform the functions of a BPA or AMA and who are trained to use IDVRS and handle recorded data.

6.2 Body Worn Camera System is the audio/video recording equipment combined into a single unit and typically worn on the authorized personnel's duty uniform.

6.3 CBPOs/BPAs/AMAs, supervisors, and CBP personnel mean persons who are trained to use IDVRS, handle recorded data, and to whom access is granted by an Executive Assistant Commissioner (EAC), the USBP Chief, an Assistant Commissioner (AC), or equivalent.

6.4 Enforcement Encounter means those actions taken by Agency personnel to carry out their mission. Such encounters include, but are not limited to, the following:

6.4.1 Use of force incidents as defined in the CBP Use of Force Policy, Guidelines, and Procedures Handbook, HB 4500-0lC;

6.4.2 Other enforcement activities in which 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

6.4.3 Observed suspicious or possible illegal activity.

6.5 IDVRS means all incident-activated, non-surveillance audio/video recording devices owned by CBP and used by authorized personnel during their official duties, including, but not limited to, vehicle mounted, nonintegrated 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.

6.6 Non-integrated Vessel Mounted Camera Systems mean all vessel camera systems not interconnected to vessel subsystems, software, hardware, or connection interfaces. Non-integrated Vessel Mounted Camera Systems are readily attached or detached without vessel reconfiguration, structural changes, or upgrades.

6.7 Officer means any class of CBP employee designated by the Commissioner as responsible for inspecting arriving and departing persons, conveyances, and baggage at

ports of entry and who are trained to use IDVRS and handle recorded data.

6.8 Office means all CBP organizational elements, including Headquarters (HQ) component offices, program management offices, facilities or centers, sectors, field offices, branches, or any other entity that reports to the CBP Commissioner or Deputy Commissioner.

6.9 Personnel means the CBP law enforcement personnel responsible for wearing the IDVRS, recording footage, and tagging footage; the CBP personnel who will function as system administrators; and CBP personnel or contractors responsible for accessing the VMS and redacting information from IDVRS footage.

6.10 Recorded data means all IDVRS data created as a result of enforcement encounters, which require on duty authorized personnel to activate an IDVRS.

6.11 Vehicle Mounted Camera System means an audio/video recording device designed for and installed (or often not interconnected to subsystems) into a vehicle to record events outside and inside (if equipped) of the vehicle during encounters.

7 RESPONSIBILITIES.

7.1 The Commissioner has overall responsibility for establishing policy and overseeing all aspects of IDVRS and recorded data and to ensure overall auditing and quality assurance. The Commissioner is also responsible for centralizing acquisition and contractual agreements, and for defining CBP operational requirements/resources.

7.1.1 The IDVRS Executive Agent will also serve in a principal role of engaging other DHS entities, government agencies, and stakeholders on all matters involving IDVRS.

7.2 The EAC for AMO, OFO, and the USBP Chief are responsible within their respective officers for the following:

7.2.1 Ensure that personnel use IDVRS for official law enforcement purposes only and in compliance with policy and SOPs;

7.2.2 Ensure that access to IDVRS and recorded data is limited to authorized personnel with a need to know;

7.2.3 Ensure that authorized personnel are properly trained to use IDVRS, as well as the correct handling of recorded data prior to issuing or allowing access to the IDVRS;

7.2.4 Ensure that training updates regarding changes to equipment or existing laws, rules, policies, or regulations are provided to authorized personnel;

7.2.5 Ensure that physical property is accounted for per CBP personal property management directives;

7.2.6 Establish procedures to ensure compliance with lost, damaged, destroyed, and stolen property reporting and accountability requirements;

7.2.7 Establish written procedures and designating responsibilities for downloading recorded data which may be delegated to the subordinate field level

offices, including reporting requirements which are not limited to inadvertent recording and failure of the previous shift to download recorded data;

7.2.8 Ensure that video is properly stored, categorized, and labeled;

7.2.9 Issue final authority for the use and release of their respective offices' IDVRS recorded data, consistent with law and policy requirements;

7.2.10 Ensure that SOPs and technical guidance are updated to reflect changes to equipment or existing law, regulations, and policies and that these updates are coordinated with all applicable offices;

7.2.11 Monitor system deployment to ensure that authorized personnel are utilizing IDVRS correctly;

7.2.12 Ensure recorded data is audited; and

7.2.13 Ensure that a case file identifier for each piece of recorded data is properly logged in the relevant CBP law enforcement systems, if of evidentiary value.

7.3 Other EACs, ACs, and equivalents ensure that access to IDVRS recorded data is granted only to authorized personnel with a legitimate need.

7.4 The Office of Information and Technology (OIT) AC is responsible for the following:

7.4.1 Ensures that IDVRS complies with relevant Federal, DHS, and CBP technology requirements and standards;

7.4.2 Ensures that all hardware and software which will connect to or be installed on the CBP network are approved and meet security standards documented in the *DHS 4300A Sensitive Systems Handbook*; and

7.4.3 Ensures any IDVRS software or storage mechanism accurately document user login credentials and maintains audit logs for each user and access to IDVRS recorded data.

7.5 The OPR AC is responsible for investigating criminal and administrative allegations and use of force incidents.

7.6 The Office of Training and Development AC is responsible for coordinating with the component offices to develop IDVRS training and to provide training materials that are consistent with existing law, regulations, and policies.

7.7 The Executive Director, Privacy and Diversity Office (PDO) is responsible for:

7.7.1 Providing notices to the general public regarding information collections which impact personally identifiable information, minimizing data collection, overseeing unauthorized disclosure of information, and managing information releases.

7.7.2 Receiving CBP Freedom of Information Act (FOIA) requests for IDVRS video footage and reviewing and redacting the video footage (applying legal exemptions consistent with the FOIA), and prior to releasing the redacted video

footage, clear with:

7.7.2.1 The appropriate operational offices-AMO, OFO, or USBP-as they have final authority for the use and release of IDVRS recorded data (see Section 7.2 above); and

7.7.2.2 OPR to ensure the release of the video does not compromise ongoing criminal investigations and/or administrative proceedings (see Section 7.5 above).

7.8 Authorized supervisory personnel are responsible for the following:

7.8.1 Ensure that authorized personnel are equipped with fully charged, fully functioning IDVRS when available;

7.8.2 Ensure that each IDVRS is properly logged in and out for use according to the CBP Personal Property Management Directives and handbook, and local property procedures;

7.8.3 Ensure that recorded data is moved to storage at the end of each shift and that all recorded data is correctly categorized and labeled; and

7.8.4 Ensure that CBPOs/BPAs/AMAs return IDVRS to the appropriate issuing point at the conclusion of each shift, except in extreme extenuating circumstances as provided in local SOPs.

7.9 CBPOs/BPAs/AMAs are responsible for the following:

7.9.1 Use IDVRS for official law enforcement purposes only and in accordance with the procedures in this directive and applicable SOPs;

7.9.2 Ensure the proper care, operation, and safekeeping of their assigned IDVRS;

7.9.3 Ensure that the IDVRS is in correct working order and the battery source (if the system requires battery power) is fully charged prior to accepting responsibility;

7.9.4 Ensure their IDVRS are correctly positioned on their clothing, vehicle, or vessel in accordance with the approved methods specified by the IDVRS manufacturer guidelines, their office's technical guidance, and applicable SOPs;

7.9.5 Notify their supervisor(s), if they discover their assigned IDVRS is lost, damaged, stolen, or inoperative, immediately, supervisors should alert TSD within 2 hours of event;

7.9.6 Ensure that all IDVRS recorded data is moved to storage at the end of their shift unless instructed otherwise;

7.9.7 Return the IDVRS at the conclusion of their shift, unless directed otherwise by their component office's SOPs; and

7.9.8 Report any known intentional misuse of IDVRS or IDVRS footage to

supervisors, CBP OPR, OIG, or appropriate security officials as appropriate.

8 PROCEDURES.

8.1 Safety

8.1.1 As outlined in existing CBP policies and procedures, authorized personnel shall continue to follow all current safety policies and procedures when conducting law enforcement operations.

8.1.2 CBP employee safety, the safety of members of the public, and the safe operation of government vehicles shall always be the primary consideration when using an IDVRS.

8.1.3 Authorized IDVRS users should not place themselves or others in dangerous situations solely for the purpose of recording an activity.

8.2 General

8.2.1 On duty CBP personnel will use only CBP issued and approved IDVRS and such use will be for official law enforcement purposes only.

8.2.2 The personal use of CBP owned IDVRS is strictly prohibited. No personally owned devices may be used in lieu of IDVRS to record law enforcement encounters, such as those described in Section 6.4.

8.2.3 CBP personnel shall not tamper with or dismantle an IDVRS, its hardware or software components.

8.2.4 CBP personnel shall not use any other device to intentionally interfere with the capability of the IDVRS.

8.2.5 IDVRS recorded data will only be accessed, downloaded, and disclosed by authorized CBP personnel.

8.2.6 CBP personnel will not delete or modify data on the IDVRS and will only dispose of IDVRS recorded data, as permitted by this policy.

8.2.7 Recorded data may not be accessed, used, downloaded, printed, copied, e-mailed, posted, shared, reproduced, or otherwise distributed in any manner, unless for official use and in accordance with this directive and office SOPs.

8.2.8 The existence of IDVRS recorded data does not relieve authorized personnel from preparing written reports or field reports or from carrying out any other responsibilities required by applicable law, policy, and procedures.

8.2.9 When not in use, all IDVRS and accessories or attachments shall be properly stored in the designated secure storage location as determined by the office SOP.

8.2.10 In the case of CBP personnel assigned to a task force composed of individuals from more than one law enforcement agency, the lead of the agency overseeing the task force shall determine, in writing, whether and in what circumstances authorized personnel assigned to the task force will use IDVRS.

8.3 Activation

8.3.1 Authorized personnel should record enforcement encounters at the start of the event or as soon as safely possible thereafter. Refer to Section 6.4 for a definition of enforcement encounter.

8.3.2 Authorized personnel shall deactivate the IDVRS once their participation or involvement in the enforcement encounter has concluded.

8.3.3 If the authorized personnel fail to activate his or her camera, the authorized personnel may be required to provide a statement indicating the reason why they failed to activate their camera.

8.4 IDVRS Notice of Recording

8.4.1 Authorized personnel should advise individuals that they are being recorded if it will not interfere with the encounter or officer/agent safety. Otherwise, this notice shall be given as soon as possible and practical.

8.4.2 Authorized personnel have no obligation to stop recording in response to a citizen's request if the recording is pursuant to an investigation, arrest, lawful search, or the circumstances clearly dictate that continued recording is necessary and is consistent with CBP policies on religious, cultural, or privacy considerations.

8.4.3 Authorized personnel should advise other authorized personnel and other agency law enforcement that they are being recorded if it will not interfere with the encounter or officer/agent safety. This will inform the other law enforcement officers' situational awareness and allow them to include this information in any written report.

8.5 Documentation Requirements

8.5.1 Authorized personnel who activate an IDVRS while on duty must document the existence of the recorded data consistent with their office's SOP.

8.5.2 In the case of a failure to record an enforcement encounter, the authorized personnel will log the reason for the failure in the manner outlined by their office's SOP.

8.5.3 In the case of any interruption in recording during a recorded enforcement encounter for reasons other than their participation in the event has concluded, the authorized personnel will log the reason for the interruption as required by their office's SOP.

8.5.4 Interruptions caused or thought to have been caused by a malfunctioning IDVRS should be reported to the authorized personnel's supervisors by the end of shift to ensure that the IDVRS is immediately taken out of service and examined. Every effort should be made to preserve any video that may be recoverable.

8.6 Recording Exemptions

8.6.1 Authorized personnel are not required to activate or continue to record enforcement encounters when any of the following applies, unless engaged in a use of force:

8.6.1.1 They receive a direct order from a supervisor to deactivate the IDVRS for the reasons outlined in, but not limited to, Section 8.7 of this directive. In this case, supervisors who order subordinates to stop recording will document the reason for doing so in a statement or report;

8.6.1.2 The continued recording may compromise officer/agent safety;

8.6.1.3 In the authorized personnel's judgment, a recording would interfere with his or her encounter or may be inappropriate because of the victim's or witness's physical condition, emotional state, age, or other sensitive circumstances (e.g., victim of domestic or sexual violence);

8.6.1.4 A witness is concerned about retaliation if they are seen cooperating with law enforcement (e.g., material witnesses, sources of information); or

8.6.1.5 Recording would risk the safety of a confidential informant or undercover law enforcement officers/agents.

8.7 Prohibited Recording Activity

8.7.1 IDVRS shall not be used to record the following:

8.7.1.1 CBP personnel were doing so is for the sole purpose of conducting or supporting a personnel investigation or disciplinary action;

8.7.1.2 Employee assessments, except for use in the training environment as part of the student/instructor feedback process;

8.7.1.3 CBP personnel during non-enforcement activities, such as actions and conversations of coworkers when not actively engaged in a law enforcement encounter or CBP personnel during briefings, meetings, or roll calls;

8.7.1.4 Privileged communications between CBP personnel and their attorney or union representative;

8.7.1.5 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;

8.7.1.6 In hospitals or to record patients during medical or psychological evaluations or during treatment, unless related to official custodial duties;

8.7.1.7 In non-CBP detention facilities, jail facilities or other law enforcement facilities which prohibit the use of recording equipment; or

8.7.1.8 For the purpose of capturing individuals who are engaged in activity protected by the First Amendment. For example, not recording people who are lawfully exercising their freedom of speech, press, association, assembly, religion, or the right to petition the government for redress of grievances, unless

there is reasonable suspicion to believe that the situation is likely to become hostile or confrontational and evolve into an enforcement action.

8.7.2 Exempt and prohibited activity as defined in Sections 8.6 and 8.7 that is unintentionally captured while recording an activity otherwise required by this policy will not be considered a violation. Authorized personnel shall notify a supervisor when they become aware of an inadvertent recording.

8.8 Video Retention and Storage

8.8.1 All recorded data captured using an IDVRS will be moved to storage and is considered official CBP records information, and as such, must be handled consistent with the National Archives and Records Administration (NARA) records schedule: DAA-0568-2015-0002 and CBP Directive 2110-040.[3]

8.8.2 IDVRS recorded data shall only be stored on a designated CBP-approved system or media. IDVRS recorded data shall not be downloaded or recorded for personal use or posted onto a personally owned device or website.

8.8.3 Unless instructed otherwise, authorized personnel shall ensure that all IDVRS recorded data is moved to storage in accordance with the prescribed storage procedures. If the storage is not complete by the end of the authorized personnel's shift, he or she should notify a supervisor.

8.8.4 Supervisory CBPOs/BPAs/AMAs should ensure that recorded data is stored by the end of each shift, and that all recorded data is correctly categorized and labeled per the office SOP.

8.8.5 When recorded data is placed in storage, each data file must be labeled with the more relevant of the three following categories:

8.8.5.1 Non-Evidentiary: Any recorded data by authorized personnel or their 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 and then destroy non-evidentiary data in accordance with NARA DAA-0568-2015-0002.

8.8.5.2 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.

8.8.5.3 Potentially Evidentiary: Any recorded data that may have material or probative value or may have bearing on any criminal, administrative, civil, or other legal proceeding that is not associated with a case file. These files will be stored for three years on a local network attached storage device.

8.8.6 Before categorizing each data file as described above, CBPOs/BPAs/AMAs and supervisors shall take reasonable steps to determine whether recorded data has investigative or evidentiary value. This cannot always be immediately determined.

[3] Department of Homeland Security, U.S. Customs and Border Protection, CBP Directive 2110-040 Records and Information Management Directive, June 3, 2019.

For example, information which may seem insignificant at the time of recording may subsequently play an evidentiary role in an investigation.

8.8.7 Upon determination that files are evidence or have a high likelihood or degree of potential to become evidence in an evidentiary proceeding, a case file identifier will be assigned within the video management system and retention of the video will be subject to the disposition schedule covering the file.

8.8.8 The IDVRS software or storage mechanism 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 include the following:

8.8.8.1 Automatically logging employee access to a recording, as well as the date, time, and location of access;

8.8.8.2 Require personnel to log the purpose of accessing, viewing, downloading, and disclosing or otherwise distributing recorded data; and

8.8.8.3 Allow offices to only dispose of recorded data as permitted by this directive.

8.8.9 If a hard copy of IDVRS recorded footage is created to aid in an investigation, prosecution or another sanctioned purpose, the footage shall be safeguarded and destroyed as outlined by component SOPs. It is the responsibility of the components utilizing IDVRS to ensure the safeguarding, appropriate labeling, destruction, and accountability of all IDVRS footage extracted from the video management software and copied to a disc, desktop, thumb drive, or any other portable storage device.

8.9 Video Viewing

8.9.1 Authorized IDVRS users should not review IDVRS recorded data prior to writing initial reports of use of force or critical incidents.

8.9.2 CBP component heads may permit the involved personnel to review footage when they are required to give a formal statement about a use of force incident or when they are the subject of an allegation of misconduct or personnel complaint. The CBPOs/BPAs/AMAs shall have the option to review the recordings in the presence of their attorneys or labor representatives.

8.9.3 Authorized IDVRS users may review files in the following instances:

8.9.3.1 To complete criminal investigations and prepare official reports;

8.9.3.2 Prior to courtroom testimonies or for courtroom presentations;

8.9.3.3 For training purposes (with PII redacted); or

8.9.3.4 In preparation for administrative investigations/interviews.

8.9.4 Authorized IDVRS users shall indicate on their reports whether IDVRS data was viewed prior to completing the report.

8.9.5 Recorded data shall not be routinely or randomly viewed by supervisors or other CBP personnel for the sole purpose of identifying policy violations and

disciplining the responsible authorized IDVRS users.

8.9.6 OPR investigators may review IDVRS recorded data in connection with suspected criminal, civil, and administrative allegations and following use of force incidents.

8.9.7 The requirements found in Sections 8.8 and 8.9 in no way relieve authorized IDVRS users from their duty to comply with the provisions of the *CBP Use of Force Policy, Guidelines, and Procedures Handbook* and verbal reporting requirements immediately following a use of force incident.

8.10 IDVRS Training and Use in the Training Environment

8.10.1 CBP offices shall ensure that authorized personnel and other CBP personnel are trained in the use of the IDVRS, the IDVRS policy, and have completed all applicable refresher training, prior to their authorization to use the IDVRS or access IDVRS recorded data. Training shall include the following:

8.10.1.1 Operation, maintenance, and care;

8.10.1.2 Correct handling of recorded data;

8.10.1.3 Privacy and proper procedures for sharing data;

8.10.1.4 Mandatory, judgmental, and non-permissible uses of IDVRS;

8.10.1.5 Training on significant changes in the law pertaining to legal developments; and

8.10.1.6 Additional training to ensure continued effective use of the IDVRS, performance, and to incorporate changes, updates, or other revisions in policies and equipment.

8.10.2 Recorded data captured using IDVRS in the training environment will only be utilized as a part of the student/instructor feedback process. Only authorized CBP instructors will utilize the recorded data for feedback purposes.

8.10.3 Data recorded using IDVRS in the field may be used for training purposes after all PII is removed from the footage.

8.10.4 Data recorded in the training environment will not be placed into official training records.

8.11 Requests for Release

8.11.1 Requests for IDVRS recorded data are subject to all applicable laws, regulations, collective bargaining agreements, and DHS and CBP policies, including but not limited to the Freedom of Information Act, as amended, 5 U.S.C. § 552, and the Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

8.11.2 Any release of IDVRS recorded data external to DHS must be coordinated with the PDO; and depending on the request (e.g., media, congressional, or personnel) must be coordinated with, but not limited to, the Office of the Commissioner, Office of Public Affairs (OPA), Office of the Chief Counsel, OPR, Office of Human Resources Management, Office of Congressional Affairs, and the

impacted operational office(s). As appropriate, DHS HQ offices, including, but not limited to, DHS Office of the General Counsel, DHS Office for Civil Rights and Civil Liberties, DHS Privacy Office (for releases of recordings to members of the media), and DHS OPA may be notified and provided with the IDVRS recording prior to any external release.

8.11.3 Select circumstances allow for the expedited release of footage. The select circumstances in which expedited release can be applied include:

8.11.3.1 A request from the CBP Commissioner; and

8.11.3.2 Where it is determined release is necessary for national security reasons.

8.11.4 For all external releases of IDVRS recorded data, the releasing office must also complete DHS Form 191, Privacy Act Disclosure Record and submit a copy to the PDO.

8.11.5 Any release of IDVRS recorded data to a DHS component or office shall be consistent with DHS policy and the requesting DHS component's or office's need to know.

8.11.6 For any release, CBP personnel from the releasing office shall log the purpose and use for the release of recorded data as designated by their office SOP.

8.12 Unauthorized Disclosure or Access

8.12.1 CBP personnel have the responsibility to immediately report any suspected or confirmed unauthorized disclosure or access, compromise, or loss of IDVRS recorded data to a supervisor, the PDO or the CBP Computer Security Incident and Response Center for review, investigation, and remediation, as necessary.

9 MEASUREMENT. The effectiveness of this program will be measured by annual post implementation review and operational analysis results, a collaborative effort involving AMO, OFO, USBP, OPR, OIT, Operations Support, PDO, and other CBP offices determined by the CBP Commissioner.

10 NO PRIVATE RIGHTS CREATED. This document is for CBP use only, and does not create or confer any rights, privileges or benefits for any person or party.

11 APPROVAL.

Troy A. Miller
Acting Commissioner
U.S. Customs and Border Protection