PRIVACY IMPACT ASSESSMENT

FHFA-OIG Body-Worn Camera and Digital Evidence Management System

Date: August 26, 2024

OVERVIEW

This section provides an overview of the System and addresses the following:

- The System name and the division/office that owns the System;
- The purpose of the program, System, or technology and how it relates to the agency's mission; and
- A general description of the information in the System.

Date submitted for review: August 26, 2024

System Owner(s)			
Name	Special Agent Kyle K. Lin	**Email**	Kyle.Lin@fhfaoig.gov
Division	Office of Investigations	**Office Phone**	202.730.4914
System Overview	*Briefly describe: (1) the purpose of the program, System, or technology, (2) the information in the System, and (3) how it relates to FHFA-OIG's mission.* The Federal Housing Finance Agency Office of Inspector General (FHFA-OIG) is vested with statutory law enforcement authority. This authority is exercised by its Office of Investigations (OI). OI is empowered to conduct criminal, civil, and administrative investigations for potential violations of federal laws or regulations affecting FHFA and its regulated entities. This privacy impact assessment (PIA) analyzes the FHFA-OIG Body-Worn Camera (BWC) Program. The BWC Program is comprised of two interconnected technologies: (1) BWCs worn by OI Special Agents (SAs); and (2) an associated digital evidence management system (DEMS) to store video and audio recordings obtained by the BWCs. OI SAs will use only BWCs that are owned, issued, and controlled by FHFA-OIG. The associated DEMS is a FedRAMP-authorized Software as a Service (SaaS) cloud platform. The BWCs record both video and audio and are configured to upload to the DEMS by various means. In addition to FHFA-OIG BWC recordings, other evidentiary digital files may be uploaded to the DEMS. This includes: BWC recordings from partner law enforcement agencies; photographs; audio and/or video recordings of in-person or telephone interviews of victims, witnesses, subjects, or targets; screenshots; mobile phone recordings; transcripts of audio recordings; and other evidentiary digital files generated by FHFA-OIG SAs or received from partner LEAs. Once uploaded to the DEMS, BWC recordings and other digital evidence can be accessed only in accordance with controls discussed in more detail below. The BWC Program is owned and managed by FHFA-OIG's Office of Investigations (OI).		

System Owner(s)	
	The purpose of FHFA-OIG's BWC Program is to foster public trust, transparency, and accountability in its law enforcement investigations and operations. The program also complies with Executive Order 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety, Sec. 13, 87 Fed. Reg. 32945 (May 31, 2022), and FHFA-OIG's Body-Worn Camera Policy.

Section 1.0 CHARACTERIZATION OF THE INFORMATION

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, System, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is being collected, used, disseminated, or maintained in the System?	The information collected and maintained is comprised of video and audio recordings generated by BWCs worn by FHFA-OIG SAs during certain law enforcement operations and investigative activities, various items of metadata attached to the recordings, and transcripts of audio recordings. In addition, information in the system includes non-BWC video recordings, audio recordings, and photographic images generated or collected by FHFA-OIG SAs during investigative activities. Finally, information in the system includes other digital media generated and provided by partner LEAs.
1.2	What or who are the sources of the information in the System?	The sources of information include FHFA-OIG SAs, partner LEAs, other individuals associated with FHFA-OIG investigations, and members of the general public. Also, BWC recordings may be generated during FHFA-OIG training exercises.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The purposes are: (1) to build public trust by providing transparency and accountability in FHFA-OIG law enforcement investigations and operations; (2) to comply with Executive Order 14074; (3) to build and conduct criminal, civil, and administrative investigations against individuals and entities for potential violations of federal laws or regulations; (4) provide reliable evidence for use in criminal, civil, and administrative proceedings resulting from FHFA-OIG investigations; (5) provide BWC data for use by FHFA-OIG supervisors and management to evaluate SA performance and to resolve allegations against SAs; and (6) to comply with the FHFA-OIG Body-Worn Camera Policy and other OI policies.
1.4	How is the information provided to FHFA-OIG?	Information is provided from BWC recordings and other video and audio recordings generated by FHFA-OIG SAs. Partner LEAs may also provide evidentiary digital files and case-related documents and recordings to FHFA-OIG for inclusion in the system.

#	Question	Response
1.5	Given the amount and type of information collected, what are the risks to an individual's privacy that are associated with collection of the data? Explain in detail how the loss or compromise of the information will/can affect an individual's privacy.	The primary risks to privacy are from improper access to BWC recordings and the unauthorized disclosure, transfer, or sharing of the recordings. The BWC data collected by the program may be shared among: FHFA-OIG SAs; federal, state, or local prosecutors and LEAs; and opposing counsel for purposes of criminal prosecutions and other legal proceedings. An individual's privacy could be adversely affected by the unauthorized or inadvertent release of video or audio recordings of the individual, visual images of private locations such as homes or businesses, audio recordings or transcripts of spoken private information, or case-related documents and recordings containing private information stored in the DEMS.
1.6	Are Social Security numbers collected or used in the system?	The system is not intended to capture Social Security numbers (SSN).
1.7	If Social Security numbers are being collected, provide the legal authority for the collection. In addition, describe in detail the business justification for collecting SSNs, what the consequences would be if SSNs were not collected, and how the SSNs will be protected while in use, in transit, and in storage.	N/A

Section 2.0 USES OF THE INFORMATION

The following questions delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	How will the information be used and for what purpose?	See Section 1.3.
2.2	Describe the types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	The DEMS is provided by Software as a Service (SaaS) cloud service providers with a FedRAMP certification. To access the DEMS, authorized users are required to use multifactor authentication. Once BWC recordings are uploaded to the DEMS, they are permanently deleted from the BWC and are available only in the DEMS. FHFA-OIG has strict policies in place to control access to and dissemination of information in the DEMS and provides training in the policy and applicable security protocols to all involved personnel. FHFA-OIG also utilizes visual and audio redactions to preserve privacy where appropriate. Under FHFA-OIG's Body-Worn Camera Policy, SAs are not permitted to share or otherwise release any BWC recordings

#	Question	Response
		outside of FHFA-OIG, and the unauthorized access, copying, or release of BWC recordings may result in disciplinary action. SAs must obtain supervisory approval prior to the disclosure of any BWC content to law enforcement partners. Access to BWC recordings is password-protected, recorded automatically by system software, and audited periodically by the BWC-DEMS Program Manager to ensure that only authorized users are accessing the data for authorized purposes. All logins, video access, and other actions taken in system software are noted in audit trail logs that are reviewable by the BWC-DEMS Program Manager and FHFA-OIG management. Original BWC recordings cannot be edited. Any change (e.g., redactions) from the original recording must be made by a system administrator or authorized user, and the system generates a duplicate with the change that is clearly marked in the system, leaving the original unchanged.

Section 3.0 RETENTION

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	FHFA-OIG's Evidence Policy (OI Policies and Procedures Manual, Chapter 8) provides the procedures for preserving the digital recordings maintained in the DEMS that constitute evidence. The FHFA-OIG Records Management Policy and the incorporated FHFA Comprehensive Records Schedule (CRS) control the retention and disposition of information in the DEMS that is incorporated into Investigative Case Records. All information in DEMS incorporated into Investigative Case Records will be retained in accordance with the above policies and CRS.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	FHFA-OIG records are addressed in FHFA's Comprehensive Records Schedule. The NARA authority for the FHFA Comprehensive Records Schedule is N1-543-11-1, as approved on January 11, 2013, and reflects GRS Transmittal No. 31, dated April 1, 2020.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	For the short-term, the risks remain the same as described above in section 1.5. The risks are mitigated by limiting and controlling access, as described above in section 2.2. Permissions are required to access the data and will not be granted without appropriate need-to-know and training. Access will be quickly terminated for employees when access is no longer needed or when no longer appropriate.

#	Question	Response
		For digital evidence requiring a longer retention period, there is a risk that technology will change, resulting in the need for a different or enhanced approach to system security. FHFA-OIG mitigates this risk by following the latest NIST, FIPS, and other relevant information security standards to protect its systems and data.

Section 4.0 NOTICE, ACCESS, REDRESS, AND CORRECTION

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created? If so, provide the SORN name and number. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	Yes. The DEMS is part of FHFA-OIG's SORN published on March 9, 2021, in the Federal Register (86 Fed. Reg. 13548). The SORN includes the FHFA-OIG Investigative Files Database (FHFA-OIG-2) as well as FHFA-OIG Investigative Document Repository MIS Database (FHFA-OIG-3).
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	Evidentiary BWC recordings are generated by FHFA-OIG during arrests, execution of search warrants, seizure orders, and other law enforcement activities. While individuals may receive general notice regarding the activity (e.g., "knock and announce" during a search warrant or verbal notification they are under arrest), they generally will not receive notice that FHFA-OIG SAs are recording with BWCs.
4.3	Do individuals have the opportunity and/or right to decline to provide information? What are the consequences if an individual declines to provide the information?	When evidentiary BWC recordings are generated during arrests, search warrants, seizure orders, and other law enforcement activities, individuals do not have the right to decline being recorded. When BWCs are used to record voluntary interviews, including voluntary custodial interviews, the individual may decline the interview, which would in effect decline BWC recording. Use of BWCs by FHFA-OIG SAs is mandatory, and FHFA-OIG SAs cannot decline to record or be recorded by BWCs during enforcement activities and training exercises.

#	Question	Response
4.4	What are the procedures that allow individuals to gain access to their information?	FHFA has issued Freedom of Information Act (FOIA) and Privacy Act regulations that address the production and release of FHFA-OIG records. See 12 C.F.R. Parts 1202 and 1204. In accordance with these regulations, FHFA-OIG independently has adopted processes, posted on the FHFA-OIG public website, for individuals to request agency records under FOIA and the Privacy Act. Criminal defendants and parties to other legal proceedings are given access to their information in accordance with applicable legal discovery rules. In all circumstances, BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings. BWC recordings will also be treated as potential evidence in a federal investigation subject to applicable federal laws, rules, chain of custody requirements, and policies concerning disclosure. All requests for FHFA-OIG BWC recordings unrelated to a pending OI criminal investigation or case will be forwarded to the Office of Chief Counsel, which is responsible for processing and responding to such requests.
4.5	What are the procedures for correcting inaccurate or erroneous information?	OI employees are responsible for ensuring the information in the DEMS is current and accurate. Under FHFA regulations, information compiled by FHFA-OIG for the purpose of law enforcement investigations is subject to Privacy Act exemptions in 5 U.S.C. 552a(j)(2), (k)(2), and (k)(5). See 12 C.F.R. 1204.7(c). In addition, as stated in the FHFA-OIG SORN, OI systems of records may contain records that are exempt from the notification, access, and amendment requirements pursuant to the provisions of 5 U.S.C. 552a(j)(2), (k)(2), and (k)(5).

Section 5.0 SHARING AND DISCLOSURE

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	With which internal organization(s) is the information shared? What information is shared and for what purpose?	Information may be shared with other FHFA-OIG offices as needed to further OIG audit, evaluation, and counsel activities. Audit, evaluation, and other OIG personnel will ensure that efforts are not duplicated, and that law enforcement activity and individuals' privacy are not compromised by inadvertent

#	Question	Response
		disclosure during the conduct of an audit, evaluation, or other matter.
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include federal, state, and local government, and the private sector.	Information may be shared with federal, state, or local law enforcement agencies, including the U.S. Department of Justice; federal, state, or local prosecutors; and other OIGs for the purpose of criminal investigation and prosecution. Other releases may be made in connection with litigation, or to members of the general public and media in response to FOIA requests, but only as appropriate and in accordance with the personal privacy protections in the FOIA statute (5 U.S.C. § 552(b)) and applicable regulations (12 C.F.R. Parts 1202 and 1204). Information may be shared with criminal defendants and parties to other legal proceedings in accordance with applicable legal discovery rules. In such cases, visual images, audio recordings, or portions of a written transcript will be redacted as allowed or required by law to protect individuals' privacy.
5.3	Is the sharing of PII outside FHFA-OIG compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA-OIG.	Yes. FHFA-OIG shares information in the DEMS in accordance with the routine uses set forth in FHFA-OIG's published SORN: https://www.govinfo.gov/content/pkg/FR-2021-03-09/pdf/2021-04796.pdf.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	Risks to an individual's privacy are that personal, financial, and other sensitive information may be improperly disclosed or compromised. There is also a risk that unauthorized persons may learn that an individual is the subject of or associated with a criminal or civil investigation by FHFA-OIG or other law enforcement agencies or is a witness to law enforcement activity. Case information from the DEMS may be shared with other federal and state law enforcement agencies, as described above. No outside law enforcement agencies have access to the DEMS. Risks to individuals' privacy are mitigated using encryption to protect data in transit and at rest. Such processes are in accordance with the protections applied to the General Support System. Data in transit is protected via network protocols encrypted with transport layer security, and data at rest is protected via database encryption. Releases may also be made to members of the general public or media in response to FOIA requests. Risks to individuals' privacy are mitigated by reviewing the information before release and withholding or redacting information in accordance

#	Question	Response
		with personal privacy exemptions in the FOIA statute and FHFA implementing regulations. In cases of external sharing, visual images, audio recordings, or portions of a written transcript will be redacted as allowed by law to protect individuals' privacy.

Section 6.0 TECHNICAL ACCESS AND SECURITY

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing? If so, provide a signed copy to the Chief Counsel with this PIA.	Access to the DEMS is restricted to authorized users. Those authorized users are identified by the Deputy Inspector General for Investigations (DIGI) and are limited to SAs, counsel, OI management, investigative support staff, and other OIG personnel with a demonstrated need for access as approved by the DIGI. Access procedures are documented in the FHFA-OIG Body-Worn Camera Policy and digital evidence management policy. Specific access rights for all users are controlled and documented in the System Administration component of the DEMS. Access to digital evidence is on a "need-to-know" basis and is restricted to OI and other FHFA-OIG staff and contractors who need to access case information (e.g., case agent, SAC, Operations Officers, counsel, and OI management). FHFA-OIG SAs have access only to digital evidence they personally recorded and from their own cases and cases they are assisting. Supervisors have access to digital evidence generated by their subordinates and for the cases they supervise in addition to the digital evidence they personally recorded. In sensitive circumstances, such as critical incidents or internal investigations, access is further restricted as directed by FHFA-OIG senior management.
6.2	Will non-FHFA-OIG personnel (e.g., contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will FHFA-OIG control their access and use of information? Are there procedures documented in writing? If so, provide a copy to the Chief Counsel with this PIA.	Information Technology (IT) contractors have access to the system for technical support but do not have access to evidence, recordings, transcripts, or information contained therein.

#	Question	Response
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System.	BWC and DEMS user training is conducted prior to use for current and new OI personnel. This typically consists of 16 hours of in-person training and additional online training maintained by the vendor. It includes use of the BWC, the DEMS, and associated software applications. This includes instruction on how to access information safely and securely in the DEMS. It also includes instruction on FHFA-OIG's BWC policy and legal obligations relative to BWC evidence. Ongoing training is conducted as needed. In addition, all FHFA-OIG employees must annually complete courses on Information Security Awareness, the FHFA-OIG IT Policy, and the FHFA-OIG IT Procedures and Rules of Behavior.
6.4	Describe the technical/administrative safeguards in place to protect the data.	See section 2.2 for detailed technical information on controls and safeguards to protect BWC data.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	The BWC-DEMS system has robust audit capabilities, which include automatically generated and detailed audit trails and activity reports for evidence, users, and BWCs. This includes a chronological record of all interactions with a piece of evidence and the creation of additional copies with any changes; system activities by the user; changes to the user account; events and changes for BWC devices; and actions taken on a report, actions performed by a user, and any export of information. This audit information is reviewed at three levels at various intervals by field supervisors, a Headquarters-based BWC-DEMS Program Manager, and FHFA-OIG management officials. Also, this audit information can be accessed at any time on an as-needed basis.
6.6	Has a Security Assessment and Authorization (SA&A) been completed for the System or Systems supporting the program? If so, provide the date the last SA&A was completed. If not, and one is required, provide the expected completion date of the SA&A.	Yes, the SA&A is dated June 11, 2024.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued, and for how long was it issued? Provide a copy to the Chief Counsel with this PIA. If not, when do you anticipate such ATO being issued?	An Authority to Use (ATU) for US Axon FedCloud (ACS) was completed on June 13, 2024. The security authorization of the information system will remain in effect for a length of time in alignment with the Office of Management and Budget Circular A-130 provided: (1) Axon Enterprise, Inc. satisfies the requirement of implementing continuous monitoring activities as documented in their security documentation; (2) Axon Enterprise, Inc. mitigates POA&M action items documented in the Security Assessment Report and as developed during continuous monitoring activities; and (3) significant changes or critical vulnerabilities are identified and managed in accordance with applicable federal law, guidelines, and policies.

Signatures

FHFA-OIG

Kyle K. Lin System Owner	KYLE LIN Digitally signed by KYLE LIN Date: 2024.08.26 10:23:20 -04'00' System Owner (Signature)	Date
Karl Kadon Executive Sponsor	KARL KADON Digitally signed by KARL KADON Date: 2024.08.27 07:04:07 -04'00' Executive Sponsor (Signature)	Date
Amanual Estefou System Administrator	AMANUAL ESTEFOU Digitally signed by AMANUAL ESTEFOU Date: 2024.08.26 10:29:34 -04'00' System Administrator (Signature)	Date
Michael Stoner Chief Information Security Officer	MICHAEL STONER Digitally signed by MICHAEL STONER Date: 2024.08.26 10:55:37 -04'00' Chief Information Security Officer (Signature)	Date
Michael Smith Chief Information Officer	MICHAEL SMITH Digitally signed by MICHAEL SMITH Date: 2024.08.26 11:17:30 -04'00' Chief Information Officer (Signature)	Date
Mary Schaefer Acting Chief Counsel	MARY SCHAEFER Digitally signed by MARY SCHAEFER Date: 2024.08.26 10:15:07 -04'00' Acting Chief Counsel (Signature)	Date

FHFA

Tasha Cooper Senior Agency Official for Privacy	Cooper, Tasha L. Digitally signed by Cooper, Tasha L. Date: 2024.08.28 14:05:05 -04'00' Senior Agency Official for Privacy (Signature)	Date