Privacy Impact Assessment of
Body Worn Cameras Data Management System
Office of Inspector General (OIG)

For Questions or Comments, please email: privacy.comments@frb.gov.

Description of the IT system:

The Office of the Inspector General (OIG) for the Board of Governors of the Federal Reserve System (Board) is an independent oversight authority established under the Inspector General Act of 1978 (IG Act), as amended. Its mission is to provide independent oversight by conducting audits, investigations, and other reviews relating to the programs and operations of both the Board and the Consumer Financial Protection Bureau (CFPB). In doing so, OIG makes recommendations to improve economy, efficiency, and effectiveness; and prevent and detect fraud, waste, and abuse. In accordance with the IG Act, the OIG shares its recommendations with the Board and the CFPB, while keeping the Board, CFPB's Director, and Congress informed of its findings and recommendations, as well as the agencies' progress in implementing corrective actions.

As part of its investigatory responsibilities, OIG uses body-worn cameras (BWCs) when gathering and preserving certain evidence in accordance with applicable laws and policies. The personally identifiable information (PII)[1] collected by a BWC is stored in OIG's Body Worn Camera Data Management System (BWC System).

BWCs are used by OIG's special agents, consistent with presidential Executive Order 14074, "*Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public*

[1] According to the Office of Management and Budget (OMB), PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. The Office of Management and Budget (OMB), OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017). Memorandum for Heads of Executive Departments and Agencies (whitehouse.gov).

Trust and Public Safety," (Executive Order 14074)[2] which also requires agencies to publicly post their BWC polices. OIG's BWC Policy (March 26, 2024) is available at https://oig.federalreserve.gov/documents/oig-policy-body-worn-cameras.pdf.

OIG deploys BWCs in planned law enforcement operations (i.e., when the use of force may reasonably be anticipated, such as the planned execution of a search warrant or arrest). The mission of OIG's BWC Program (BWC Program) is to gather and preserve evidence during the specified field operations as outlined in the OIG BWC Policy.

BWCs capture video and audio recordings that are then uploaded to a cloud-based system, to which OIG Special Agents, OIG Officers, and support staff have limited access to perform their official business responsibilities. Recordings, and transcriptions of recordings, may be used as evidence in OIG investigations, and for training purposes. BWCs may collect PII from individuals under investigation, as well as complainants and witnesses relevant to OIG's investigations. In the course of such investigations, BWCs may also record bystanders and others who are not part of OIG's investigation but are in the vicinity of a target.

The BWC System maintains recordings that contain PII, as discussed below, which may be shared as required by a court order, applicable laws, rules, or regulations.

Prior to sharing any recordings, video and audio redactions, or audio to text transcriptions may be made using artificial intelligence (AI) tools as described below:

> Video redactions: Automatically detects and redacts screens (computer screens, digital signs), faces and license plates captured. Prior to redacting any evidence, a special agent must first approve the redactions before sharing any evidence.
>
> Audio redactions: Audio recordings may be redacted.
>
> Audio to Text Transcriptions: Audio recordings may be transcribed to text. Transcripts are then labeled "unverified" until an OIG designated member reviews, edits and approves the final transcript.

OIG BWC Roles and Responsibilities

OIG's Assistant Special Agent in Charge (ASAC) of Headquarters Operations (HQ) in the Office of Investigations (OI) provides general oversight of the BWC Program under the direction of the Special Agent in Charge (SAC). The BWC Coordinator is responsible for the day-to-day management of the program, reports to the ASAC, and periodically reviews a sampling of recordings to provide reasonable assurance that BWC equipment is operating properly and that

[2] Executive Order 14074 (May 25, 222) is available at Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety | The White House.

special agents are using the devices in accordance with OIG's BWC Policy.

The Use of BWCs

OIG prohibits the use of BWCs for anything other than official law enforcement duties. BWCs may be used in undercover operations only with the written authorization of the Associate Inspector General for Investigations (AIGI). The BWC Program uses cameras provided by a third-party vendor, which are attached to the chest-level areas of protective vests or outer garments of special agents. The BWC Program also uses the vendor's cloud-based storage software as a service (SaaS) solution, which is Federal Risk and Authorization Management Program (FedRAMP)[3] authorized at the "High Impact Level."[4] PII is collected, maintained, and disseminated as appropriate under applicable law, policy, or regulation. Video and audio recordings captured by cameras are uploaded to a secure third-party cloud-based system (BWC System). When BWCs are turned on, there is a 30-second "buffering period" during which the camera only captures video (no audio), which is automatically deleted every 30 seconds. Both video and audio recordings begin once the record button is pressed, which includes any video captured during the buffering period.

Special agents are required to wear and activate BWCs during any preplanned attempt to serve an arrest warrant or other preplanned arrest, including apprehending fugitives sought on state or local warrants, the execution of a search and seizure warrant or a court order. If a special agent encounters an individual who is uncooperative, violent, assaultive, or discussing criminal conduct that, in the special agent's judgment, could lead to the use of physical or deadly force or be relevant to the investigation, the special agent must activate their BWC when doing so is safe and practical. An intentional failure to activate the BWC or the intentional unauthorized termination of a BWC recording may result in disciplinary or adverse action, up to and including termination.

The BWC System contains video and audio recordings of individuals under investigation by the OIG, as well as complainants and witnesses. The BWC System may also contain the inadvertent or unavoidable recording of bystanders and others who are not part of the OIG's investigation. Video and audio recordings (and, when requested, transcriptions of the recordings) may include, but is not limited to, video and audio of people, driver licenses, personal information verbally requested for the purposes of identifying individuals, and criminal history information. Any sounds or images that are collected inadvertently or unavoidably by BWCs during the course of an investigation will

[3] How to Become FedRAMP Authorized | FedRAMP.gov.
[4] "High Impact data is usually in Law Enforcement and Emergency Services systems, Financial systems, Health systems, and any other system where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." Understanding Baselines and Impact Levels in FedRAMP | FedRAMP.gov.

be redacted, to the extent practicable, prior to the release of such recordings, though the original unredacted copy will be maintained in accordance with the applicable records schedule.

1. Source(s) of each category of information listed in item 1:

Information may come from a variety of sources including, but not limited to individuals under investigation, complainants, witnesses, publicly available sources, and confidential sources.

2. Purposes for which the information is being collected:

PII is maintained in the BWC System for the purpose of conducting and managing investigations, related to the programs and operations of the Board (including Board-delegated functions performed by the Federal Reserve Banks) and CFPB.

3. Who will have access to the information:

Access to PII in the BWC System is limited to authorized OIG employees for official business purposes. In limited circumstances, an OIG contractor(s) may also have access on a need-to-know basis. In accordance with the Privacy Act of 1974 (Privacy Act) (5 U.S.C. § 552a), the Board exercises certain Privacy Act exemptions and routine uses (i.e., records that may be disclosed without the written consent of individuals to whom the records pertain), as described in the System of Records Notices (SORN) (*see Section 9 herein*). OIG may also disclose information subject to the Freedom of Information Act, 5 U.S.C. § 552, and as directed by court order or applicable laws, rules and regulations.

In determining whether to publicly release a BWC recording, OIG will, as appropriate, consider applicable law (e.g., the Privacy Act); consult with the applicable U.S. Attorney's Office; and take into account the need to promote transparency and accountability, protect the privacy rights of individuals, and any need to protect ongoing law enforcement operations.

The BWC coordinator is required to periodically review the audit log to ensure that only authorized users access the recordings and associated data for authorized purposes. The audit log is also reviewable by OIG Legal and the ASAC. This information may be discoverable and may be requested by the prosecution or the defense during court proceedings. All requests for BWC recordings unrelated to a pending criminal, civil, administrative review, or investigation are forwarded to OIG Legal, which is responsible for the initial processing of such requests. Special agents may review BWC recording in performing their official business responsibilities and with their attorneys or other representatives if they become the subject of a review or investigation.

4. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses):

Individuals generally do not have the opportunity to consent or decline to provide information obtained through BWCs, unless otherwise provided by law.

5. Procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date:

OIG relies on information collected directly from individuals, the Board, the Federal Reserve Banks, or the CFPB for the accuracy, completeness, and timeliness of that information. PII provided by individuals may also be corroborated during the course of an investigation.

6. The length of time the data will be retained and how will it be purged:

The National Archives and Records Administration (NARA) approved OIG investigative records, including BWC recordings and transcriptions, which have a records retention period of 10 years beginning when the investigation is closed, unless the records relate to a significant investigation (e.g., cases resulting in substantive change in agency policy, cases with national or regional media attention, and cases that attract congressional attention). In such instances, the files are retained permanently transferred to NARA in five (5)-year blocks 30 years after the investigation is closed. (See, N1-82-00-01 Inspector General Records Approved by NARA).

7. The administrative and technological procedures used to secure the information against unauthorized access:

In addition to access controls, PII and other sensitive information are stored on servers at the FedRAMP "High Impact Level," which includes applicable controls under the National Institute of Standards and Technology's (NIST) Special Publication 800-53. Once a law enforcement activity has concluded, the team leader for the operation directs all involved special agents to upload recordings from their BWCs to the appropriate storage cloud mechanisms as soon as possible, but no later than one (1) week after the operation or activity has ended. Although recordings stored on the cameras are not encrypted, they cannot be accessed from the BWC alone. Evidence data is encrypted both in transit and while at rest in storage. An audit log is automatically created and maintained for every recording. The audit log contains a history of all user logins and all user actions. BWC recordings uploaded to the cloud, as well as audit logs generated from BWC recordings uploaded to the cloud are protected using multi-factor authentication. Database servers and all approved OIG mobile devices containing the vendor's apps are also encrypted.

8. Whether a new system of records under the Privacy Act of 1974 (Privacy Act) will be created. (If the data are retrieved by name, unique number or other identifier assigned to an individual, then a Privacy Act system of records may be created):

The Body Worn Camera Data Management System is covered by Privacy Act System of Records Notice BGFRS/OIG-1, "*OIG Investigative Records*," which may be accessed at Federal Reserve Board - System of Records Notices (SORNs).

Reviewed:

//Signed// *11/25/2024*
Charles Young Date
Senior Agency Official for Privacy

//Signed// *11/26/2024*
Jeff Riedel Date
Chief Information Officer