Privacy Impact Assessment

for the

ICE Use of Body Worn Cameras

DHS Reference No. DHS/ICE/PIA-060(a)

February 14, 2024

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) is implementing its Body Worn Camera (BWC) Program nationwide, by geographic Areas of Responsibility, within the Office of Enforcement and Removal Operations (ERO), Office of Homeland Security Investigations (HSI), and Office of Professional Responsibility (OPR) for ICE Law Enforcement Officers and Agents.[1] The ICE Office of Firearms and Tactical Programs is coordinating the effort among the designated ICE program offices, and is responsible for the training, testing, evaluation, and oversight of the BWC Program. ICE conducted a BWC Pilot to assess workload impacts, time commitments, and logistical challenges. ICE is publishing this Privacy Impact Assessment (PIA) to evaluate the privacy risks associated with full nation-wide deployment of ICE's BWC Program.

Overview

The ICE BWC Pilot was mandated by Congress.[2] House Bill 116-458 (Fiscal Year 2021 Appropriations Bill) directed ICE, in consultation with the DHS Office for Civil Rights and Civil Liberties (CRCL), to design a pilot program for the implementation of body worn cameras. The bill also required ICE and the Office for Civil Rights and Civil Liberties to provide a joint briefing to the Committee detailing the parameters of the pilot no later than 90 days after the date of enactment (around March 28, 2021).

On May 25, 2022, the Administration issued Executive Order 14074[3] to increase public trust and enhance public safety and security by encouraging equitable and community-oriented policing. The Executive Order required federal law enforcement agencies to meet certain standards of effectiveness and accountability by, among other things, requiring federal law enforcement agencies to issue policies with requirements that are equivalent to, or exceed the requirements of the Department of Justice's June 7, 2021, policy, which mandated its law enforcement components develop policies that require their agents to use body worn cameras during certain pre-planned enforcement operations. The Executive Order also requires all federal law enforcement agencies to ensure that their body worn camera policies are publicly posted to promote transparency and protect the privacy and civil rights of members of the public.

---

[1] For the purposes of this Privacy Impact Assessment and pursuant to the ICE BWC Directive, "ICE Law Enforcement Officers and Agents" means ICE personnel authorized by statute to enforce the laws of the United States, carry firearms, and make arrests in the performance of assigned duties. Throughout this document the term "ICE Law Enforcement Officers" will refer to both officers and agents that meet this definition.

[2] U.S. DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS BILL, H.R. 116-458, p. 31, 116th Cong. (2019-2020).

[3] Exec. Order 14074, 87 FR 32945, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety," *available at* https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and.

In furtherance of the BWC Pilot, the ICE Office of Regulatory Affairs and Policy sponsored the RAND Homeland Security Research Division to independently assess ICE's use of body worn cameras. Following completion of the BWC Pilot in March 2023, the RAND Corporation issued *Independent Assessment of the ICE Body Worn Camera Pilot Program*,[4] a final report evaluating the potential operational benefits and shortcomings of incorporating body worn cameras into ICE's enforcement operations. The report also addressed ICE's overall efforts to increase transparency and accountability associated with law enforcement encounters between ICE and members of the public. The BWC Pilot informed ICE on the use of body worn camera technology, the policy issues that needed additional consideration, as well as the impact on operational environments and risk assessments that full implementation entails.

ICE incorporated lessons learned from the BWC Pilot and the independent assessment report in the updated BWC Directive on which this Privacy Impact Assessment is based.[5] ICE will add the new functionalities described below and deploy the BWC Program, enterprise-wide, in a phased approach based on resources. Full implementation is expected by September 30, 2025.[6] This Privacy Impact Assessment will be updated if there are any programmatic changes impacting privacy.

Deploying body worn cameras in ICE enforcement operations can have multiple potential benefits, including:

- Helping to objectively determine what happened during a law enforcement encounter;
- Providing corroborating evidence in arrests and prosecutions;
- Enhancing training capabilities through use of body worn camera recordings as a learning tool;
- Strengthening ICE personnel's performance and accountability;
- Providing an assessment tool to examine use of force incidents; and

[4] Independent Assessment of the ICE Body Worn Camera Pilot Program, Homeland Security Operational Analysis Center (Washington, D.C. 2023). The research was sponsored by ICE and conducted in the Management, Technology, and Capabilities Program of the RAND Homeland Security Research Division, which operates the Homeland Security Operational Analysis Center. The RAND Corporation operates the Center as a Federally Funded Research and Development Center for DHS. The report is *available at* https://www.rand.org/pubs/research_reports/RRA2014-2.html.

[5] While the BWC Pilot used one vendor's body worn camera, it provided ICE with the opportunity to evaluate whether that body worn camera was suitable for all ICE environments, or if other body worn cameras should be considered to support ICE's mission.

[6] The date is subject to change due to the availability of appropriated funding resources and unforeseen events or circumstances that may delay implementation.

- Enabling the quick and immediate review of recordings.

To enable ICE to achieve full implementation in a privacy-preserving manner, this Privacy Impact Assessment describes how personally identifiable information is collected, used, disseminated, and maintained in ICE's BWC Program; the privacy risks associated with such activities and appropriate mitigation measures; issues identified during the BWC Pilot; and technological developments that were unavailable at the BWC Pilot stage.

ICE Body Worn Camera Policy

ICE issued its Body Worn Camera Policy, Directive 19010.2 on January 12, 2024.[7] The Directive outlines the policies for ICE's use of body worn cameras, identifies the responsible parties and details their responsibilities, and establishes operational, retention, storage, and training procedures. Additionally, the BWC Directive establishes several prohibitions and requirements, including the following:

- ICE Law Enforcement Officers must record enforcement activities at the start of the enforcement activity, or, if not practicable, as soon thereafter as safely possible. Once a body worn camera is activated, ICE Law Enforcement Officers should only deactivate the body worn camera when the scene is secure as determined by the supervisor or team lead. *Directive at § 5.5*. If ICE Law Enforcement Officers fail to activate their body worn camera, or if the recording is interrupted, they must document the reason for the failure to activate the camera or the interruption. *Directive at § 5.5.* ICE Law Enforcement Officers must also provide notification if they become aware of any unintentional body worn camera recordings, including prohibited recordings. *Directive at § 5.5.*
- ICE Law Enforcement Officers will orally notify individuals that they are being recorded as soon as practicable and safe to do so, unless doing so would jeopardize the safety of ICE Law Enforcement Officers or any other person.[8] *Directive at § 4.13(8).* This notice should not be construed as a requirement for ICE to obtain consent from the individuals being recorded.
- ICE Personnel[9] are prohibited from intentionally making body worn camera recordings in

[7] The ICE BWC Directive defines body worn camera as an "ICE approved combined audio/video/digital recording equipment combined into a single unit, designed to capture a first-person perspective, which is typically worn on clothing or otherwise secured to a person." *Directive at § 3.3.* This Directive is on file with DHS and ICE Privacy Offices and *available at* https://www.ice.gov/news/releases/ice-announces-updated-policy-body-worn-cameras. This Directive superseded Directive 19010.1: *Interim Policy Authorizing the Body Worn Camera (BWC) Pilot* (*Interim Policy*) (October 2021).

[8] This notification shall be given only when operationally feasible, and with the understanding that the safety of ICE personnel or any other person is of paramount importance in all interactions.

[9] "ICE-Personnel" includes all ICE law enforcement officers and agents authorized to use body worn cameras and other employees and contractors authorized to service the BWC Program sand/or view, review, or redact body worn

places or areas where cameras generally are not allowed or permissible, unless related to an enforcement activity. *Directive at § 5.6.* Prohibited use of a body worn camera includes recording the following types of activities, purposes, or locations:

- Recording an activity if doing so places ICE Law Enforcement Officers or others in a dangerous situation;
- Recording solely to capture individuals engaged in activity protected by the First Amendment of the U.S. Constitution;[10]
- Recording solely to support a personnel investigation, disciplinary action, or employee performance assessment;
- Recording to capture undercover personnel, confidential informants, confidential sources, or any undercover activity;
- Recording within healthcare facilities;
- Recording within court rooms during proceedings;
- Recording any non-enforcement activities, such as actions and conversations of ICE Personnel when not actively engaged in an enforcement activity;
- Recording to capture privileged communications (i.e., statements made by people within protected relationships);
- Recording inside detention facilities or government facilities that otherwise prohibit the use of recording equipment;
- Recording to conduct facial recognition in conjunction with the recording;[11]
- Recording for personal reasons unrelated to official duties; and
- Recording solely to capture a particular individual based on the person's race, color,

camera footage. Solely for the purpose of the ICE BWC Directive and this Privacy Impact Assessment, the definition of ICE personnel may include Task Force Officers on ICE-led Task Forces per Section 5.3 of the ICE BWC Directive.

[10] This prohibition does not preclude use of body worn cameras where ICE Law Enforcement Officers are otherwise addressing unlawful activity, or while engaged in enforcement activities, or if the situation becomes violent, dangerous, or otherwise unlawful and requires the law enforcement officer to take an enforcement action as described in Section 5.4 of the BWC Directive.

[11] While-body worn camera live recordings will not be used simultaneously to conduct facial recognition, ICE may use-still pictures derived from body worn camera video data for facial recognition purposes after the picture has been downloaded into an ICE system of record, in compliance with applicable law, policies, and privacy requirements and protections, and in support of authorized law enforcement activities. For more information about how ICE may use facial recognition services, please *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (2020 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.

religion, national origin,[12] sex, age, disability, sexual orientation, marital status, parental status, personal appearance, gender identity or expression, or political affiliation. *Directive at § 5.6.*

- Enforcement activities where body worn cameras will not be worn or activated include:
  - Where agents are conducting undercover activity or confidential informants will or may be present;
  - Information-gathering surveillance activities where and when an enforcement activity is not planned;
  - Onboard commercial flights; and
  - Custodial interviews conducted inside jails, prisons, detention centers, or ICE owned or leased facilities. *Directive at § 3.7.*
- All recorded data captured by ICE Law Enforcement Officers using ICE issued body worn cameras, whether the data qualifies as evidence, will be maintained and preserved on a designated ICE-approved system or media (described below) and retained in accordance with applicable National Archives and Records Administration records retention schedules.[13] ICE Personnel must take reasonable steps to determine whether a body worn camera recording has investigative or evidentiary value, which includes possible use in civil and/or criminal litigation, and mark the recording appropriately for storage and tracking purposes for future litigation, investigation, and/or for responses to Freedom of Information Act requests. *Directive at § 5.7.*
- Body worn camera recordings are subject to all applicable laws, regulations, and DHS and ICE policies, including, but not limited to the Freedom of Information Act; the Privacy Act of 1974, as amended;[16] and the Non-Disclosure of Information Protected under 8 U.S.C. § 1367. Prior to any external release[14] of body worn camera recordings (other than release pursuant to litigation or in response to Freedom of Information Act requests), the releasing office must complete DHS Form 191, *Privacy Act Disclosure Record*, and submit a copy to the ICE Office of Information, Governance, and Privacy. Release of a recording to a DHS component or office must be consistent with DHS policy, applying all required

[12] These limits, however, do not apply to antiterrorism, immigration, or customs activities in which nationality is expressly relevant to the administration or enforcement of a statute, regulation, or executive order, or in individualized discretionary use of nationality as a screening, investigation, or enforcement factor.
[13] To the extent that an approved NARA records schedule has not been implemented, records must be maintained indefinitely until an approved records schedule has been approved and implemented.
[14] External release is the sharing of information outside of DHS. *See DHS Privacy Policy Directive 047-01-007, Revision 3, Handbook for Safeguarding Sensitive PII*, located at https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

privacy safeguards and affirming the requesting component's or office's need to know.

- In all cases, prior to the public release of body worn camera footage, the ICE Law Enforcement Officer who captured the footage, and any ICE Personnel whose image was captured in the footage, must be notified. Any public release of body worn camera recordings must be coordinated with the ICE Office of Public Affairs. Additionally, releases of body worn camera recordings to Congress must be coordinated through the Office of Congressional Relations. Releases of body worn camera recordings to the media must also be coordinated through the Office of Public Affairs. The specific nature of the release of footage[15] may require coordination with ICE Headquarters Responsible Officials,[16] Office of Firearms and Tactical Programs, Office of the Principal Legal Advisor, Office of Regulatory Affairs and Policy, Office of Congressional Relations, Office of Public Affairs, and the Field Responsible Officials in the impacted operational office(s). If the footage contains officers or agents from outside law enforcement agencies, it may also be appropriate to provide advance notice to the impacted agencies. As appropriate, DHS Headquarters offices including, but not limited to DHS Office of the General Counsel, DHS Office for Civil Rights and Civil Liberties, DHS Privacy Office, and DHS Office of Public Affairs may require notification prior to any external release of body worn camera recordings. *Directive at § 5.11.*

***Training** (Directive at § 5.9)*

ICE Headquarters Responsible Officials and Field Office Responsible Officials will ensure assigned ICE Personnel, including any necessary support staff, are trained on the BWC Program, and have completed all applicable refresher training prior to their authorization to use body worn cameras or to access body worn camera recorded data. Training must occur annually and include:

- Body worn camera operation, maintenance, and care;
- Appropriate handling of body worn camera recordings;
- Privacy compliance and proper procedures for redacting and sharing body worn camera data (e.g., proper labeling and categorization);
- Required wear and activation, optional wear and activation, deactivation, and non-permissible uses of body worn cameras;

[15] Circumstances that may require additional coordination are in Section 5.11 of the ICE BWC Directive. Such instances include, but are not limited to, expedited release in the event of a serious bodily injury or death in custody, as defined in the BWC Directive.

[16] ICE Headquarters Responsible Officials include Executive Associate Directors (EADs); the Principal Legal Advisor; the Associate Director for Office of Professional Responsibility; and the Assistant Directors (ADs), or equivalent positions who report directly to the Director, Deputy Director, or Chief of Staff. *Directive at § 3.9.*

- Officer/agent and public safety considerations when wearing/operating body worn cameras;
- The laws, regulations, and policies governing the use of body worn cameras, including any related updates;
- Proper labeling and categorization of body worn camera footage;
- Civil rights and civil liberties considerations;[17] and
- Any other additional training ICE Headquarters Responsible Officials or Field Office Responsible Officials deem necessary.

Deployment of the Body Worn Camera *(Directive at § 3.6)*

The BWC Program will be implemented in all aspects of ICE law enforcement activities – planned and orchestrated in advance – conducted by ICE Law Enforcement Officers with certain exceptions.[18] Such activities include but are not limited to:

- At-large arrests (i.e., not pursuant to an arrest warrant), including searches incident to such arrests;
- Brief investigatory detentions, including frisks conducted during such brief investigatory detentions;
- Execution of and attempt to execute, criminal and administrative arrest warrants and in-person issuance of subpoenas;
- Execution of and attempt to execute a search or seizure warrant or order;[19]
- Execution of a Removal Order, including removals aboard Special High-Risk Charter Flights[20] and to conduct verification of commercial removal;[21]

[17] This training must be developed in coordination with the ICE Office of Diversity and Civil Rights and DHS Office for Civil Rights and Civil Liberties.
[18] See Section 3.7 of ICE Body Worn Camera Directive 19010.2 for a list of the exceptions. Examples include, but are not limited to, undercover activities, use on-board commercial flights, and custodial interviews conducted inside jails, prisons, detention centers, or ICE owned or leased facilities.
[19] Body worn cameras are deactivated when the scene is secure as determined by the supervisor or team lead on scene. Documentation of search(es) after execution of a warrant will be conducted in accordance with existing guidance for searches, including evidence recovery, and search and seizure.
[20] Special High-Risk Charter Flights are ICE-chartered flights and are distinct from commercial flights where there may be civilians traveling on the same flight as ICE personnel and a non-citizen who is being removed.
[21] Body worn cameras are not authorized for wear or use aboard commercial flights, which are distinct from aircraft chartered by ICE for the purposes of transport and/or removals. Deportation officers will activate the body worn camera while the individual being removed is boarding (e.g., on the jetway to the commercial plane) and deactivate the body worn camera when the individual boards or enters the commercial plane.

- Deployment of ICE Law Enforcement Officers to protect Federal Government facilities;
- Responding to public, unlawful/violent disturbances at ICE facilities, not including activities conducted within ICE detention facilities;
- Interactions with members of the public while conducting the above-listed activities in the field; and
- When responding to emergencies in cases where the officer is already outfitted with a body worn camera as part of the BWC Program. Law Enforcement Officers should not delay in responding to an emergency to outfit themselves with a camera.

ICE Law Enforcement Officers must activate body worn cameras as part of the BWC Program to capture footage of enforcement activities at the start of the activity or, if not practicable, as soon as safely possible thereafter. Once a body worn camera is activated, ICE Law Enforcement Officers should only deactivate it when a supervisor or team lead declares the scene secure. ICE Law Enforcement Officers who fail to activate their body worn cameras must provide a statement explaining, or detail in after-action case summaries or records of encounter, the reason that they failed to activate them. Additionally, ICE Law Enforcement Officers who activate the body worn camera for an enforcement activity are required to document the existence of any recording in any reports about the enforcement activity. Further, ICE Law Enforcement Officers must provide a statement detailing the reason for any interruption in recordings (e.g., body worn camera deactivation, malfunction) during enforcement activities. ICE Law Enforcement Officers must notify their supervisor and the BWC Coordinator if they become aware of any unintentional body worn camera recordings, including prohibited recordings discussed in the BWC Directive, at Section 5.6.

The Body Worn Camera System

The Equipment

The body worn camera system in the ICE BWC Program consists of the camera, the docking station, Digital Evidence Management System (maintained in the cloud) cloud , and the vendor's desktop applications. The cameras are mountable on a variety of clothing and equipment (e.g., jacket, body armor, or helmet). Docking stations charge the cameras and upload footage from the camera to the cloud-based (FedRAMP certified[22]) Digital Evidence Management System.

The body worn cameras used in the ICE BWC Program possess a battery life of approximately 12 hours, have storage capacity sufficient for extended situations, and have a programable pre-event buffer that allows the capture of video prior to activation. The pre-event

[22] FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. *See* https://www.fedramp.gov/.

buffer ensures that the body worn camera captures activities that occur directly prior to the user activating the body worn camera. The buffer is programmed to record 30 seconds of video (not audio). The programmable buffer increases the probability that a recording is captured in its entirety. The buffer is constantly overwritten until the camera is activated. Upon activation, the pre-event buffer video recording becomes the start of the recording at activation. The system does not record when the body worn camera is turned off.

The Digital Evidence Management System

The vendor's web-based Digital Evidence Management System (which manages and maintains the video/audio files) supports ICE Law Enforcement Officers' direct upload of videos; categorization and labeling of videos; and direct sharing of videos with appropriate parties, such as U.S. Attorney's Offices and other law enforcement partners, for use in case development while providing a full chain of custody. It will also include redaction technology for blurring individuals who are not the subject of an inquiry and for redacting any other personally identifiable information incidentally captured within the video (e.g., license plate numbers, bystanders). ICE Freedom of Information Act (FOIA) personnel fully trained on FOIA will apply appropriate exemptions consistent with law, regulation, and/or policy. Finally, the system will be FedRAMP certified, as required by the ICE Office of the Chief Information Officer.

Each ICE user of the Digital Evidence Management System will be assigned a role with specific permissions limiting access to information on a need-to-know basis. The system will have appropriate safeguards and audit trails in place to restrict access to and viewing of recorded data to those with an official need-to-know as described in the BWC Directive. Only personnel with need-to-know have access (e.g., to maintain evidence, redact information, engage in related administrative tasks). Once they are granted need-to-know access, they are given a specific level of access to support their assigned, need-to-know activities. The vendor does not have access to the Digital Evidence Management System unless ICE grants it for support/administrative purposes, as needed. Safeguards include logging whenever ICE Personnel access a recording (including date, time, and location of access), requiring ICE Personnel to note the purpose of accessing or viewing the recorded data, and prohibiting the deletion, editing, or modification of any recording unless expressly permitted by ICE policy, as indicated in the BWC Directive and federal law. *Directive at § 5.1.* The vendor will not be able to view any videos in the system uploaded by ICE; only designated ICE Personnel will have access to view the captured data.

The Evidence Capture/Sync Process

When ICE Law Enforcement Officers activate the body worn camera, the following will occur:

- Video and audio data is captured and stored in encrypted form on the camera; and
- Data upload and synchronization.

- Option 1
  - ICE Law Enforcement Officers place the camera on the docking station at the respective field office.
  - The camera automatically begins to upload recording data and syncs to the ICE-owned, vendor-provided Digital Evidence Management System.
  - Once the footage is uploaded to the Digital Evidence Management System, the data on the camera (including buffer video) is automatically deleted from the camera.
  - ICE Personnel then sign into the Digital Evidence Management System to access the footage and categorize data as appropriate. See below for more information on how data is categorized.
- Option 2
  - ICE Law Enforcement Officers connect the body worn camera to an ICE government-furnished laptop.
  - Then, ICE Law Enforcement Officers use the vendor's application on the ICE laptop to review the video.
    - ICE Law Enforcement Officers will categorize the evidence in accordance with policy, as either "Evidentiary," "Potentially Evidentiary," or "non-Evidentiary," within the application before the captured data is uploaded.
    - ICE Law Enforcement Officers will choose "sync-now" from an ICE protected laptop to upload evidence to the Digital Evidence Management System.
    - As in Option 1, the recording (including buffer recording) is then automatically deleted and removed from the camera.

Data Tagging and Retention of Body Worn Camera Data

All body worn camera recordings will be preserved for the longest retention period applicable to the category of recorded data (as described below). Records will be retained in compliance with applicable National Archives and Records Administration (NARA) approved records retention schedules, FOIA requirements, and litigation holds, if applicable.

ICE Personnel will categorize the recorded data files according to one of the following

applicable categories:[23]

- Non-Evidentiary – Any recorded data during the normal course of ICE personnel's performance of their duties that is determined to have no evidentiary value, such as. accidental recordings. ICE will retain this data for 60 days and destroy non-evidentiary data in accordance with the NARA-approved records retention schedule DAA-0567-2023-0002-0001.[24]
- Potentially Evidentiary – Any recorded data that may have material, probative, or exculpatory value, or may have bearing on any criminal, administrative, civil, or other legal proceeding will be handled consistent with records of evidentiary value and shall be preserved for three years under NARA records retention schedule DAA-0567-2023-0002-0002. If the records do not become associated with a case file, they will be destroyed after three years. If records become associated with a case file, the records will be retained in accordance with the retention requirements of the case file in which they are incorporated.
- Evidentiary – Any recorded data that may have material, probative, or exculpatory value, or have bearing on any criminal, administrative, civil, or other legal proceeding or determined to have a high likelihood of evidentiary value shall be preserved under NARA records retention schedule DAA-0567-2023-0002-0002 for a period of three years. If records become associated with an ICE case file, the records will be retained in accordance with the retention requirements of the case file in which they are incorporated.

The retention period for categories of ICE records is based on NARA Retention Schedules, the Federal Rules of Evidence, Rule 401 (Relevance) (*Directive at § 7.10*), the Federal Rules of Civil Procedure, Rule 37(e), and the Federal Records Act.[25] ICE will update this Privacy Impact Assessment if pending records retention schedules are inconsistent with the information above.[26]

Recordings within the vendor's Digital Evidence Management System are stored and can be retrieved by date/time of recording, personal identifier of the ICE Law Enforcement Officer operating the body worn camera, or the camera's unique serial number. The personal identifier can only be viewed in the Digital Evidence Management System, not on the video itself. Body worn cameras will be assigned on an individual basis and will not be assigned to multiple ICE Law Enforcement Officers at the same time. Cameras may be reassigned when the originally assigned

[23] Supervisors will complete random audits to verify that selected uploaded recordings are correctly categorized and labeled.
[24] NARA's approved records retention schedule for evidentiary and non-evidentiary records is *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-567/daa-0567-2023-0002_sf115.
[25] 44 U.S.C. ch. 31 § 3101 et seq. (Sept. 5, 1950).
[26] Until a records retention schedule is approved, records must be maintained indefinitely by the agency. If the records are subject to a litigation hold, they may not be disposed of under a records retention schedule until the litigation hold has been lifted.

person is no longer a participant in the BWC Program.

All recorded data for which ICE has received a FOIA request will be labeled as potentially responsive to a FOIA request. All recorded data subject to a litigation hold will also be labeled.

The Digital Evidence Management System maintains audit trails for every action taken on body worn camera recordings within the system, starting with the time recording began. In addition, body worn camera software and storage mechanisms 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 as described in the BWC Directive at Section 5.8. Such safeguards will include logging ICE Personnel access to a recording (including date, time, and location of access), requiring ICE Personnel to log the purpose of accessing or viewing recorded data, and prohibiting the deletion, editing, or modification of any recording unless expressly permitted by the BWC Directive and/or law. *Directive at §§ 5.1 and 5.7.*

ICE Law Enforcement Officers are required to upload body worn camera footage after each operation or as soon as practicable but not to exceed 24 hours following an enforcement activity's completion, and correctly categorize and label all uploaded body worn camera recordings within 72 hours after upload.[27] However, if the footage captures a reportable use of force, critical incident, serious bodily injury, or a death in custody, the uploaded body worn camera recording(s) must be categorized and labeled no later than 12 hours[28] after upload. *Directive at § 4.12*.

Viewing Recordings

Pursuant to the BWC Directive, Section 5.8, ICE will permit viewing of body worn camera collected data within DHS/ICE as follows:

By the ICE Law Enforcement Officer of Self-Captured Footage: ICE Law Enforcement Officers are permitted to review their own body worn camera recordings prior to the submission of official reports. ICE Law Enforcement Officers may also review their own body worn camera recordings in the following circumstances:

- Prior to a required formal statement about a use of force incident;
- When they are the subject of an allegation of misconduct or personnel complaint;
- As part of training;
- To complete authorized actions in an investigation, including preparation of official reports

[27] Except where exigent circumstances or the remote location of the activity make doing so impossible. In such cases, upload, categorization, and labeling must be done as soon as practicable.
[28] If the incident is captured on a Special High-Risk Charter Flight, the footage will be uploaded and labeled as soon as practicable on return.

or A-File materials;

- Prior to courtroom testimony, courtroom presentation, or the potential thereof; and
- To prepare for administrative investigations and/or interviews.

Any time an authorized ICE Law Enforcement Officer reviews their own body worn camera recordings prior to completing a report, the report must accurately reflect that fact.

By Other ICE Personnel: Pursuant to the BWC Directive, Section 5.8 (2), ICE Personnel may review others' body worn camera recordings only for auditing, training, and defense of federal litigation. Body worn camera footage may also be viewed if there is an official need-to-know and a responsibility to do so (e.g., FOIA processing) pursuant to Section 4 of the BWC Directive.

Only representatives of the Body Worn Camera Review Group, ICE Headquarters Responsible Officials, Office of Firearms and Training Program, Office of the Principal Legal Advisor, and Office of Professional Responsibility may review an ICE Law Enforcement Officer's body worn camera recording if the recording has been identified as containing evidence of misconduct or an allegation of misconduct.

ICE and DHS Headquarters: ICE Headquarters Responsible Officials, including appropriate ICE Headquarters personnel with an official need-to-know, are permitted to review body worn camera recordings to assess, evaluate, or address any officer action, technological, policy, legal, operational, financial, civil liberties, privacy, or any other issue. In certain circumstances, ICE may share body worn camera recordings with DHS Headquarters personnel (e.g., Office for Civil Rights and Civil Liberties, DHS Privacy Office, Office of the General Counsel, Office of Inspector General) or Department of Justice counsel where appropriate and/or required.

Additional Technology Features

Based on ICE's assessments from the BWC Pilot, the BWC Program at full deployment will include the following additional features.

Desktop Application

- *Third-Party Upload Software*. A desktop application that enables users to easily upload recordings to the Digital Evidence Management System.
- *Video Upload Software*. This software enables the upload of videos from a body worn camera connected to a laptop or computer via USB cable to the Digital Evidence Management System. It also allows users to view recordings and add metadata to recordings (i.e., categorize the recordings).
- *Third Party Video Support.* This software tool allows for easy conversion of outside video

formats to standard formats (e.g., Audio Video Interleave or MP4) and includes video forensic tools (e.g., video timing, enhancement, and key measurements calculator from videos). It can play back hundreds of video file types, significantly expediting the review, analysis, and processing of multimedia evidence. This feature allows the import of third-party video, a requirement for maintaining body worn camera video recorded by task force officers assigned to ICE-lead task forces.[29]

Mobile Applications

The following mobile applications are available for download to authorized ICE phones:

- *Real-time Viewing App*. This mobile application allows a user to view their assigned camera view in real time for optimal camera placement and to replay the most recent video. No video data is stored on the mobile device. This application also contains video categorization tools for immediate video marking within the body worn camera, which assists ICE Personnel while in the field.
- *Camera and Dock Manager App*. This mobile application allows a user to register, assign, and reassign devices. This feature assists the Office of Firearms and Tactical Program's Program Management Office with inventory management. It enables ICE Law Enforcement Officers in the field to register cameras to the Digital Evidence Management System upon receipt of cameras from the vendor instead of having the cameras shipped to the BWC Program Management Office for registration, then shipped again to ICE Law Enforcement Officers in the field. It allows the user to take advantage of near-field communication[30] and quick response codes on physical devices to manage inventory remotely.
- *Global Positioning System Locater App*. This mobile application allows access to Global Positioning System tracking for body worn cameras. It is an officer safety feature that will display an active camera as a blue circle overlayed on a map, and is not used for any other purpose.[31]

Additional Functionalities

- *Video compliance software*. This software assists the administration and oversight of body worn camera usage. The software provides metrics (i.e., the number of recordings, total GB of video, battery life/status) to document camera usage and track recordings. These technical metrics will inform the Office of Firearms and Tactical Program's BWC Program

[29] For additional information on task force participation see the ICE BWC Directive, Sections 3.11, 3.15, and 5.3.
[30] Near-field communication is a short-range wireless connectivity technology that lets near-field communication-enabled devices communicate with each other. It is an extension of RFID technology that relies on radio waves via encryption to transmit data.
[31] The body worn cameras used by ICE also include a live-streaming function, which will not be used by ICE.

Management Office on the resource requirements, including future procurement. It also provides features to assist with maintaining data quality, including a randomized recording review process to check for policy compliance. This application feature is designed to reduce the amount of time the Office of Firearms and Tactical Programs and field coordinators spend reviewing data quality compliance with agency policies and programs. These tools allow ICE to streamline the coordinator's review and enable supervisors to deliver tailored personnel training and feedback to ensure that teams are operating within agency guidelines and policies.

- *Third-Party Video Playback*. This feature allows the conversion and upload of other recording footage that may be in a different format (e.g., different vendor device used by a task force officer)[32] to the Digital Evidence Management System, permitting use of administrative tools such as redaction, transcription, and chain of custody tasks.
- *Redaction*. This feature automatically alerts the user to images such as faces and license plates in videos, which assist ICE Personnel in the review of information for release. For example, ICE FOIA personnel process all requests for information, pursuant to FOIA, and apply all legal exemptions (in the form of redactions). Any redactions made to facilitate release of a BWC recording are made to a copy of the original recording to maintain data integrity of the original recording which remains untouched.
- *Video Transcription*. This feature automatically creates a transcript of any uploaded video and provides transcript search tools (e.g., enter a keyword and the user jumps to that location in the video in which that word is spoken).[33]

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974,[34] 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. Section 222(2) of the Homeland Security Act,[35] 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.[36]

In response to this obligation, the DHS Privacy Office developed a set of FIPPs from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the

[32] Examples of this include but are not limited to non-ICE body worn camera recordings, cell phone recordings, and security video recordings, which are covered by other policies and procedures.
[33] Access to uploaded video and transcript search results is restricted to those with a need-to-know based on the existing permissions of a user's system access. This feature does not allow for additional access.
[34] 5 U.S.C. § 552a.
[35] 6 U.S.C. § 101, et seq.
[36] 6 U.S.C. § 142(a)(2).

information and interactions of DHS.[37] The Fair Information Practice Principles 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 on both programs and information technology systems, pursuant to section 208 of the E-Government Act[38] and section 222 of the Homeland Security Act of 2002.[39] Given the technologies involved, and the scope and nature of their use, ICE is conducting this Privacy Impact Assessment, which examines the privacy impact of the use of body worn cameras and the collection and maintenance of recorded data, as it relates to the Fair Information Practice Principles.

1. Principle of Transparency

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

ICE Law Enforcement Officers will attempt to orally inform individuals at the beginning of an enforcement activity that they are being recorded. However, there may be situations in which providing such notice might compromise enforcement operations, is impractical, may interfere with the officer's and/or a third party's safety, or may inhibit ICE from accomplishing its mission. Additionally, some law enforcement encounters do not provide the opportunity for ICE to notify individuals that their facial image or voice will be or has been recorded. However, ICE Law Enforcement Officers are required to position or affix the body worn camera in a visible location to be easily seen by the subject(s) of the encounter and any bystander. ICE also provides general notice of its use of body worn cameras by the publication of this Privacy Impact Assessment.

Privacy Risk: There is a risk that individuals may not receive appropriate notice that their image and voice may be recorded when they are near a law enforcement encounter, regardless of whether they are a subject of the encounter.

Mitigation: This risk is partially mitigated. According to the BWC Directive, Section 4.13 (8), ICE law enforcement officers should advise individuals they encounter that they are being recorded as soon as practicable and safe to do so, unless doing so would jeopardize the safety of the ICE Law Enforcement Officer or any other person. Notice shall be given only when operationally feasible and with the overarching understanding that safety of ICE personnel or any other person is of paramount importance in all interactions. In addition, a body worn camera is

[37] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[38] Pub. L. 107-347; 44 U.S.C. § 3501 note.
[39] Pub. L. 107-296; 6 U.S.C. § 142.

required to be positioned or mounted visibly on the ICE Law Enforcement Officer. ICE also provides general notice to the public through this Privacy Impact Assessment.

While captured video and audio recordings from a body worn camera clearly identify an individual's face and/or verbal communications, the recordings will not be linked to any personally identifiable information unless the individual is detained beyond brief investigative detention or arrested. In such instances, the associated personally identifiable information would be maintained in an ICE case file, as discussed below under System of Records coverage. The different means by which an authorized individual may search for body worn camera recordings further mitigate any potential privacy risk. They are:

- Personal Identifier - Each body worn camera is randomly assigned a unique serial number and tracked in the Digital Evidence Management System. The camera's serial number and assigned ICE Law Enforcement Officer information (but not the recordings) are logged in ICE's asset inventory system. ICE will not assign a personal identifier that would identify any non-ICE personnel captured in the body worn camera footage in the Digital Evidence Management System.
- System Identifiers - In addition to the unique evidence identification assigned to each recording,[40] the camera serial number may be used to search for recordings. The Office of Firearms and Tactical Programs has created custom metadata fields for the Enforcement Integrated Database Arrest Graphical User Interface for Law Enforcement (EAGLE) event number,[41] Homeland Security Investigations case number, Investigative Case Management System[42] case number, Investigative Case Management System operation plan number, Significant Incident Report number, and FOIA request number.
- Date/Time of the Recording - Body worn camera recordings can be searched by date and time of the recording within the Digital Evidence Management System. This feature is expected to increase the efficiency of the FOIA response process as a request may only indicate minimal information, such as the date and time of the requested recording. No personally identifiable information is used in a date and time search to retrieve the body worn camera recording.

  Additionally, the BWC Program is governed by the following System of Records Notices:

[40] This is a random alpha numeric identifier assigned by the system that is unique to each recording.
[41] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE ENFORCEMENT INTEGRATED DATABASE (EID), DHS/ICE/PIA-015 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-ice.
[42] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), *available at* privacy-pia-ice045a-icm-august2021.pdf (dhs.gov).

- DHS/ALL-003 Department of Homeland Security General Training Records[43] and DHS/ALL-004 General Information Technology Access Account Records System,[44] which include records pertaining to the training of DHS personnel and auditing/accountability logs for DHS Information Technology systems.
- DHS/ICE-008 Search, Arrest, and Seizure System of Records,[45] which covers the collection and maintenance of records pertaining to ICE's arrests of individuals and searches, detentions, and seizures of property pursuant to ICE's law enforcement authorities.
- DHS/ICE-009 External Investigations System of Records Notice,[46] which provides coverage for Office of Homeland Security Investigations case files.
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records System of Records Notice,[47] which covers records documenting ICE's criminal arrests and most of ICE's immigration enforcement activities (e.g., the issuance of immigration detainers, the arrest, charging, detention, and removal of individuals for administrative immigration violations; the search for and apprehension of fugitives; and ICE decisions concerning the grant or denial of parole).
- DHS/ALL-020 Department of Homeland Security Internal Affairs System of Records Notice,[48] which provides coverage for body worn camera recordings sought due to an individual's complaint against ICE.

If body worn camera recordings become associated with an investigation or case file, then the data will be retained and governed by the System of Records Notice(s) that apply to the investigation or case file.

Body worn camera recordings may be disclosed externally (outside of DHS), including, but not limited to other federal, state, or local law enforcement agencies, in accordance with approved DHS and ICE policies and procedures, the Privacy Act, and the applicable System of

[43] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[44] DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792 (November 27, 2012), *available at* https://www.dhs.gov/system-records-notices-sorns.
[45] DHS/ICE-008 Search, Arrest, and Seizure System of Records 73 FR 74732 (December 9, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.
[46] DHS/ICE-009 External Investigations, 85 FR 74362 (November 20, 2020), *available at* https://www.dhs.gov/system-records-notices-sorns.
[47] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, 81 FR 72080 (October 19, 2016), *available at* https://www.dhs.gov/system-records-notices-sorns. This SORN will be updated to include body worn camera recordings as a category of records.
[48] DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014), *available at* https://www.dhs.gov/system-records-notices-sorns.

Records Notices.

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.

ICE Law Enforcement Officers will use body worn cameras to record law enforcement activities as provided in the BWC Directive. Due to ICE's law enforcement and national security missions and the purpose of body worn cameras (i.e., to record law enforcement activities), it is not practical or feasible for ICE to obtain an individual's consent before capturing their image or other information in a body worn camera recording.

The BWC Directive requires ICE Law Enforcement Officers to activate body worn cameras at the start of an enforcement activity or as soon as safely possible thereafter. ICE Law Enforcement Officers should only deactivate a body worn camera when the scene is secure, as determined by the supervisor or team lead. *Directive at § 5.5*. ICE personnel's safety and the safety of the public will always be the primary consideration for use of a body worn camera to capture an enforcement activity. Enforcement activities are often in public areas and may result in the inadvertent recording by a body worn camera of individuals who are not the subject of the law enforcement encounter or other personally identifiable information, such as license plate numbers. When a body worn camera recording is categorized as non-evidentiary, it will only be retained for up to 60 days. Redaction of body worn camera footage will only be done for legal reasons, to safeguard privacy, or to prevent the unauthorized public release of law enforcement sensitive information. As noted previously, redactions are made to a copy of the recording to maintain the integrity of the original footage.

The System of Records Notices listed above describe the procedures through which individuals may request access to and correction of records about them. All or some of the requested information may be exempt from access pursuant to the Privacy Act or FOIA exemptions to prevent harm to law enforcement investigations or interests. For example, providing individual access to such records could inform the target of an actual or potential criminal, civil, or regulatory investigation or reveal investigative interest on the part of DHS or another law enforcement agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

ICE will review FOIA requests for body worn camera recordings on a case-by-case basis and release or withhold records which may be subject to FOIA exemptions, in accordance with the ICE BWC Directive, the applicable System of Records Notice(s), and applicable laws, including,

but not limited to, the Privacy Act of 1974, 5 U.S.C. § 552(a), the Freedom of Information Act, 5 U.S.C. § 552, 8 U.S.C. § 1367, or the Federal Rules of Evidence, Rule 401.

Individuals seeking notification of or access to any of the records covered by this Privacy Impact Assessment may submit a request in writing to the ICE Freedom of Information Act Officer by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

Individuals seeking to correct records maintained in an ICE system of records, or seeking to contest their content, may submit a Privacy Act request in writing to the ICE Office of Information Governance and Privacy by mail:

U.S. Immigration and Customs Enforcement
Office of Information Governance and Privacy Attn: Privacy Unit
500 Street SW, Stop 5004
Washington, D.C. 20536-5004
http://www.ice.gov/management-administration/privacy

All or some of the requested information may be exempt from access/correction pursuant to the Privacy Act to prevent harm to law enforcement investigations or interests.

If an individual believes more than one component maintains Privacy Act records concerning them, the individual may submit the request to the DHS Chief Privacy Officer electronically at https://www.dhs.gov/foia or the address below.

Chief Privacy Officer and Chief Freedom of Information Act Officer
Privacy Office, Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528

Privacy Risk: There is a risk that members of the public may not be able to access ICE body worn camera footage maintained by ICE.

Mitigation: This risk is partially mitigated. ICE will consider individual requests to access and/or correct records. As indicated above, individuals may submit requests to ICE to access, correct, or contest records about them. ICE will consider these requests on a case-by-case basis to determine if release of the information is appropriate under applicable law. As discussed, ICE may be required to withhold records to prevent the compromise of law enforcement investigations or

proceedings. Generally, ICE considers requests to correct a record about an individual, though such a request in the context of body worn camera footage is inconsistent with the purpose of the use of body worn cameras: to record an enforcement activity.

If ICE becomes aware that a recording contains images or audio of individuals that may potentially belong to a special protected class pursuant to 8 U.S.C. § 1367, the recording will be labeled to indicate that it contains information on an individual in a protected class. Any such recording will be appropriately redacted prior to release.

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.

ICE is authorized to collect data through body worn cameras in support of the operations described and pursuant to congressional mandate. Specifically, ICE is authorized to operate the BWC Program under Executive Order 14074, 8 U.S.C. § 1101 *et seq*.; and 19 U.S.C. § 1589a.

ICE authorizes the use of body worn cameras to collect audio and video recordings under the conditions and in accordance with the procedures stipulated in the BWC Directive. ICE Law Enforcement Officers will be required to activate the body worn cameras when engaging in certain enforcement activities, under the circumstances set out in the Directive, including but not limited to *(Directive at § 3.6 (1)-(9))*:

- At-large arrests (i.e., not pursuant to a warrant), including searches incident to such arrests;
- Brief investigatory detentions, including frisks conducted during such brief investigatory detentions;
- Execution of and attempt to execute criminal and administrative arrest warrants, and in-person issuance of subpoenas;
- Execution of and attempt to execute a search or seizure warrant or order;
- Execution of a Removal Order, including aboard Special High-Risk Charter Flights and to conduct verification of Commercial Removal;
- Deployment of ICE Law Enforcement Officers to protect Federal Government facilities;
- Responding to public, unlawful/violent disturbances at ICE facilities, not including activities conducted within ICE detention facilities;
- Interactions with members of the public while conducting the above-listed activities in the field; and

- When responding to emergencies in cases where the Law Enforcement Officer is already outfitted with a body worn camera as part of the BWC Program. Law Enforcement Officers should not delay in responding to an emergency to outfit themselves with a camera.

ICE will use body worn cameras to fulfill its mission, which includes executing preplanned law enforcement activities. Use of body worn cameras is expected to increase officer safety, enhance ICE accountability, and increase transparency to build trust in the communities ICE serves.

Privacy Risk: There is a risk that ICE Law Enforcement Officers may use body worn cameras to record facial and video images outside the scope of an enforcement activity or use the captured recordings for purposes other than what is permitted under the ICE BWC Directive.

Mitigation: This risk is partially mitigated. ICE limits the use of body worn cameras to record enforcement activities that support the ICE mission in accordance with the ICE BWC Directive. Assigned ICE personnel, including any necessary support staff, are trained on the BWC Program, and have completed all applicable refresher training prior to their authorization to use body worn cameras or to access body worn camera recorded data. The appropriate training for users must occur annually and must include the following elements *(Directive at § 5.9):*

- Body worn camera operation, maintenance, and care;
- Appropriate handling of body worn camera recordings, including proper maintenance and disclosure of video;
- Privacy compliance and proper procedures for redacting and sharing body worn camera data (e.g., proper labeling and categorization);
- Required wear and activation, optional wear and activation, deactivation, and non-permissible uses of body worn cameras;
- Officer/agent and public safety considerations when wearing/operating body worn cameras;
- The laws, regulations, or policies governing the use of body worn cameras, including any related updates;
- Civil rights and civil liberties considerations; and
- Any other additional training ICE Headquarters Responsible Officials or Field Office Responsible Officials deem necessary.

Training will include classroom discussion and practical exercises on topics such as proper disclosure, data tagging, operation, maintenance, and care of devices, and privacy, civil rights and civil liberties considerations. All ICE Personnel will be required to certify that they have received

training and that they understand the requirements set forth in the Directive.

ICE field office supervisors are responsible for daily oversight of the program and will review random samples of body worn camera logs created by ICE Personnel under their supervision. Misuse of body worn camera data, including improper recording, improper dissemination, or tampering with data may result in disciplinary action for the ICE employee.

4. Principle of Data Minimization

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

Body worn cameras will be used to record enforcement activities outlined in the ICE BWC Directive except when doing so may jeopardize ICE personnel or public safety. ICE limits body worn camera data collection and retention to recordings that are necessary and relevant to carry out ICE's mission consistent with the ICE BWC Directive and the applicable NARA records retention schedules. ICE policy instructs ICE Law Enforcement Officers to record enforcement activities at the start of the enforcement activity, or as soon as safely possible thereafter, and continue recording until the scene is secure, to ensure transparency of and accountability for ICE operations.

Body worn camera data uploaded and categorized as non-evidentiary will be stored for up to 60 days, and then disposed of in accordance with the NARA approved records retention schedule. All recordings will include automatically generated tags for date, time, and camera identification for ease of retrieval when uploaded. ICE will maintain a record of camera assignments to personnel. If records become associated with an ICE case file, the records will be retained in accordance with the retention requirements of the case file in which they are incorporated.

If a requester seeks body worn camera recordings (whether evidentiary, potentially evidentiary, or non-evidentiary) under the FOIA, ICE will review requests on a case-by-case basis and release or withhold information as appropriate in accordance with Freedom of Information Act requirements.

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

Mitigation: This risk is partially mitigated. ICE will only use body worn cameras per the ICE Directive to record enforcement activities. Misuse of body worn camera data, including improper recording may result in disciplinary action for the ICE employee. If ICE incidentally

captures images of individuals or other identifiers (e.g., license plates) through its use of body worn cameras, that information will only be retained in accordance with NARA-approved records retention schedules and will be redacted as appropriate if ICE releases the recording to an external party.

Privacy Risk: There is a risk that ICE may retain a recording or personally identifiable information for longer than necessary.

Mitigation: This risk is mitigated. Each recording is categorized and labeled within the Digital Evidence Management System as either non-evidentiary, potentially evidentiary, or evidentiary. Supervisors are responsible for verifying that the Law Enforcement Officers' uploaded body worn camera recordings are correctly categorized and labeled within 72 hours after upload,[49] and no later than 12 hours after upload where the footage captured a Reportable Use of Force, Critical Incident, Serious Bodily Injury, or Death in Custody.[50]

Within the Digital Evidence Management System, each of the three categories of records is associated with a NARA retention schedule. The Digital Evidence Management System automatically deletes the recording when the designated retention period expires.

Recordings may also be tagged with an additional label (e.g., "litigation hold"), which prevents the Digital Evidence Management System from deleting the recordings indefinitely until personnel authorized to lift such hold instructs the assigned user (e.g., the Law Enforcement Officers or their supervisor) that the litigation hold label on the recordings can be removed.

The ICE Office of Firearms and Tactical Programs Program Management Office maintains oversight of the Digital Evidence Management System and requires supervisors to conduct regular audits of their offices' recordings to ensure that any recordings that have not been categorized are reviewed and correctly categorized and labeled. Law Enforcement Officers and ICE BWC Program personnel receive training on categorization as part of the BWC Program training. *Directive at § 4.12.*

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.

Body worn cameras cannot be used outside of the enforcement activities specified in the BWC Directive. Appropriate uses include:

[49] Except where exigent circumstances or the remote location of the activity make doing so impossible. In such cases, upload, categorization, and labeling must be done as soon as practicable. *Directive at § 4.12 and 4.13.*
[50] If the incident is captured on a Special High-Risk Charter Flight, the footage will be uploaded and labeled as soon as practicable on return. *Directive at § 4.12.*

- At-large arrests (i.e., not pursuant to an arrest warrant), including searches incident to such arrests;
- Brief investigatory detentions, including frisks conducted during such brief investigatory detentions;
- Execution of and attempt to execute, criminal and administrative arrest warrants and in-person issuance of subpoenas;
- Execution of and attempt to execute a search or seizure warrant or order;
- Execution of a Removal Order, including removals aboard Special High-Risk Charter Flights and to conduct verification of commercial removal;
- Deployment of ICE Law Enforcement Officers to protect Federal Government facilities;
- Responding to public, unlawful/violent disturbances at ICE facilities, not including activities conducted within ICE detention facilities;
- Interactions with members of the public while conducting the above-listed activities in the field; and
- When responding to emergencies in cases where the officer is already outfitted with a body worn camera as part of the BWC Program. Law Enforcement Officers should not delay in responding to an emergency to outfit themselves with a camera.

ICE Personnel are prohibited from intentionally making body worn camera recordings in places or areas where cameras generally are not allowed or permissible, unless related to an enforcement activity. *Directive at § 5.6.* Prohibited use of a body worn camera includes recordings of the following types of activities, purposes, or locations:

- For the purpose of recording an activity if doing so places ICE law enforcement officers or others in a dangerous situation;
- Solely to record individuals engaged in activity protected by the First Amendment of the U.S. Constitution;[51]
- Solely to support a personnel investigation, disciplinary action, or employee performance assessment;
- To record undercover personnel, confidential informants, confidential sources, or any undercover activity;

[51] This prohibition does not preclude use of body worn cameras where ICE law enforcement officers are otherwise addressing unlawful activity, or while engaged in enforcement activities, as defined in Section 3.7 of the BWC Directive, or if the situation becomes violent, dangerous, or otherwise unlawful, and requires the law enforcement officer to take an enforcement action as described in Section 5.4 of the BWC Directive.

- Within healthcare facilities;
- Within court rooms during proceedings;
- Any non-enforcement activities, such as actions and conversations of ICE personnel when not actively engaged in an enforcement activity;
- To capture privileged communications (i.e. statements made by people within protected relationships;
- Inside detention facilities or government facilities that otherwise prohibit the use of recording equipment;
- To conduct facial recognition in conjunction with the recording;[52]
- For personal reasons unrelates to official duties; and
- Solely to record a particular individual based on the person's race, color, religion, national origin,[53] sex, age, disability, sexual orientation, marital status, parental status, personal appearance, gender identity or expression, or political affiliation. *Directive at § 5.6.*

Body worn camera recordings are subject to all applicable laws, regulations, collective bargaining agreements and DHS and ICE policies governing ICE data and operations. As such, ICE may be authorized to disseminate a body worn camera recording outside the agency. This includes, but is not limited to, dissemination to the U.S. Attorney's Office or to partner law enforcement agencies to develop an investigation or prosecution; pursuant to a FOIA request, in response to media requests, and pursuant to Congressional inquiries.

Prior to any external release of body worn camera recordings (other than release pursuant to litigation or in response to FOIA requests), the releasing office must complete DHS Form 191, *Privacy Act Disclosure Record*, and submit a copy to the ICE Office of Information, Governance, and Privacy. Release of a recording to a DHS component or office must be consistent with DHS policy and the requesting Component's or office's need to know. Any public release of body worn camera recordings must be coordinated with the ICE Office of Public Affairs. The specific nature of the release of footage may require further coordination with ICE Headquarters Responsible Officials, Office of Firearms and Tactical Programs, Office of the Principal Legal Advisor, Office of Regulatory Affairs and Policy, Office of Congressional Relations, Office of Public Affairs, and

[52] While-body warn camera live recordings will not be used simultaneously to conduct facial recognition, ICE may use-still pictures derived from body worn camera video data after it has been downloaded into a system of record, in compliance with applicable privacy requirements and protections, and in support of authorized law enforcement activities. System of records are discussed later in this Privacy Impact Assessment.

[53] These limits do not apply to antiterrorism, immigration, or customs activities in which nationality is expressly relevant to the administration or enforcement of a statute, regulation, or executive order, or in individualized discretionary use of nationality as a screening, investigation, or enforcement factor.

the Field Responsible Officials in the impacted operational office(s). If the footage contains officers or agents from outside law enforcement agencies, it may also be appropriate to provide advance notice to the impacted agencies. As appropriate, DHS Headquarters offices including, but not limited to DHS Office of the General Counsel, DHS Office for Civil Rights and Civil Liberties, DHS Privacy Office, and DHS Office of Public Affairs may require notification prior to any external release of body worn camera recordings. *Directive at § 5.11.*

Prior to release pursuant to a FOIA request, trained ICE FOIA personnel will apply FOIA exemptions in the form of redactions within the cloud storage system. The vendor's cloud storage solution automatically records a timestamp and destination email address every time a file is shared with any party, including any individual or entity outside ICE.

When ICE discloses body worn camera data outside DHS, the receiving agency is required to use the body worn camera recording only for the purpose for which ICE disclosed the data, and must return the data to ICE, or destroy the recording after analysis, unless they have independent authority to retain the information. Any ICE personnel who are unsure if body worn camera records can be shared with a party outside DHS should contact the ICE Privacy Unit for guidance to ensure compliance with law, regulation, and policy.

Privacy Risk: There is a risk that the body worn cameras may be used during non-enforcement activities and/or capture prohibited activities.

Mitigation: This risk is partially mitigated. In accordance with the BWC Directive, ICE authorizes the use of body worn cameras to record enforcement activities,[54] and prohibits use in other contexts.[55] For example, ICE Law Enforcement Officers may not use body worn cameras solely to record protected First Amendment activities; within healthcare facilities; within courtrooms during proceedings; to record privileged communications; in places where cameras generally are not allowed or permissible, unless related to an enforcement activity; for the purpose of conducting facial recognition in conjunction with live recording; for personal reasons unrelated to official duties; and solely for the purpose of recording a particular person's race, color, religion, national origin (except in certain circumstances as noted above), sex, age, disability, sexual orientation, marital status, parental status, personal appearance, gender identity or expression, or political affiliation.[56]

Since unauthorized use or release of body worn camera 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.

Privacy Risk: There is a risk that body worn camera recordings may be shared with third

[54] *See* Section 3.6 of the ICE BWC Directive and the discussion above.
[55] *See* Section 3.7 of the ICE BWC Directive and the discussion above.
[56] *See* Section 4.6 of the ICE BWC Directive and the discussion above.

parties for purposes other than the purpose for which the recordings were made.

Mitigation: This risk is partially mitigated. Data requests for body worn camera recorded information is subject to all applicable laws and regulations, ICE and DHS policies, and governing System of Records Notices. The ICE BWC Directive requires the releasing office to complete a DHS Privacy Act Disclosure Record (DHSForm 191) prior to any external release of body worn camera recordings other than release pursuant to litigation or in response to FOIA requests. The receiving agency is required to use the body worn camera recording only for the purpose(s) for which ICE disclosed the data and must return the data to ICE or destroy the recording after analysis unless the receiving agency has separate statutory authority to retain the recording.

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

Mitigation: This risk is mitigated. ICE determines whether the recording has evidentiary value. Recordings determined to have non-evidentiary value will be disposed of within 60 days in accordance with the NARA approved records retention schedule. Additionally, body worn camera recorded data is only disclosed for official purposes in accordance with applicable DHS/ICE policies and legal authorities.

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.

ICE captures data using body worn cameras in real-time to maintain an audio/video record of specified law enforcement activities. ICE uses the recording, in part, to verify what occurred during an enforcement activity.

ICE outlined a standard for camera equipment and recording based on market research and best practices. 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 pre-determined standards are used in the BWC Program. The standards for camera equipment and video recording shall have the following:

- A minimum video resolution of 480p (standard definition);
- Definition configurable to 720p (high definition);
- Video compression of at least H.264.[57] Use the lowest possible amount of compression to

[57] H.264, or MPEG-4 AVC (Advanced Video Calling), is a video calling format commonly used for the recording, compression, and distribution of video content that maximizes quality but minimizes impact on video storage.

maximize the amount of information available;

- Frame rate of at least 30 frames per second; and
- Audio compression sufficient to capture high speech quality.

The Digital Evidence Management System automatically tags the recording with time, date, and camera identification metadata, assists in recording retrieval, and ensures the availability of the recording. Additionally, the evidence management system allows for manual tagging of uploaded recordings by date and time based on the event or type of encounter. Finally, ICE will follow the NARA approved records retention schedule to prevent the over-collection of non-evidentiary recordings and the retention of potentially evidentiary and evidentiary recordings within the applicable record retention schedules.

Privacy Risk: There is a risk that ICE will identify individuals through body worn camera footage and take enforcement action against them based solely on a body worn camera recording.

Mitigation: This risk is mitigated. ICE body worn camera recordings are made during enforcement activities. Any use of body worn camera recordings to support future enforcement activities not associated with the enforcement activity that was the subject of the recording, must be based on the totality of evidence, including, but not limited to ICE Personnel's observations and other relevant and corroborating evidence. ICE Personnel are required to report up their chain of command all potential privacy violations, or any violations of the ICE BWC Directive and ensure that no live body worn camera recordings are used in any facial recognition system or facial recognition queries. *Directive at §§ 4.12, 4.13.*

Additionally, safeguards pertaining to audit trails that restrict access and viewing of records data to those with an official need-to-know, and log the purposes for which a video was accessed include: logging ICE Personnel access to a recording (including date, time, and location of access), requiring ICE Personnel to log the purpose of accessing or viewing recorded data, and prohibiting the deletion, editing, or modification of any recording unless expressly permitted by the ICE BWC Directive. *Directive at § 5.7.*

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.

Recordings on the body worn camera are encrypted at rest and in transit to the Digital Evidence Management System. As discussed previously, body worn camera recordings are uploaded by ICE Law Enforcement Officers, either using the vendor-supplied secure docking station or personal ICE laptop computer, to the Digital Evidence Management System. The

docking station is connected to an ICE local area network and uses a dedicated virtual local area network for device isolation. When the camera is docked in the docking station, it immediately begins synchronizing the recordings to the cloud-based Digital Evidence Management System. Once the sync is complete, the Digital Evidence Management System conducts a hashing validation against the video stored on the body worn camera. If the hash confirms the integrity of the recording, the recording is then deleted from the body worn camera.[58]

When a government-issued laptop is used, the camera is connected via USB cable to the laptop. The ICE Law Enforcement Officer selects which video(s) to upload to the Digital Evidence Management System. Once uploaded, the original recording is automatically deleted from the camera.

The Digital Evidence Management System provides the appropriate role-based access controls within an access-restricted FedRAMP facility. Access to the audio/video data on the system requires a user verification, consisting of two levels of security at each evaluation site: local area network and body worn camera application-level security. Access to the Digital Evidence Management System is restricted by ICE/DHS internet protocol address ranges and user accounts that must be validated within the ICE active directory. Body worn camera application-level security consists of secure containers on the body worn camera devices with trusted device certificates issued by the evidence management certificate authority. Each body worn camera has a unique serial number and is assigned to a one ICE Law Enforcement Officer in the BWC Program. The user must also be authorized to access the Digital Evidence Management System.

ICE prohibits personnel from: (1) tampering with or dismantling a body worn camera, its hardware, or software components; (2) using any other device to intentionally interfere with the capability of the body worn camera; (3) accessing, printing, copying, e-mailing, web-posting, sharing, or reproducing body worn camera recordings without authorization; or (4) deleting, modifying, or disposing of body worn camera recordings unless in accordance with ICE policies and procedures, as well as NARA approved records retention schedules. ICE takes precautions to prevent body worn camera recorded data alteration or deletion to maintain audio/video data integrity and to protect the recorded data. ICE also prohibits body worn camera recorded data from being uploaded onto public servers or social media websites. All ICE Personnel must upload body worn camera data to the designated Digital Evidence Management System after each operation or as soon as practical, but not to exceed 24 hours following completion of an enforcement activity. The uploaded data will be stored within the Digital Evidence Management System for the duration of the period required by an approved NARA records retention schedule and any applicable litigation hold or FOIA requirements. ICE Personnel will label the respective recordings

[58] "Hashing" allows the system to maintain the integrity of the original recordings. Data hashing creates a "forensic fingerprint" that shows that a file is authentic and has not been changed. Hashing is used whether the recording is uploaded via the docking system or remote option.

appropriately and supervisors will randomly verify that ICE Personnel correctly label the recordings in accordance the BWC Directive §§ 4.12, 4.13.

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

Mitigation: This risk is mitigated. ICE mitigates this risk by establishing and implementing role-based access controls preventing ICE Personnel from manipulating or deleting the data directly on the camera or prior to upload to the Digital Evidence Management System. Data will be securely transferred to the Digital Evidence Management System which complies with DHS security requirements. If necessary and appropriate, the ICE Personnel's supervisor will facilitate additional access to parties that have a need to view the information in the performance of official duties.

The body worn camera's associated software is designed with protocols to prevent manipulation or deletion of audio and video recordings. ICE further mitigates this risk by requiring two-factor authentication via a personal identity verification card to log into ICE (or the vendor's) computers. ICE also has additional safeguards and audit trails in place to restrict access to and viewing of recorded data to those with an official need to know. System access is granted on an individual basis, based on a need-to-know, by system administrators. Access to footage is limited by an "evidence hierarchy"[59] within the system. Additional safeguards include automatically logging employee access to a recording, as well as the date, time, and location of access, ensuring that any file manipulation is captured in an audit log. Lastly, prior to the authorization to use body worn cameras or access body worn camera recorded data, ICE Personnel receive appropriate training on their proper use and access. Training includes, but is not limited to body worn camera operation, maintenance, and care; appropriate handling of body worn camera recordings; privacy compliance and proper procedures for redacting and sharing body worn camera data, required wear and activation, optional wear and activation, deactivation, and non-permissible uses of body worn cameras; laws, regulations or policies governing the use of body worn cameras; proper labeling and categorizing of body worn camera footage, and civil rights and civil liberties considerations.[60]

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. The ICE Office of Professional Responsibility is responsible for investigating

[59] For example, an agent has access to only their body worn camera recordings; the agent's first-line supervisor has access to that agent's and the other five agent's video under the supervisor's command; the unit director has access to all videos.
[60] *See* Section 5.9 of the BWC Directive and the discussion above.

criminal and administrative allegations of misconduct.[61] In addition, every ICE 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.

All ICE Personnel participating in the BWC Program will be trained regarding body worn camera operation and care, appropriate handling of body worn camera recordings, privacy safeguards, civil rights and civil liberties restrictions, appropriate and permissible use of body worn camera recordings, and rules of behavior regarding body worn camera use. Training will include classroom and practical exercise on topics such as proper disclosure, data tagging, operation, maintenance, and care of devices, and privacy and civil rights and civil liberties considerations. All personnel will be required to certify that they have received training, and they understand the requirements set forth in the ICE BWC Directive. ICE field office supervisors will be responsible for daily oversight of the program and will review random samples of the body worn camera logs created by ICE Personnel they supervise. Misuse of body worn camera data, including improper recording, improper dissemination, or tampering with data may result in disciplinary action.

Records maintained by ICE may only be disclosed to authorized individuals with a need to know in accordance with their official duties and only for uses that are consistent with the intended purposes of the BWC Program. All information stored in ICE 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.

All recordings captured on the body worn cameras have audit trails of all actions on the recording from the time of capture until deletion. After the evidence is uploaded at the conclusion of an enforcement activity, but no later than 24 hours following the enforcement activity, the audit trails are transferred to the Digital Evidence Management System and managed by the system from that point on. Any attempt to view, delete, tag, download, or any other means of manipulation are captured within the evidence management system audit logs.

ICE will ensure that recordings are properly stored, categorized, and labeled; and that technical guidance is updated to reflect changes to equipment or existing laws, regulations, and

[61] BWC Directive at § 4.12(6); *see also*, ICE Policy 17001.1, *Functions of the Office of Professional Responsibility* (Feb. 3, 2005), and the *ICE Employee Code of Conduct* at § 4.4 (Aug 7, 2012). These documents are on file with the DHS and ICE Privacy Offices.

policies. These updates will be coordinated with all applicable oversight and operational offices. ICE will also monitor system deployment to ensure ICE personnel are using and accessing body worn cameras and recordings correctly. These documented audits will be completed by selecting recorded data at random to ensure it is properly categorized and ensuring that all recorded data determined to be of evidentiary or potentially evidentiary value is properly transferred to ICE law enforcement systems. Additional training will be provided for any corrective measures.

Responsible Officials

Caleb Vitello
Assistant Director
Office of Firearms and Tactical Programs
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Kenneth N. Clark
Assistant Director
Office of Information Governance and Privacy
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Approval Signature

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

_____

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