U.S. DEPARTMENT OF HOMELAND SECURITY
U.S. Customs and Border Protection

CBP DIRECTIVE NO. 1440-036 **EFFECTIVE DATE:** 20 January 2025

ORIGINATING OFFICE: U.S. Customs and Border Protection (CBP), Office of Professional Responsibility
SUPERSEDES: N/A
REVIEW DATE: September 30, 2028

VIDEO MONITORING ACCOUNTABILITY PROGRAM

1. PURPOSE.

The purpose of this directive is to establish the minimum capability requirements and accountability for the authorized use and safeguarding of Video Surveillance Systems (VSS) used by U.S. Customs and Border Protection (CBP) in facilities designated to detain or process migrants.

2. BACKGROUND.

2.1 VSS provides CBP with tactical, live-feed video monitoring and forensic video recordings of CBP employees and contractors while performing law enforcement activities, emergency medical services, and care-in-custody actions in facilities designated to detain or process migrants.

2.2 VSS technology has demonstrated its value to provide tactical, live-feed video monitoring of CBP operations and interactions with the public. VSS also provides both situational awareness and validation of emergency notifications (i.e., intrusion detection systems and duress alarms), thereby contributing to the safety of CBP employees and the public.

2.3 VSS technology has demonstrated its value in establishing facts surrounding a law enforcement encounter with the public. VSS provides evidence of criminal activity, documenting and validating the performance of CBP employees and contractors during interaction with the public and promotes integrity in the execution of the CBP Mission.

2.4 VSS recorded data can only provide limited and visually constrained perspective of an encounter and should only be used to confirm or invalidate other forms of evidence such as, applicable witness statements, interviews and testimonies, forensic analysis, and documentary evidence.

2.5 VSS technology is used to enhance CBP's ability to document and review statements and actions for reporting purposes, congressional oversight, or legal defense for allegations of misconduct or other complaints against the agency. The technology may also be useful to validate the integrity and professionalism of CBP employees and contractors against unsubstantiated accusations, provide evidence in support of criminal prosecutions, and

safeguard the rights of CBP employees and contractors, and the members of the public that CBP serves.

3. SCOPE.

This directive applies to all CBP employees and contractors performing law enforcement duties at, and mission support services for, any facility that is designated to detain or process migrants. This directive also applies to anyone who operates VSS, or accesses video records at facilities designated to detain or process migrants.

4. POLICY.

This directive establishes the authorities for an effective Video Monitoring and Accountability Program (VMAP) to ensure VSS capabilities to support CBP Operations in facilities that detain and process migrants.

Congress directed CBP under Public Law 116-93, Consolidated Appropriations Act, 2020, to report any equipment failure of closed-circuit television (CCTV) or VSS and associated video storage equipment in-excess of 120 hours at any CBP facility with the capability for holding, detaining, and/or processing migrants to the CBP Office of Professional Responsibility (OPR).

In the US House Report 116-458, Department of Homeland Security Appropriations Bill, 2021, the need for effective video monitoring was specifically identified within the US Customs and Border Protection, Title II, Security, Enforcement, and Investigations section, which directed CBP to maintain and preserve all video recordings of any individual who dies in CBP custody until the completion of all related investigations.

The 2024 House Appropriations Bill further expanded the agency's responsibility of oversight of CBP Efforts to Improve Integrity and Accountability which states, "Video Monitoring-In lieu of direction under this heading in the House report and under the heading, "Operating Video Monitoring" in the Senate report, the Commissioner shall ensure continuous video monitoring and recording in CBP facilities that house and process migrants.

(b) (7)(E)

5. AUTHORITIES/REFERENCES.

5.1 Public Law 116–93, Consolidated Appropriations Act, 2020, December 20, 2019.

5.2 Department of Homeland Security Appropriations Bill, 2021, Committee on Appropriations Report, 116-458, September 30, 2021.

5.3 National Institute of Standards and Technology (NIST) Special Publication 800-30 revision 1, Guide for Conducting Risk Assessments.

5.4 The Risk Management Process, an Interagency Security Committee (ISC) Standard, 2021 Edition.

5.5 DHS 4300A Information Technology System Security Program, Sensitive Systems (ITSSP) 2/13/2023 Version 13.3.1.

5.6 US Customs and Border Protection National Standards on Transport, Escort, Detention, and Search (TEDS) policy, October 2015.

5.7 CBP Directive Number 3340-025, Reporting Significant Incidents to the U.S. Customs and Border Protection WATCH.

5.8 Department of Homeland Security Appropriations Act, 2024

5.9 John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115–232) section 889(a)(1)(B)

5.10 CBP Design Standards and Reference Materials (Resource Library for Facility Design Standards and Reference Materials (sharepoint.com))

5.11 CBP Directive No. 2110-040, Records and Information Management Directive

5.12 CBP Directive No. 5510-004-001, Shadow Technology

5.13 CBP Directive No. 5225-03 Rev A, Cost-Wise Readiness

5.14 CBP Handbook 4400-01B, Seized Asset Management and Enforcement Procedures (SAMEPH)

6. DEFINITIONS.

Solely for purposes of this document, the below terms are defined as follows:

6.1 AT-RISK POPULATIONS/AT-RISK DETAINEES: Individuals in the custody of CBP who may require additional care or oversight as determined by applicable CBP policy defining At-Risk individuals. These may include juveniles; unaccompanied children (UAC); pregnant individuals; those known to be on life-sustaining or life-saving medical treatment; those at higher risk of sexual abuse (including but not limited to gender nonconforming, intersex, and transgender); reported victims of sexual abuse; those who have identified mental, physical, or developmental disabilities; those of advanced age; or family units.

6.2 CHAIN OF CUSTODY: CBP personnel must safeguard and protect forensic video records during retrieval, download, and delivery to protect the integrity of the record.

6.3 DETAINEES: Any person, regardless of citizenship or nationality, under arrest, restrained, or confined by CBP.

6.4 DETENTION: Restraint from freedom of movement. Physical restraint is not an essential element of detention.

6.5 EXIGENT CIRCUMSTANCES: Any set of temporary and unforeseen circumstances that requires immediate action to combat a threat to the security or institutional order of a facility or a threat to the safety or security of any person.

6.6 FEDERAL FACILITY: CBP owned or leased building, structure, or the land it resides on, in whole or in part, that is regularly occupied by CBP employees or CBP contracted workers for nonmilitary activities. The term "Federal facility" also means any building or structure acquired by a contractor through ownership or leasehold interest, in whole or in part, solely for the purpose of executing a nonmilitary Federal mission or function under the direction of an agency. Federal facilities include both fixed and temporary facilities. The term "Federal facility" does not include public domain land, including improvements thereon; withdrawn lands; facilities owned and operated by a non-federal government entity (i.e., free space), or buildings or facilities outside of the United States.

6.6.1 FIXED FACILITY: A permanent, generally not movable, building or structure owned or leased by CBP to support mission requirements.

6.6.2 TEMPORARY FACILITY: CBP requires additional capacity to accommodate the processing and holding of non-US citizens crossing the US borders and water-boundaries. Temporary, soft-sided (tent) holding facilities, Forward Operating Bases (FOB) in forward or remote locations, ancillary structures, and equipment are used as temporary facilities for detaining and processing these individuals while other solutions are being developed.

6.7 FORENSIC VIDEO RECORDINGS: Video recordings retrieved as a historical record of incidents and events that may have material or probative value, or may have bearing on any criminal, administrative, civil, or other legal proceeding as part of an ongoing investigation, legal proceeding, administrative action, or other inquiries involving interactions between CBP employees and contractors in the performance of their duties. For purposes of records management, forensic video recordings include both potentially evidentiary and evidentiary records.

6.8 HOLDING FACILITY: A CBP-controlled space, building (or part thereof), set of buildings, structure, secure area, used for temporary confinement of migrants or detainees, or area that was constructed or retrofitted for the purpose of detaining and processing individuals in CBP custody and routinely used for migrant detention. A structure that contains hold rooms, or other secure enclosures must: (a) be under the control of CBP; and (b) primarily used for the short-term confinement of individuals who have recently been detained, or are being transferred to or from a court, jail, prison, other agency, or elsewhere within CBP.

6.9 LAW ENFORCEMENT: Officers or Agents of CBP authorized law enforcement authorities that are responsible for the supervision, control, and processing of migrants or detainees in a holding facility.

6.10 MIGRANTS: Individuals entering a state or territory of the United States from another country or other international boundary.

6.11 PROCESSING: The process of conducting interviews, recording individual responses, and entering required information from migrants into the appropriate electronic system(s) of record by CBP employees and contractors.

6.12 RAPID DEPLOYMENT SYSTEM: A Rapid Deployment Video Surveillance System (VSS) is intended to provide a temporary solution to a lack of video surveillance in migrant holding and processing areas, until a permanent solution can be identified, funded, installed, and fully operational. (b) (7)(E)

6.13 TACTICAL VIDEO MONITORING: Continuous, live-feed monitoring provides real-time situational awareness of current CBP operations. This enables time sensitive notifications, ability to initiate an appropriate incident response, reinforces facility access controls, and awareness for other notifications; when available, tactical video monitoring may also be used to verify emergencies and duress alarms. Tactical video monitoring may be used to supplement other forms of live monitoring of At-Risk individuals but may not be used as the only form of monitoring those individuals.

6.14 VIDEO SURVEILLANCE SYSTEM (VSS): Also known as closed-circuit television (CCTV), VSS is the integration of cameras, recorders, workstations, and monitors that allow the viewing and recording of events. (b) (7)(E)

7. RESPONSIBILITIES.

7.1 The CBP Commissioner, or their designee, has overall responsibility for establishing policy and overseeing all aspects of VSS and recorded data, and to ensure overall oversight and compliance with all applicable laws, policies, and procedures. The CBP Commissioner, or their designee, is also responsible for centralizing acquisition and contractual agreements, identifying funding for installation, maintenance, and lifecycle replacement of VSS, and for defining other CBP operational priorities, requirements, and resources.

7.2 The Executive Assistant Commissioner (EAC) for operational components Office of Field Operations (OFO) and Air and Marine Operations (AMO), and the U.S. Border Patrol (USBP) Chief, are responsible within their respective offices for the following:

7.2.1 Ensuring that needs assessments are conducted to identify the minimum operational requirements necessary to effectively manage physical security, integrity, and operational risks.

7.2.2 Ensuring that authorized personnel with a need-to-know use VSS for official purposes only and in compliance with all applicable laws, policies, regulations, and directives.

7.2.3 Ensuring that authorized personnel are properly trained to use VSS, as well as the correct handling of recorded data prior to issuing or allowing access to the VSS storage.

7.2.4 Ensuring that VSS physical property and equipment are accounted for per CBP Personal Property and Asset Management directives.

7.2.5 Ensuring monthly operational testing of total VSS capabilities to ensure system operational status of tactical and forensic capabilities, minimum clarity requirements to properly document migrant or detainee processing procedures, and minimum VSS storage and retrieval capability are met in accordance with this directive.

7.2.5.1 Maintain a log consisting of monthly testing results to include test date and VSS operational status.

7.2.5.2 Any VSS or component that remains non-working after 24 hours shall be reported as a Serious Incident Report (SIR) to the CBP WATCH.

7.2.5.3 Any VSS or component that has failed will be replaced with like items from the (b) (7)(E) within 24-hours.

7.2.5.4 If replacement is unattainable, the component will consider installing an approved Rapidly Deployable Interim Solution identified in the (b) (7)(E) within 72-hours.

7.2.5.5 If there is no cost-effective solution available in the current (b) (7)(E) the component will identify a r(b) (7)(E) solution and request an immediate OIT determination prior to installation. OIT CTO determination will vet within 5-days.

7.2.5.6 If OIT CTO does not respond within five (5) business days, the component will notify OPR of its intent to install a (b) (7)(E) Rapidly Deployable Interim Solution to meet congressional requirements.

7.2.6 Ensure that video is properly preserved, retained consistent with National Archives and Records Administration (NARA)-approved retention schedules, stored, categorized, and labeled.

7.2.7 Monitor system deployment to ensure that authorized personnel are utilizing VSS correctly.

7.2.8 Coordinate with the Office of Finance to identify funding resources for the installation, maintenance, and lifecycle replacement of VSS.

7.2.9 Coordinate with CAE on complying with reference 5.13 CBP CWR Directive by establishing and achieving minimum required VSS performance outcomes for availability (readiness), minimum ownership costs, optimum reliability, and minimum mean down time.

7.2.10 Ensure that all deployed technologies have a valid and unexpired Privacy Threshold Analysis (PTA) on file with the CBP Privacy Office.

7.3 The CBP Chief Information Officer is responsible for the following:

7.3.1 Support Tier 1 (organization level) and Tier 2 (mission/business process level) VSS operational component risk assessments.

7.3.1.1 VSS operational components conduct Tier 1 and 2 risk assessments to determine if the available communications infrastructure for each location is sufficient to support tactical, live-feed video monitoring, remote access, and retrieval of forensic video records in accordance with this directive.

7.3.2 Conduct and record Tier 3 (information system level) in accordance with National Institute of Standards (NIST) Special Publication 800-30, Guide for Conducting Risk Assessments.

7.3.2.1 Conducting updated Tier 3 risk assessments in the risk management hierarchy whenever significant changes to the system configuration or to the operational or threat environment occur, or every three (3) years, whichever comes first.

7.3.2.2 Providing to all operational components (OFO, USBP, and AMO) a copy of Tier 3 risk assessments completed for each, individual system in their respective office.

7.3.3 Ensuring that the VSS complies with applicable Federal, DHS, and CBP technology requirements and standards.

7.3.4 Ensuring that all hardware and software which will connect to, or be integrated onto, the CBP network are approved and meet necessary standards documented in the DHS 4300A Sensitive Systems Handbook.

7.3.5 Ensuring that all hardware and software proposed for temporary measures comply with CBP Directive 5510-004-001, Shadow Technology.

7.3.6 Ensuring VSS equipment meets CBP standards and is added to the (b) (7)(E) approved for use.

7.3.6.1 OIT will provide components with options listed on the (b)(7)(E) for installation of temporary, rapidly deployable interim solutions to provide comparable coverage and recording capability authorized for use until a permanent solution is fully operational.

7.3.7 Ensuring any VSS storage mechanisms accurately document and retain recorded data in accordance with Federal, DHS, and CBP requirements and standards and comply with CBP records management policies.

7.3.8 Monitoring and reporting to the affected operational component (OFO, USBP, and AMO) the status of repairs and replacement of inoperable systems and components on systems with an approved Authority to Test (ATT) or Authority to Operate (ATO).

7.3.9 Assist program owners in completion of any privacy compliance documentation as required by the CBP Privacy Office for use of privacy sensitive technologies.

7.3.10 Reporting violations of this directive to the OPR Intake Center.

7.4 The CBP Assistant Commissioner for the Office of Facilities and Asset Management (OFAM) is responsible for the following:

7.4.1 Including VSS requirements in the design for all new facilities and for existing facility updates, designations, and/or repurposing facilities designated to detain or process migrants.

7.4.1.1 Obtaining confirmation from operational components that a new or updated VSS is fully tested and operational, including continuous recording requirements (b) (7)(E)
(b) (7)(E)

7.4.1.2 Including specific component requirements in the design guide for any facilities designated to detain or process migrants.

7.4.2 Identifying requirements and prioritize workorders for VSS systems at locations designated for detention and processing.

7.4.3 Monitoring and reporting to the affected operational component (OFO, USBP, and AMO) the status of current projects to repair or replace inoperable VSS or any of its components.

7.4.4 Reporting violations of this directive to the OPR Intake Center.

7.5 The CBP Chief Security Officer/Assistant Commissioner for OPR, is responsible for the following:

7.5.1 Conducting a physical security risk assessment, in accordance with the Interagency Security Committee (ISC) Risk Management Process, to identify the appropriate level of protection required for each specific CBP facility.

7.5.1.1 Incorporating VSS requirements into initial recommendations for Baseline Security Requirements (BSR) during the design phase of a project, or for any facility changes that may impact or affect the existing VSS configuration and its capabilities.

7.5.1.2 In coordination with the CBP Chief Medical Officer, establishing risk criteria that include determining, consistent with applicable policy defining, At-Risk populations, and At-Risk individuals to assist in establishing the appropriate level of protection for facilities designated to detain and process migrants. VSS may be used to supplement other forms of monitoring for At-Risk individuals; however, may not be the only form of monitoring used for those individuals.

7.5.2 Obtaining VSS records and data to support investigations for criminal and administrative allegations, allegations of misconduct, use of force incidents, violation of CBP Integrity Strategy and Core Values, and death-in-custody incidents.

7.5.3 Maintaining the CBP VMAP, reporting data collection procedures from operational components, (OFO, USBP, and AMO), OIT, and OFAM, and maintaining current reports on deficiencies in VSS minimum capabilities requirements identified in this directive.

7.5.4 Providing VMAP reports as required for accountability and provide the Committee on Homeland Security with a monthly update on the operational status of all such video capabilities.

7.5.5 Providing oversight on maintaining compliance with physical security standards in accordance with Interagency Security Committee guidelines.

7.5.6 Providing Office of Acquisitions with physical security compliance standards for temporary migrant holding and processing, such as soft-sided facilities.

7.6 The Assistant Commissioner for the Office of Acquisitions (OA) is responsible for:

7.6.1 Ensuring procurement actions for VSS used in CBP facilities designated to detain or process migrants follow this directive.

7.6.1.1 Incorporating the appropriate provisions and clauses in the Statement of Work for soft-sided facilities in accordance with this directive.

7.6.1.2 Incorporating the appropriate provisions and clauses in the Statement of Work for operational component specific requirements in accordance with this directive.

7.6.1.3 Requiring contract awardee to conduct testing and reporting on the operational status of VSS and provide weekly updates to the Contracting Officer Representative (COR) for systems not in compliance with this directive. The COR or appropriate designee will report any non-operational VSS to the managing operational component (OFO, USBP, AMO).

7.6.2 Reporting violations of this directive to the OPR Intake Center.

8. PROCEDURES.

8.1 Authorized usage: CBP authorizes the use of VSS to collect video and audio, unless otherwise restricted, and recordings of interactions between CBP employees, contractors, guests, visitors, migrants, and detainees within a CBP facility designated to detain and process migrants, according to procedures stipulated in this directive contingent upon critical operational priorities, and the availability of resources. VSS will be used within a CBP facility to record all encounters during arrest, detention, processing, and other activities involving direct contact with migrants or detainees, except when doing so may jeopardize CBP personnel or public safety. CBP acknowledges that there may be situations in which the use of a VSS is impractical and may be an impediment to the public and employee safety.

8.2 Chain of custody: During the retrieval process, CBP personnel must maintain a log of who and when the forensic video records were accessed and disposition of the records. CBP personnel receiving forensic video records, shall acknowledge and accept receipt of the record to the sender.

8.3 Remediation: A remediation plan is required at any CBP facility designated to detain or process migrants if the facility does not have the capability to provide a fully operational VSS and/or associated storage capability more than 24 hours.

8.3.1 Any failure of the VSS and/or its associated storage capability in excess of 24 hours at any CBP facility designated to provide migrant detention and processing must be reported to: (1) OPR VMAP, and (2) SIR to the CBP WATCH.

8.3.2 The remediation plan will utilize available resources to provide temporary, alternate technology solutions, dedicate additional workforce to provide observation and monitoring of migrant detention and processing areas, or relocate migrant detainees to a location with full operational capabilities.

8.3.3 Rapidly deployable interim solutions will be reviewed by OPR and approved by OIT which provide comparable coverage and recording capability are authorized for use until a permanent solution is fully operational.

8.3.4 Exigent circumstances require that temporary measures, such as Body Worn Cameras (BWCs) or portable Digital Video Recorder (DVR) systems, may be used to provide forensic video record of official law enforcement encounters during arrest, detention, processing, and other activities with direct contact to the public within a CBP facility.

8.3.4.1 These temporary measures shall not replace or be used in lieu of a permanent VSS solution within a CBP facility and are only considered as a limited mitigation measure for ensuring that CBP is practicing the highest level of integrity in the execution of our Mission.

8.3.4.2 Use of temporary measures will not delay or impede the installation, repair, or replacement of a permanent VSS.

8.3.4.3 (b) (7)(E)

8.3.4.4 Equipment purchased for temporary measures must be NDAA compliant.

8.3.4.5 Any temporary measures must be listed on the TRM and approved for use.

8.3.5 Remediation plans including all risk mitigation countermeasures implemented to provide alternate technology solutions, as well as identify any assumed risks, will be provided in writing and approved by the designated official for the facility.

8.3.6 When all efforts for remediation of exigent circumstances are exhausted unsuccessfully, the EAC for AMO and OFO, or the USBP Chief may authorize in writing, acceptance of all risks associated with continuing operations for detaining or processing migrants without VSS capability (tactical and/or forensic). This authorization is to be renewed every 30 days from initial date of risk acceptance and must be incorporated into CBP monthly congressional reports.

8.3.7 Record and obtain positive confirmation of all work orders and requests for upgrades or replacements of any non-operational VSS or components.

8.3.8 Reported VSS failures shall be updated weekly, until the VSS is returned to full tactical and forensic capabilities.

9. RECORDS MANAGEMENT.

VSS recorded data, including recorded data captured via temporary measures, shall be stored and retained only on a designated CBP-approved system or storage media. VSS recorded data shall not be downloaded or recorded for personal use or posted onto a personally owned device or uploaded to a website or social media platform. VSS recorded data will only be accessed, downloaded, and disclosed by authorized CBP personnel. Any release of VSS recorded data is subject to CBP policies for public release of information.

System video data on a designated CBP-approved system or storage media (minimum video recording capability) will be maintained for a minimum of 30- days. VSS recorded data captured by body worn cameras (temporary measures) should be destroyed 180 days after the recorded footage is removed from the camera, placed in storage, and labeled as non-evidentiary. For other temporary measures, contact CBP Records and Information Management (RIM) for minimum retention requirements. Forensic video data records retrieved from a VSS will be maintained in accordance with all CBP records management policies.

All other Federal Records generated because of this directive shall be assigned a NARA-approved records retention schedule, placed on the appropriate Component Office File Plan(s), and managed in accordance with CBP Directive No. 2110-040, Records, and Information Management Directive, dated June 2019 and CBP Handbook No. 2100-05B, Records and Information Management Handbook, dated June 2019 (or the successor documents to those policies). System owners, business process owners, record owners, and other relevant stakeholders shall work with CBP's RIM Division to identify and assign records retention schedules to their respective records. Any records not yet assigned a schedule shall be retained and managed indefinitely until such time as a NARA-approved record retention schedule is assigned by CBP's RIM Division.

10. POINT OF CONTACT.

Direct all questions regarding this directive and the requirements it establishes to (b) (7)(E)

11. NO PRIVATE RIGHTS CREATED.

This directive is an internal policy statement of CBP and does not create or confer any rights, privileges, or benefits upon any person, party, or entity.

TERMINATION

This directive remains in effect until September 30, 2028.

12. APPROVAL AUTHORITY.

(b) (6)

Pete Flores (Date)
Senior Official Preforming Duties of Commissioner
U.S. Customs and Border Protection