Privacy Impact Assessment

for the

ICE Pilot on Use of Body Worn Cameras

DHS Reference No. DHS/ICE/PIA-060

November 2, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) is conducting a Body Worn Camera (BWC) Pilot at select field office locations: three within the Office of Enforcement and Removal Operations (ERO) and three within the Office of Homeland Security Investigations (HSI) (collectively, ICE). The ICE Office of Firearms and Tactical Programs (OFTP) is coordinating the effort among the respective ICE program offices, and is responsible for the training, testing, evaluation, and oversight of the Body Worn Camera Pilot. The purpose of the Body Worn Camera Pilot is to examine the operational feasibility of an enterprise-wide Body Worn Camera requirement by identifying the costs and benefits, including workload impacts, time commitment, and logistical challenges associated with implementation. The initial goals of the Pilot are to determine the effectiveness of using Body Worn Camera technology to provide an accurate representation of law enforcement encounters, while allowing ICE field personnel to safely perform their duties. This pilot will be executed in an operational environment; therefore, any data collected in support of enforcement activity during the Pilot will be used to support the mission. ICE is publishing this Privacy Impact Assessment (PIA) to evaluate the privacy risks associated with the potential use of Body Worn Camera technology on a wider scale and to address any issues related to the product selection, collection, retention, and storage of the information collected from Body Worn Camera usage.

Overview

This Body Worn Camera Pilot is mandated by Congress.[1] House Bill 116-458 (Fiscal Year 21 Appropriations Bill) directs ICE, in consultation with the DHS Office of Civil Rights and Civil Liberties (CRCL), to design a pilot program for the implementation of Body Worn Cameras. The bill also requires ICE and CRCL to provide a joint briefing to the committee detailing the parameters of the pilot no later than 90 days after the date of enactment (on/about March 28, 2021). On December 28, 2020, the Fiscal Year 21 Appropriations Bill became law.

Until recently, most federal agencies did not use Body Worn Cameras. As late as October 2019, the Department of Justice (DOJ) typically did not use Body Worn Cameras in its operations, even in task force operations where partner law enforcement agencies had Body Worn Camera

[1] U.S. DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS BILL, H.R. 116-458, p. 31, 116th Cong. (2019-2020) states: "The Committee continues to believe that the use of body-worn cameras would be beneficial for the execution of many ICE operations. To that end, in consultation with CRCL, ICE is directed to design a pilot program for the implementation of body-worn cameras. Not later than 90 days after the date of enactment of this Act, ICE and CRCL shall provide a joint briefing to the Committee that details the parameters of the forthcoming pilot; the metrics for success; a cost and workload analysis; activities and civil liberties concerns that may present challenges; how recorded footage would interface with Freedom of Information Act requirements; specific activities/operations where the use of body worn cameras could compromise undercover criminal investigations; and activities where the use of body-worn cameras would be of particular benefit to the safety and wellbeing of officers, detainees, and the public." *See* https://www.congress.gov/congressional-report/116th-congress/house-report/458.

programs. In November 2019, DOJ initiated a Body Worn Camera pilot program for federally deputized task force officers to use Body Worn Cameras that proved successful. In October 2020, DOJ finalized a formal Body Worn Camera policy for federally deputized task force officers, officially authorizing task force officers across the country to use Body Worn Cameras in certain DOJ operations. On June 7, 2021, the DOJ issued a memorandum directing its components to develop Body Worn Camera policies and submit those policies for review.[2]

The President's Task Force on 21st Century Policing[3] *Final Report*[4] concluded in 2015 that implementing Body Worn Cameras at law enforcement agencies can improve policing practices and build community trust and legitimacy, but cautioned that implementing technologies into policing activities must be built on a defined policy framework with clearly stated purposes and goals. Implementing Body Worn Cameras can give law enforcement agencies an opportunity to fully engage and educate communities in a dialogue about their expectations for transparency, accountability, privacy, and civil rights and civil liberties. The Task Force's *Final Report* came on the heels of events suggesting that equipping law enforcement personnel with Body Worn Cameras could have indicated whether violent encounters between law enforcement agencies and the public were avoidable, whether there was an overreaction on the part of the police, or whether the actions of certain members of the public required forceful police intervention. Body Worn Cameras also may provide an additional perspective to by-stander recordings of law enforcement encounters with members of the public.

Given this backdrop, deploying Body Worn Cameras at ICE can have multiple potential benefits, including:

- Helping to objectively determine what happened during a law enforcement encounter;
- Deterring frivolous allegations and complaints (e.g., evidence contradicting allegations of use of force);
- Enhancing training capabilities through use of Body Worn Camera recordings as a learning tool;
- Contributing to a "civilizing effect" on law enforcement/civilian interactions by reducing

[2] *See* U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL DOJ OIG Releases Report on the Department of Justice Policy on Body Worn Cameras for Law Enforcement Officers (June 24, 2021), *available at* https://oig.justice.gov/news/doj-oig-releases-report-department-justice-policy-body-worn-cameras-law-enforcement-officers.

[3] Exec. Order No. 13684, 3 CFR 13684, Establishment of the President's Task Force on 21st Century Policing (December 18, 2014), available at: https://obamawhitehouse.archives.gov/the-press-office/2014/12/18/executive-order-establishment-presidents.

[4] *See* Final Report on the President's Task Force on 21st Century Policing (Washington, DC, May 2015), *available at* https://www.cops.usdoj.gov/pdf/taskforce/taskForce_Finalreport.pdf.

hostilities between ICE personnel and the public;

- Strengthening ICE personnel's performance and accountability;
- Increasing ICE personnel's awareness and safety by influencing public behavior; and
- Simplifying incident review by enabling the quick and immediate review of recordings.

While the requirements and timelines of this Pilot are being driven by a Congressional mandate, ICE understands that the use of Body Worn Cameras in appropriate circumstances is beneficial to the execution of many of its operations. Body Worn Cameras will enhance service to the community by accurately documenting events, actions, conditions, and statements or allegations made by encountered individuals; it will increase officer safety and agency accountability; and the transparency will increase public trust in the communities ICE serves.

ICE assembled a working group in 2021 to evaluate the feasibility of incorporating Body Worn Camera technologies into the breadth of its enforcement operations. The working group recommended a six-month Body Worn Camera Pilot program to study whether incorporating Body Worn Camera technology into ICE's operations would assist its continued emphasis on transparency and accountability. The Pilot will explore operational issues, such as whether ICE needs to expand the audio and video recording capability to enhance transparency and accountability; it also will allow ICE to assess any record tagging, retention, and storage issues. All Pilot audio/video is first encrypted on the Body Worn Camera device during recording. Upon conclusion of operations, the cameras are docked and the evidence is uploaded to ice.us.evidence.com. This is an ICE-owned FEDRAMP accredited Software as a Service (SaaS) evidence management system (EMS) within an Azure government cloud tenant.

Following completion of the six-month Pilot, ICE will issue a final report evaluating the potential operational benefits, as well as any shortcomings, of incorporating Body Worn Cameras into ICE's enforcement operations. The report is expected to address ICE's overall efforts to increase transparency and accountability associated with law enforcement encounters between ICE and members of the public. While the Pilot will only use one vendor's Body Worn Camera solution, it is an opportunity to evaluate whether this specific solution is suitable for all ICE environments, or if other Body Worn Cameras should be considered to support ICE's mission. In short, the Pilot should inform ICE on the advantages and disadvantages of Body Worn Camera technology, the policy issues that need additional consideration, as well as the impact on operational environments and risk assessments that need to be examined before implementation beyond the Pilot to more widespread usage. An update to this Privacy Impact Assessment will be submitted for any implementation beyond what is described in this Privacy Impact Assessment.

ICE Body Worn Camera Policy

In October 2021, ICE issued Directive 19010.1: *Interim Policy Authorizing the Body Worn*

Camera (BWC) Pilot (*Directive*), governing the use of Body Worn Cameras.[5] The Body Worn Camera Directive outlines the policies for ICE's use of Body Worn Cameras, identifies the various responsible parties, details their responsibilities, and lays out operation, retention, storage, and training procedures. The Directive establishes a number of prohibitions and requirements, including:

- ICE personnel must record Pilot 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 personnel should only deactivate the Body Worn Camera when their participation or involvement in the enforcement activity has concluded. If ICE personnel fail to activate their Body Worn Camera, or if the recording is interrupted, they must provide a statement detailing the reason why they failed to activate the Body Worn Camera or why the recording was interrupted. *Directive at § 5.3.*
- ICE personnel will verbally notify (i.e., provide notice to) individuals that they are being recorded if (or as soon as) it is operationally feasible. *Directive at § 5.3.* This notice should not be construed as a requirement for ICE to obtain consent from the subjects being recorded. The Body Worn Camera will be placed on a visible location on ICE personnel's outerwear (e.g., on vest or helmet) so that individuals can see the Body Worn Camera.
- ICE personnel are prohibited from intentionally making Body Worn Camera recordings in places or areas where cameras generally are not allowed or permissible (e.g., locker rooms, dressing rooms, medical facilities, restrooms, in facilities where recording is prohibited) unless related to an enforcement activity. [6] *Directive at § 5.4.5.* ICE personnel should not record encounters with undercover officers, confidential informants, and cooperating defendants. *Directive at § 5.4.7.*
- ICE personnel should not record in a manner that would infringe on activity protected by the First Amendment (e.g., lawful protests).[7] *Directive at § 5.4.8.*[8]
- Body Worn Cameras will not be used during undercover operations or in situations in which it would pose a risk to officer or public safety. *Directive at § 2.3.*
- Body Worn Camera recordings will not be used for any facial recognition activities.

[5] The ICE Directive defines Body Worn Camera as "Any audio and/or video recording equipment combined into a single unit and typically worn on the authorized ICE personnel's exterior clothing, bulletproof vest, or jacket identifying them as ICE employees during the course of their official duties in order to capture Body Worn Camera recordings." *Directive at § 3.3. This Directive is on file with the DHS and ICE Privacy Offices.*
[6] Interactions between ICE medical providers and patients will not be recorded.
[7] While ICE personnel may be wearing Body Worn Camera during lawful protests, they will only activate the Body Worn Cameras when engaged in a law enforcement activity (e.g., an at-large arrest), and not in a manner that may discourage individuals from exercising their First Amendment rights.
[8] *See also, Department Guidance for Enforcement Action at Protected Areas (Oct. 27, 2021). This Guidance is on file with the DHS and ICE Privacy Offices.*

Directive at § 2.3.

- All recorded data collected or captured using Body Worn Cameras during the Pilot, whether it qualifies as evidence or not, will be stored and preserved on a designated ICE-approved system or media (described below). ICE personnel and Body Worn Camera coordinators must take reasonable steps to determine whether a Body Worn Camera recording has investigative or evidentiary value and mark the recording appropriately for storage and tracking purposes for potential litigation, investigation, and/or for responses to Freedom of Information Act (FOIA) requests. *Directive at § 5.5*.
- Any release of Body Worn Camera recordings external to DHS must be coordinated with the ICE Office of Information Governance and Privacy (OIGP). Certain releases must be coordinated with other impacted operational office(s), such as: DHS HQ offices, including, but not limited to DHS Office of the General Counsel (OGC), DHS Office for Civil Rights and Civil Liberties (CRCL), DHS Privacy Office (PRIV) for releases of recordings to members of the media, and DHS Office of Public Affairs (OPA), who may be notified prior to any external release of Body Worn Camera recordings. *Directive at § 5.8.*

ICE's deployment of Body Worn Cameras is bound by the Body Worn Camera Directive and its requirements, which are discussed in more detail in the privacy analysis portion of this document.

Training

Before the Pilot begins at either the Office of Homeland Security Investigations or Office of Enforcement and Removal Operations locations, all participating ICE personnel who will be using Body Worn Cameras are required to undergo mandatory training (led by the Office of Firearms and Tactical Programs in coordination with the ICE Office of the Principal Legal Advisor (OPLA)) regarding proper use of the devices, adherence to the ICE Directive, legal considerations, and privacy, civil rights, and civil liberties safeguards. This training, which will take place in the Office of Firearms and Tactical Programs' facility in Georgia and Pilot site locations as necessary (identified in the section immediately below), will also include training by representatives of the vendor from which ICE purchased both the physical Body Worn Camera hardware and the cloud-based storage solution (described in more detail below). The participants will be trained in data uploading, storage, retention, and tagging. At the end of the training phase, ICE will issue an interim report, based on the feedback from all who participated in the training (ICE field personnel, attending supervisors, instructors). ICE will retain all training materials, such as books and manuals, in accordance with ICE records retention schedule DAA-0567-2015-0009-0001. In the event the records are subject to a litigation hold, they may not be disposed of under a records retention schedule until notified that the litigation hold has been lifted.

Location of the Body Worn Camera Pilot Program

Following training, ICE expects a total of 110 personnel (not including instructors, supervisors, or administrative personnel) from the six selected field offices to participate in the Pilot (i.e., wear Body Worn Cameras in the course of their enforcement duties). The Body Worn Camera will be mounted on ICE personnel's outerwear (such as the vest, shirt, or helmet), using the manufacturer's attachments. The personnel will be visibly identified as "ICE."

The personnel will be field officers and agents from the following six locations, representing varied environments and different enforcement missions of the Office of Enforcement and Removal Operations and Office of Homeland Security Investigations:

- ERO – Atlanta, Los Angeles, and Salt Lake City;
- HSI – Houston, New York, and Newark.

While the locations listed above are the expected sites of Body Worn Camera field locations, unforeseen events may require ICE to relocate one or more of the planned Pilot sites to a different field location. Further, the camera system or associated software utilized in the pilot may not necessarily be what is ultimately employed in a future, expanded use of Body Worn Cameras at ICE.

Deployment of the Body Worn Camera

The Pilot, which is expected to last approximately six months, will be conducted in a variety of operational environments for ICE encounters and planned enforcement activities, such as:

- At-large arrests, including searches incident to that arrest;[9]
- Investigatory detentions, however brief, including frisks conducted during the detentions;
- Execution of, and attempting execution, criminal and administrative arrest warrants;
- Execution of search warrants, including during the time securing the location to be searched as well as the ultimate search of the location; and
- Questioning of any individual encountered during the above-listed activities in the field.[10]

Homeland Security Investigations will begin its Pilot in mid-November 2021. The Office of Enforcement and Removal Operations' Pilot start date is still to be determined. While the two offices' Pilots will not begin at the same time, each is expected to last for 180 days from the

[9] At large arrests are those made outside of a custodial setting.
[10] However, the video recordings can be used to support any activity in the usual course of enforcement, such as criminal prosecutions where warranted.

respective start date.

Once a Body Worn Camera is activated, ICE personnel may only deactivate the Body Worn Camera after they have left the scene of the law enforcement action being conducted (not when an arrest has been made). ICE personnel who fail to activate their Body Worn Camera must provide a statement detailing the reason why they failed to activate the Body Worn Camera and must also provide a statement detailing the reason for any interruption in Body Worn Camera recordings (e.g., Body Worn Camera malfunctioned). This information will be stored in the vendor's Body Worn Camera evidence management system (described below).

Notice of Recordings

ICE personnel will verbally advise subjects of the law enforcement activity that they are being recorded so long as it does not interfere with the planned, overt enforcement activity or otherwise risk the officer's or the public's safety. Otherwise, verbal notice will be provided as soon as practicable for the overt enforcement activity. Cameras will be positioned in obvious places on ICE personnel, such as on their outerwear, on the chest, or on the helmet, which will allow the public to visually determine if the ICE personnel are using a camera. Individuals whom ICE encounters during the Pilot will not have the opportunity to opt in or out (provide consent) to their image or statements being recorded by the Body Worn Camera, as the ICE Directive requires ICE personnel to record the entirety of the encounter.

Body Worn Camera Privacy, Civil Rights, and Civil Liberties Requirements for Recording

The Directive for the ICE Body Worn Camera Pilot institutes several restrictions on recording individuals. Primary among these purposes is protecting individual privacy, civil rights, and civil liberties. As such, personnel are prohibited from recording any of the activities specifically prohibited by the Body Worn Camera Directive. By policy, ICE also prohibits use of facial recognition systems or technologies derived on or from any video captured by ICE Body Worn Camera.

Equipment and Uploading Data for Storage

The Equipment

The Body Worn Camera system consists of the camera, the docking station, the software as a service evidence management system/software, the cloud with storage, and the vendor's desktop application. The initial purchase from the vendor for the Pilot program will include 240 cameras able to be mounted on outer clothing (e.g., jacket, body armor, or helmet), docking stations, and a cloud-based (FedRAMP certified) evidence management system.

The Body Worn Camera equipment will be able to capture what the eye can see in reduced light environments; possess battery life commensurate with the average ICE workday; have storage capacity sufficient for extended situations; and have a programable pre-event buffer that

allows the capture of audio and video prior to activation. This buffer is constantly overwritten until the camera is activated. Upon activation the pre-event buffer video recording becomes the start of the evidence at activation. When a Body Worn Camera is activated, up to 60 seconds of video (not audio) will be captured directly before activation. Buffering mode starts only after the Body Worn Camera is turned on. The system does not record when the camera is turned off.

The Evidence Management System

The vendor's web-based evidence management system (which is the component that manages the video/audio files and permissions within ice.us.evidence.com) will allow for ICE personnel's direct upload of videos; tagging and labeling of videos; and direct sharing of videos with appropriate parties, such as the U.S. Attorneys' Offices and other law enforcement partners, for use in case development while providing a full chain of custody. It will also have redaction technology within the system for blurring individuals who are not the subject of an inquiry and for redacting any other PII incidentally captured within the video (e.g., license plate numbers).[11] ICE personnel who use this system will be fully trained on redaction procedures to ensure that ICE does not release information to external parties outside the bounds of the law, regulation, or policy. Finally, the system will be FedRAMP certified, as required by the ICE Office of the Chief Information Officer (OCIO).

Each ICE user of the evidence management system will be assigned a role with specific permissions limiting access to information on a need-to-know basis. The storage system will have appropriate safeguards and audit trails in place to restrict access and viewing of recorded data to those with an official need-to-know as described in the Body Worn Camera Directive. Only personnel with need-to-know have access (e.g., to create evidence, redact evidence, administration). 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 unless ICE grants it for support purposes at the time of need. Such safeguards will include: logging which ICE personnel access a recording (including date, time, and location of access), requiring ICE personnel to note the purpose of accessing or viewing recorded data, and prohibiting the deletion, editing, or modification of any recording unless expressly permitted by ICE policy. Vendor personnel 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.

[11] Accidental/incidental recordings will be deleted at the end of the 180-day Pilot unless the recordings occurred less than 60 days before the end of the Pilot. The National Archives and Records Administration specifies such records be kept for 60 days. Therefore, if accidental/incidental recordings took place 10 days before the end of the Pilot, it will not be deleted at the end of the Pilot but will be kept for the full 60-day retention requirement under the National Archives and Records Administration records retention schedule.

The Evidence Capture/Sync Process

Once ICE personnel activate the Body Worn Camera, the following will occur:

- Video data is captured and stored in encrypted form on the camera.
- Data upload and synchronization
    - Option 1
        - ICE personnel dock the camera by placing the camera on the docking station at the field office.
        - The camera immediately begins to upload and syncs to the ICE-owned, vendor-provided software as a service evidence management system.
        - The evidence management system confirms data integrity by comparing the hashing checksum. If the checksum passes the evidence management system, it then automatically deletes and removes the data from the camera.
        - ICE personnel will then go to ice.us.evidence.com to tag data as appropriate.
    - Option 2
        - ICE personnel connect the Body Worn Camera to an ICE government-furnished laptop.
        - Then, using the vendor's application on the ICE laptop to review the video:
            - ICE personnel will tag the evidence per Directive.
            - ICE personnel will either choose to sync-now from an ICE protected laptop or dock the Body Worn Camera to upload evidence to the evidence management system.

Data Tagging and Retention of Body Worn Camera Data

All Body Worn Camera recordings will be preserved during the pendency of the Body Worn Camera 180-day Pilot in order to ensure ICE has adequate data to inform the outcome of the Pilot. During the course of and after the conclusion of the Body Worn Camera Pilot, and in the preparation of the final report, records will be retained in compliance with the applicable National Archives and Records Administration approved records retention schedule, FOIA requirements, and any litigation holds, if applicable. Any records for which the retention period is shorter than the Pilot's duration (i.e., non-evidentiary material) will be disposed of in accordance with the applicable records retention schedule.

After the issuance of the Body Worn Camera Pilot final report, all records will be maintained in accordance with an approved National Archives and Records Administration records

retention schedule and any applicable litigation or FOIA hold. *Directive at § 5.5.*

ICE personnel will label the recorded data files according to one of the following applicable categories:

- 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. Accidental recordings are considered non-evidentiary. ICE will retain this data for 60 days (or for the pendency of the Pilot, whichever is longer), and subsequently destroy non-evidentiary data in accordance with the National Archives and Records Administration (National Archives and Records Administration) – approved records retention schedule DAA-0567-2021-0001.
- Evidentiary – Any recorded data that may have material or probative value, or may have bearing on any criminal, administrative, civil, or other legal proceeding. Files determined to have evidentiary value shall be preserved under established rules of evidence, the National Archives and Records Administration records retention schedule applicable to the associated case file, and in accordance with the Federal Records Act.

The categories for ICE records are retained based on National Archives and Records Administration Retention Schedules, the Federal Rules of Evidence, Rule 401 (Relevance) (*Directive at § 7.8*) and the Federal Rules of Civil Procedure, Rule 37(e) (*Directive at § 7.7*), and the Federal Records Act. During the Pilot, ICE will also consider the handling of data that may not fall in either of the two primary categories (non-evidentiary or evidentiary) at the time of tagging, specifically the handling of any information collected that may be "potentially" evidentiary, but whose evidentiary significance is not yet known. When a recording is tagged as "potentially" evidentiary in nature, such recording will be handled consistent with "evidentiary" recorded data requirements. ICE will update this Privacy Impact Assessment to the extent records retention schedules are approved by National Archives and Records Administration.

Generally, agency records must be maintained in accordance with an applicable National Archives and Records Administration General Records Schedule or a National Archives and Records Administration-approved agency-specific records retention schedule. If the records are not subject to a records retention schedule, they must be maintained indefinitely by the agency. In the event the records are subject to a litigation hold, they may not be disposed of under a records retention schedule until further notification. For purposes of the Body Worn Camera Pilot, the recorded data deemed to have evidentiary value or potentially evidentiary value will be maintained indefinitely until an approved National Archives and Records Administration records retention schedule is established.[12]

[12] ICE is also working to develop additional, secondary tags beyond the Evidentiary vs. Non-Evidentiary distinction. Once these tags are finalized, ICE will update this Privacy Impact Assessment accordingly.

Recordings within the vendor's system will not be stored or retrieved by personal identifier. Rather, the cloud storage solution will automatically assign a unique video identification number to each video file when the file is uploaded to the system. That identification number will be associated with a Body Worn Camera and a date/time of recording, but not to an individual user of the device. A separate spreadsheet of which agent/officer is assigned a Body Worn Camera at a given time will be maintained by ICE personnel to assist with tracking. It should be noted that a Body Worn Camera may be assigned to multiple ICE personnel for a variety of reasons (e.g., individual ends employment with ICE or moves to a field office outside the Body Worn Camera Pilot location).

All recorded data for which ICE has received a FOIA request will be tagged as having received a request under FOIA and assigned a case number. All recorded data for which DHS/ICE has received notice of any litigation will also be tagged as having a "litigation hold," and assigned a case number.

The evidence management system has audit trails for every action taken on the video evidence, starting with the time it was recorded. In addition, Body Worn Camera software or 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. 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. *Directive at § 5.5.*

Once ICE personnel appropriately categorize a recording as "Evidentiary" or "Non-Evidentiary," the captured data will be uploaded to the vendor's FedRAMP-certified cloud software as a service evidence management system. This is done by ICE personnel at the end of their shift.

Viewing of Recording

ICE will permit viewing of the Body Worn Camera collected data as follows:

Authorized ICE personnel participating in the Body Worn Camera Pilot are generally permitted to review their own Body Worn Camera recordings when submitting official reports. Authorized ICE personnel may review their own Body Worn Camera recordings in the following circumstances:

- To complete authorized actions in an investigation, including preparation of official reports or A-File materials;
- Prior to courtroom testimony, courtroom presentation, or the potential thereof; and
- To prepare for administrative investigations and/or for interviews.[13]

[13] Body Worn Camera recordings will not be created in the field for the purposes of training. The only permissible

In all instances where authorized ICE personnel participating in the Body Worn Camera Pilot reviewed their own Body Worn Camera recordings prior to completing a report, the report must reflect that fact. *Directive at § 5.6.*

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974,[14] 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 PII. Section 222(2) of the Homeland Security Act,[15] 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.[16]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[17] 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[18] and section 222 of the Homeland Security Act of 2002.[19] 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 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 bedescribed in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

During the Pilot, ICE personnel will attempt to verbally inform individuals at the beginning of the law enforcement-related encounter that they are being recorded. However, there may be situations in which providing verbal notice might compromise enforcement operations, is

viewing of recording for training purposes during the Pilot will be video recorded in a specific training environment for the purposes of training.

[14] 5 U.S.C. § 552a.

[15] 6 U.S.C. § 101, et seq.

[16] 6 U.S.C. § 142(a)(2).

[17] 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.

[18] Pub. L. 107-347; 44 U.S.C. § 3501 note.

[19] Pub. L. 107-296; 6 U.S.C. § 142.

impractical, may interfere with the officer and/or a third party's safety, or may inhibit ICE from accomplishing its mission. 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 personnel are required to position or affix the camera in a visible location (i.e., on their outer clothing/armor/helmet), so the Body Worn Camera can be easily seen by the subject(s) of the encounter. ICE also provides general notice of its use of Body Worn Cameras by the publication of this Privacy Impact Assessment. For purposes of the Body Worn Camera Pilot, System of Records Notice (SORN) coverage is as follows:

Body Worn Camera recordings captured during the Pilot (and maintained in the vendor's evidence management system) are retrieved by the camera ID number, which is not necessarily linked to a specific agent or officer. Because this information is not retrieved by personal identifier, a SORN is not required.

After the Pilot, if ICE determines that Body Worn Camera recordings must be retrieved by a personal identifier, ICE will update the DHS/ICE-008 Search, Arrest, and Seizure Records System of Records Notice,[20] 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. ICE will update the System of Records Notice to incorporate Body Worn Camera video recordings as a category of records.

Records contained in the tracking and auditing documentation associated with the pilot program are retrievable by personal identifier and are covered under DHS/ALL-003 Department of Homeland Security General Training Records,[21] and DHS/ALL-004 General Information Technology Access Account Records System,[22] which outline, respectively, the training of DHS personnel, and auditing/accountability logs for DHS IT systems.

If Body Worn Camera recorded data becomes associated with an individual's investigation or case file, then the data will be retained and governed by the SORN(s) that apply to such investigation or case file. The DHS/ICE-009 External Investigations SORN[23] would provide coverage for Office of Homeland Security Investigations case files, while the DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records System of Records Notice[24] would cover Office of Enforcement and Removal Operations records.

If the Body Worn Camera recording is sought due to an individual's complaint against an officer or agent, then the DHS/ALL-020 Department of Homeland Security Internal Affairs

[20] DHS/ICE-008 Search, Arrest, and Seizure Records SORN, 73 FR 74732 (December 9, 2008).
[21] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).
[22] DHS/ALL-004 General Information Technology Access Account Records System, 77 FR 70792 (November 27, 2012).
[23] DHS/ICE-009 External Investigations, 85 FR 74362 (November 20, 2020).
[24] DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records, 81 FR 72080 (October 19, 2016).

System of Records Notice,[25] would provide coverage.

Privacy Risk: There is a risk that individuals may not receive adequate notice that their images and voice communications may be recorded when they are in close proximity to a law enforcement encounter, regardless of whether they are directly or indirectly involved.

Mitigation: This risk is partially mitigated. ICE personnel generally attempt to provide verbal notice at the onset of an encounter when possible. In addition, Body Worn Cameras are required to be positioned or mounted in highly visible locations on the ICE personnel's outer clothing. However, given the unpredictability of law enforcement interactions or encounters, there may be times when providing notice is impractical, impossible, or jeopardizes the safety of ICE personnel or third parties. Therefore, ICE also provides general notice to the public through this Privacy Impact Assessment.

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 personnel will use the Body Worn Cameras to record law enforcement activities involving members of the public. Due to ICE's law enforcement and national security missions, requiring ICE to obtain an individual's consent before ICE's capture of their image or other information in a video recording is not practical or feasible, and is not necessary for this Pilot's evaluation of Body Worn Cameras.

During the Pilot, the Body Worn Camera Directive requires ICE personnel to only use the Body Worn Cameras to capture law enforcement encounters between authorized, on-duty uniformed ICE personnel and members of the public. ICE personnel's safety and the safety of the public will always be the primary consideration, even when using the Body Worn Cameras. ICE personnel are instructed to continue recording until the law enforcement-related encounter ends, subject to certain specified exceptions. These interactions are often in public areas and may result in the capture of individuals besides those who are the subject of the law enforcement encounter. In the event that ICE inadvertently captures the image of an individual who is not the subject of an encounter or other PII (e.g., license plate number) through its use of Body Worn Cameras, ICE will blur and redact those images prior to making any external disclosure Any video recording recorded during an operation within the scope of the Directive may be used as evidence to support the enforcement activities of Office of Enforcement and Removal Operations' mission.

Individuals can look to the System of Records Notice(s) listed above to determine the

[25] DHS/ALL-020 Department of Homeland Security Internal Affairs, 79 FR 23361 (April 28, 2014).

appropriate procedures to obtain access to and correct their requested record(s). All or some of the requested information may be exempt from access pursuant to the Privacy Act and FOIA in order to prevent harm to law enforcement investigations or interests. Providing individual access to these records could inform the target of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another 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 requests for Body Worn Camera recordings on a case-by-case basis and release records, as appropriate, in accordance with the ICE Body Worn Camera Directive, the applicable SORN(s), and other applicable laws.[26] The ICE FOIA Unit may redact any portion of recordings that are protected or exempted from release under applicable statutes and regulations, including 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 and access to any of the records covered by this Privacy Impact Assessment may submit a request in writing to the ICE FOIA 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 contained in a system of records, or seeking to contest its 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 correction pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests.

If an individual believes more than one component maintains Privacy Act records

[26] Any release of Body Worn Camera recorded data external to DHS must be coordinated with the ICE Privacy Office and depending on the request, coordinated with, but not limited to: the impacted operation office(s), Office of the Commissioner, Office of Public Affairs, Office of Chief Counsel, Office of Professional Responsibility, Office of Human Resources Management, and Office of Congressional Affairs. The appropriate DHS Headquarters offices must be notified and provided the Body Worn Camera recording prior to any external release. *Directive at § 5.8.*

concerning him or her, the individual may submit the request to the Chief Privacy Officer, electronically at https://www.dhs.gov/dhs-foia-privacy-act-request-submission-form 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 or modify their records given the law enforcement nature of the activities captured in the audio and visual recordings.

Mitigation: This risk is partially mitigated. ICE will consider individual requests to determine whether an individual can access records about themself. As indicated above, individuals can submit requests to ICE to access, correct, or contest their records per the instructions listed above. ICE will consider these requests on a case-by-case basis to determine if release of the information is appropriate under applicable law. Further, ICE will also consider requests to correct an individual's record if the individual provides ICE with information that ICE maintains inaccurate records. This will help ensure data quality and accuracy, and will increase the likelihood that ICE is using the most current data in furtherance of its mission. However, there remains some risk to access, given ICE may be required to withhold records to prevent the compromise of law enforcement investigations or proceedings.

Privacy Risk: There is a privacy risk to individuals who are in the range of the recording device but not direct participants in any interactions with ICE, and their images or voices may be captured without notice or opportunity to opt out of the collection.

Mitigation: This risk is partially mitigated. In accordance with the Body Worn Camera Directive, ICE personnel should advise individuals that they are being recorded, if it will not interfere with the encounter or the safety of ICE personnel or members of the public.[27] Any recordings that are extraneous and do not become associated with case files will be labeled non-evidentiary and will be retained for the pendency of the Pilot (180 days) and disposed of in accordance with the applicable National Archives and Records Administration approved records retention schedule. Under FOIA, faces of officers and any uninvolved bystanders will be blurred or redacted as appropriate. Only the face(s) of the subject(s) of the encounter and ICE personnel directly involved in the encounter is appropriate to release. These actions reduce the risk that ICE will capture and retain images of individuals who are incidentally in the area of recording.

[27] *Directive* at § 5.3.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which allows for the collectionof PII and specifically articulate the purpose or purposes for which the PII is being collected andhow 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 recorded data from audio and video recordings in support of the operations described, and in response to congressional mandate. Specifically, ICE is authorized to operate the Body Worn Camera Pilot under H.R. Rep. 116-458; 8 U.S.C. § 1101 et seq.; 8 U.S.C. § 1357; and 19 U.S.C. § 1589a.

ICE authorizes the use of Body Worn Camera to collect audio and video recordings of interactions between ICE personnel and the public under the conditions andin accordance with the procedures stipulated in the Body Worn Camera Directive. ICE personnel in the Body Worn Camera Pilot offices (excluding covert or undercover activities) will be required to activate the Body Worn Cameras when engaging in certain ICE enforcement activities, under the circumstances set out below, including:

- At-large arrests, brief investigatory detentions, and searches incident to arrest;
- Executing, or attempting to execute, criminal and administrative arrest warrants;
- Executing search warrants, including while securing the location to be searched as well as the ultimate search; and
- Questioning of any individual encountered during the above-listed activities in the field.

ICE will use Body Worn Cameras to fulfill the goals of the Pilot, which include:

- Assessing the suitability and effectiveness of a Body Worn Camera solution offered by the vendor for ICE's operational environments;
- Enabling ICE to collect and analyze data to assess the overall operational feasibility of Body Worn Cameras in ICE's enforcement activities; and
- Assessing the additional training necessary for the potential long-term deployment of Body Worn Cameras, including training on the procedures for retention and storage of information collected by the Body Worn Cameras.

Privacy Risk: There is a risk that ICE personnel may record facial and video images outside the scope of a law enforcement encounter, or use the captured images for purposes other than what is permitted under the ICE Directive.

Mitigation: This risk is mitigated. ICE limits recordings to official law enforcement encounters that support the ICE mission and are consistent with ICE policy, in accordance with

the ICE Body Worn Camera Directive. All ICE personnel participating in the Body Worn Camera Pilot will be trained regarding Body Worn Camera operation and care, appropriate handling of Body Worn Camera evidence, privacy procedures, civil rights and civil liberties restrictions, appropriate and permissible use of Body Worn Camera evidence, and rules of behavior regarding Body Worn Camera use. Training will include classroom and practical exercises. All personnel will be required to certify that they have received training and they understand the requirements set forth within the Directive. ICE field office supervisors will be responsible for daily oversight of the program and will review the 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.

To the extent any recording does not involve an activity authorized under the Directive, it will be considered "non-evidentiary." However, it will still be stored for the pendency of the Pilot, and then disposed of in accordance with a National Archives and Records Administration approved records retention schedule. Non-evidentiary data collected during the Pilot will be retained for 60 days or the pendency of the Pilot, whichever is longer, in accordance with the National Archives and Records Administration approved records retention schedule, and will not be entered into any hard copy case file or electronic case management system. ICE will copy and retain information from Body Worn Camera only when it is considered evidentiary or potentially evidentiary or relevant to an active case file for law enforcement or security purposes. ICE will not use any facial recognition technology on Body Worn Camera recordings. Further, ICE will not associate the recorded video or other data with an individual unless the individual is later apprehended or otherwise identified as part of a law enforcement investigation or other administrative or judicial action.

4. Principle of Data Minimization

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

Body Worn Cameras will be used to record official law enforcement encounters outlined in the ICE Directive except when doing so may jeopardize ICE personnel or public safety. ICE seeks to limit Body Worn Camera data collection and retention to recordings that are necessary and relevant to carry out ICE's mission and to support the goals outlined in the ICE Directive. ICE policy instructs personnel to record enforcement encounters at the start of the event, or as soon as safely possible thereafter, and continue recording until the encounter has concluded to ensure transparency and accountability of ICE operations.

For the duration of the Pilot, Body Worn Camera data uploaded and categorized as non-

evidentiary will be stored pending completion of the Pilot, and then disposed of in accordance with the National Archives and Records Administration approved records retention schedule. All recordings will include automatically generated tags for date, time, camera identification for ease of retrieval when uploaded on-site. ICE personnel might not be assigned a specific camera for use throughout the Pilot, but ICE will maintain a record of camera assignments to personnel. Recordings that have an associated connection with a law enforcement-related system, must adhere to the appropriate System of Records Notices as indicated above.

To ensure retention requirements align with the relevant enforcement record, ICE will transfer all evidentiary data, upon receiving the appropriate tag, to the vendor's FedRAMP-certified cloud environment.

If Body Worn Camera recordings (whether evidentiary or non-evidentiary) are requested under FOIA, ICE will review requests on a case-by-case basis and release information as appropriate in accordance with FOIA requirements.

Privacy Risk: There is a risk of over-collection, since Body Worn Cameras may capture images of individuals recorded in the proximity of an incident that are irrelevant to the interaction or encounter.

Mitigation: This risk is partially mitigated. ICE will only use Body Worn Cameras per the instructions outlined in the ICE Directive in support of ICE's law enforcement mission. Misuse of Body Worn Camera data, including improper recording, improper dissemination, or tampering with data may result in disciplinary action for the ICE employee. To the extent that 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 National Archives and Records Administration-approved records retention schedules and will be redacted as appropriate in the event that ICE must release recording to an external party.

Privacy Risk: There is a risk that ICE may retain a recording or PII for longer than necessaryto meet ICE's mission.

Mitigation: This risk is mitigated. ICE automatically deletes non-evidentiary recordings after 60 days.

5. Principle of Use Limitation

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

ICE restricts its use of Body Worn Camera recordings captured during the evaluation to the following purposes:

- To further evaluate if Body Worn Camera assumptions hold true in ICE's operational environments;
- To assist in drafting a report or any other paperwork required in association with an incident;
- For training purposes, after all PII has been removed;
- For evidence in association with a law enforcement action or investigation; and
- To review ICE personnel actions in relation to an incident tagged asevidentiary.

The Body Worn Camera recordings from the Pilot can be used as evidence or for discovery pending approval and direction from the Headquarters Responsible Officials or Field Responsible Official. However, the Body Worn Cameras cannot be used outside of the authorized activities in the Body Worn Camera Directive. For example, ICE personnel cannot activate the Body Worn Cameras with the sole intent of obtaining evidence of an administrative violation by another officer, as this would not be an activity authorized by the Directive.

ICE personnel are trained to record enforcement encounters at the start of the event, or as soon as safely possible thereafter. In addition, the Body Worn Camera Directive prohibits the use of Body Worn Cameras in the following circumstances:

- ICE personnel are prohibited from intentionally making Body Worn Camera recordings for the purpose of recording any of the following activities and/or locations:
- Conducting or supporting a personnel investigation or disciplinary action;
- Assessing ICE employees, except for use in the training environment as part of the Body Worn Camera Pilot training student/instructor feedback process;
- Any non-enforcement activities, such as actions and conversations of coworkers when not actively engaged in a Pilot enforcement activity;
- Privileged communications (e.g., communication with ICE counsel);
- In places or areas where cameras generally are not allowed or permissible, such as locker rooms, dressing rooms, medical facilities, or restrooms, unless related to a Pilot enforcement activity;
- Inside detention facilities or government facilities that prohibit the use of recording equipment, unless related to a Pilot enforcement activity;
- Encounters with undercover officers, or confidential informants, and cooperating defendants; and
- Capturing Body Worn Camera recordings in a manner that would infringe on activity

protected by the First Amendment.

Directive at § 5.4.

Body Worn Camera recordings are subject to all applicable laws, regulations, collective bargaining agreements and DHS and ICE policies regarding ICE data and operations. As such, ICE may be required to disseminate a Body Worn Camera recording outside the agency. This includes dissemination to the U.S. Attorney's Office or to partner law enforcement agencies to develop an investigation or prosecution. Any release of Body Worn Camera recordings external to DHS will first be coordinated with the ICE Privacy and/or FOIA units (depending on the nature of the request) to ensure the release is proper and all appropriate redactions are applied. Trained ICE FOIA personnel will handle redaction activities 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 outside ICE.

In cases in which 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 all the information after analysis, unless they have an 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: Due to the portable nature of Body Worn Cameras and their compactness, there is a risk that the cameras may accidentally be used in areas where an individual has a reasonable expectation of privacy (e.g., private residence or restroom).

Mitigation: This risk is partially mitigated. In accordance with the Body Worn Camera Directive, ICE prohibits the use of ICE-owned Body Worn Cameras for personal use and prohibits Body Worn Camera recordings in places or areas where persons have a reasonable expectation of privacy, such as locker rooms, dressing rooms, and restrooms, unless related to official duties or incidents pertaining to those locations. ICE restricts personnel from recording events that are not law enforcement encounters, including actions and conversations of co-workers and management that are not part of the law enforcement incident. In addition, supervisors or other personnel may not routinely or randomly view recorded data for the sole purpose of identifying policy violations, conducting or supporting personnel investigations, or disciplining the responsible ICE personnel. Further, ICE will not use Body Worn Cameras to infringe on activity protected by the First Amendment.

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. ICE specifically

limits Body Worn Camera use to law enforcement activities outlined in the Directive.

Privacy Risk: There is a risk that recordings may be shared with third parties for purposes other than the purpose for which the recordings were made.

Mitigation: This risk is partially mitigated. Data requests for Body Worn Camera recorded information are subject to all applicable laws, regulations, collective bargaining agreements, ICE policies, and governing SORNs. ICE requires its components to seek approval from ICE stakeholder offices prior to releasing Body Worn Camera recorded data to a third-party. Specifically, the ICE Directive requires personnel to complete a DHS Privacy Act Disclosure Record (DHS Form 191) upon sharing information outside of DHS. 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 all the information after analysis, unless the receiving agency has separate statutory authority to retain the recordings.

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

Mitigation: This risk is mitigated. ICE determines whether or not the recording has evidentiary value. Recordings determined to have non-evidentiary value will be disposed of in accordance with the National Archives and Records Administration approved records retention schedule. Additionally, Body Worn Camera recorded data is only disclosed for official purposes in accordance with applicable DHS/ICE policies, including FOIA and Privacy Act request procedures listed in Section 2 of this document.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely,and complete, within the context of each use of the PII.

ICE captures Body Worn Camera recorded data in real-time to maintain an audio/video record of lawenforcement encounters. ICE uses the recording, in part, to verify what occurred during the encounter. Although the collection of a Body Worn Camera recording does not generally involve the collection of PII, ICE verifies any PII that may be captured in the audio or video recording prior to entering it into a hard copy case file or electronic case management system. In addition, audio and video recordings of law enforcement encounters would not be the sole source to identify potential subjects in cases or investigations. These recordings would supplement existing processes in building law enforcement cases.

ICE outlined a standard for camera equipment and video 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 will be utilized during the Body Worn Camera Pilot. The standards for camera equipment and video recording are as follows:

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

The evidence management system automatically tags the time, date, camera identification to standardize 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 National Archives and Records Administration approved records retention schedule to prevent the over-collection of non-evidentiary recordings.[28]

Privacy Risk: There is a risk that ICE will identify and take enforcement action against an individual based solely on a Body Worn Camera recording.

Mitigation: This risk is mitigated. ICE personnel will consider a variety of evidence prior to taking action and would use Body Worn Camera recordings only to supplement information obtained via other investigative techniques. ICE is currently finalizing Standard Operating Procedures, which will provide Pilot personnel with detailed guidance regarding their roles and responsibilities under the Body Worn Camera Directive, including the roles of the Field Responsible Officials who will be responsible for identifying which enforcement activities conducted at a Body Worn Camera Pilot site fall within the scope of "Pilot Enforcement activities" for purposes of the Body Worn Camera Pilot.

The Standard Operating Procedures will also inform the ICE Pilot participants that their responsibilities include:

- Ensuring that Body Worn Cameras are working properly, have an adequate power supply and sufficient memory prior to deployment, activating and deactivating the team's Body Worn Cameras as closely to the same time as operationally feasible during a planned enforcement action;
- Ensuring that, when activated, the Body Worn Camera recordings include the following:

[28] ICE Records will prioritize developing a records retention schedule for evidentiary video recordings.

- Badge number of the ICE personnel wearing the Body Worn Camera;
- The Body Worn Camera Pilot office where the ICE personnel is stationed;
- The date and time of each Pilot enforcement activity;
- Either an audible or visual method of identifying the individuals encountered during Pilot enforcement activity (e.g., name, date of birth, A-number), if operationally feasible; and
- Any verbal notice given to individuals that their encounter is being recorded during the Pilot.

In addition, the Standard Operating Procedures will instruct the Pilot participants to provide:

- Any relevant information to inform ICE's ability to correlate the Body Worn Camera recording with a particular overt, planned enforcement activity in order to better evaluate the results of the Body Worn Camera Pilot.
- Any use of force incidents as directed by ICE Directive 19009.2: Firearms and Use of Force (8/2/2021),[29] and notifying the Body Worn Camera Coordinator of such incidents; and
- Reporting to Headquarters Responsible Officials all potential privacy, civil rights, or civil liberties violations reported by the Body Worn Camera Coordinator within their office as soon as practicable.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguardsagainst risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

ICE stores Body Worn Camera recordings uploaded by ICE personnel at the end of each shift using the vendor-supplied secure docking station to the ice.us.evidence.com software as a service 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. Once the camera is docked in the docking station, it immediately begins synchronizing video evidence to the cloud-based evidence management system. Once the evidence sync is complete the evidence management system conducts a hashing validation against the video stored on the Body Worn Camera. If the hash confirms evidence integrity, the video evidence is then deleted from the Body Worn Camera.

This evidence management system provides the appropriate role-based access controls within an access-restricted FEDRAMP facility. Access to the audio/video data on the ICE evidence

[29] This policy is on file with the DHS and ICE Privacy Offices.

management 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 evidence management system is restricted by ICE/DHS Internet Protocol addresses 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. In order to communicate with a Body Worn Camera device, a user must be authorized for installation of the Body Worn Camera vendor application containing a Body Worn Camera trusted certificate and also be an authorized user within the 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) unauthorized accessing, printing, copying, e-mailing, web-posting, sharing, or reproducing Body Worn Camera recordings; or (4) deleting, modifying, or disposing of Body Worn Camera recordings unless it is in accordance with ICE policies and procedures, as well as National Archives and Records Administration approved records retention schedules. *Directive at §5.2.* 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. By policy, ICE prohibits Body Worn Camera recorded data from being uploaded onto public servers or social media websites. All ICE personnel must upload all Body Worn Camera recorded data to the designated evidence management system at the end of each shift, unless otherwise specified by their respective offices. The uploaded data will be stored within the ice.us.evidence.com for the duration of the Pilot. Personnel and their supervisors will label the respective videos and recordings appropriately per Body Worn Camera Directive.

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

Mitigation: This risk is mitigated. ICE mitigates this risk by establishing and developing role-based access controls preventing ICE personnel from manipulating or deleting the data directly from the camera or prior to upload at the end of the shift. Data will be securely transferred to the evidence management system within ice.us.evidence.com that complies with DHS security requirements. The ICE personnel's Supervisor also facilitates additional access to the chain of command that has a need to view the information in the performance of official duties.

Body Worn Camera manufactured 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 Personal Identify Verification card to log into ICE (or the vendor's) computers. ICE alsohas appropriate safeguards and audit trails in place to restrict access and viewing of recorded data to those with an official need to know. Such safeguards include automatically logging employee access to a recording, as well as the date, time, and location of

access, ensuring that filemanipulation is captured in an audit log. Lastly, prior to the issuance of Body Worn Cameras, ICE personnel receive extensive training in the proper use of Body Worn Cameras. Training includes: correct procedures for operating Body Worn Cameras; understanding and acknowledging protocols regarding usage; and demonstrating proper uploading, safeguarding, and labeling procedures for Body Worn Camera recorded data.

Any unauthorized access, use, release, or removal of recorded data or other violations of confidentiality laws and Department policies may result in disciplinary action and/or criminal or civil sanctions, as applicable. The ICE Office of Professional Responsibility (OPR) is responsible for investigating criminal and administrative allegations of misconduct.[30] In addition, every ICE employee has a duty to report any matters that could reflectsubstantive 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 Body Worn Camera Pilot will be trained regarding Body Worn Camera operation and care, appropriate handling of Body Worn Camera evidence, privacy procedures, civil rights and civil liberties restrictions, appropriate and permissible use of Body Worn Camera evidence, and rules of behavior regarding Body Worn Camera use. Training will include classroom and practical exercises. All personnel will be required to certify that they have received training and they understand the requirements set forth within the ICE Body Worn Camera Directive. ICE field office supervisors will be responsible for daily oversight of the program and will review the 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 personnel.

Records maintained by ICE may only be disclosed to authorized individuals with a work-related need for the information and only for uses that are consistent with the intended purposes of the program. All information stored in 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.

[30] Body Worn Camera *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). This policy is on file with the DHS and ICE Privacy Offices.

All evidence captured on the Body Worn Cameras have audit trails of all actions to the evidence from the time of capture until deletion. Once the evidence is uploaded at the conclusion of each shift these audit trails are transferred to the evidence management system and managed by the evidence management system from that point on. Any attempt to view, delete, tag, download, or any other means of evidence manipulation are captured within the evidence management system audit logs.

ICE will ensure that video is properly stored, categorized, and labeled; and that standard operating procedures and technical guidance are updated to reflect changes to equipment or existing laws, regulations, and policies. These updates will be coordinated with all applicable offices. ICE will also monitor system deployment to ensure ICE personnel are utilizing Body Worn Cameras correctly. The ability to audit the recording is necessary once the evaluation is complete and ICE has determined how to move forward with camera technology at the enterprise level based on the assessment of the evaluation. These documented audits will be completed by selecting recorded data at random to ensure it is properly categorized and named according to established standard operating procedures and ensuring that all recorded data determined to be of evidentiary value or requested under FOIA is properly transferred to ICE law enforcement systems.

Responsible Officials

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

Jordan Holz
Privacy Officer
U.S. Immigration and Customs Enforcement
U.S. Department of Homeland Security

Approval Signature

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

_____

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