OIG-OI DIGITAL EVIDENCE MANAGEMENT SYSTEM (DEMS) PRIVACY IMPACT ASSESSMENT

1. OVERVIEW

The use of the Digital Evidence Management System (DEMS) by OIG-OI Special Agents fosters public trust, transparency, and accountability. DEMS enables Special Agents to capture contacts between witnesses, subjects, targets, and other members of the public using a body worn camera (BWC). BWC footage captured during these contacts is the only information retained in DEMS. Recordings from a DEMS BWC can help resolve complaints made against agency personnel and possible wrongdoing by third parties. In some cases, recordings from a DEMS BWC can have evidentiary value, or may capture things that the Special Agent did not see, hear, or otherwise notice. Personally identifiable information (PII) may be captured on law enforcement camera systems when the recording device is activated during law enforcement citizen interactions. Data recorded is directly related to law enforcement activities and emergency response, and may include video images of people, driver licenses, personal information verbally requested for the purposes of violation notices and/or arrests during a lawful contact, and criminal history information provided over the radio by a dispatch communications center. DEMS footage is categorized and searched by the name of the Special Agent who recorded the footage and the date of the recorded footage. The OIG Inspector General Act of 1978, as amended, 5 U.S.C. App. 3 provides the authority to collect any information for the DEMS system as well as Executive Order 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety."

2. CHARACTERIZATION OF THE INFORMATION

While the system's purpose it not to collect PII, PII on members of the public, Federal employees, and Federal contractors may be captured on the DEMS BWC during law enforcement activity.

From whom is information to be collected?

Federal Employees, members of the public, and Federal contractors.

Why is the Information being collected?

Per Executive Order 14074 on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, OIG Special Agents will deploy BWCs during enforcement operations, such as search warrant executions and arrests. During enforcement operations, Special Agents may also use the BWC to record interviews.

What is the PII being collected, used, disseminated, or maintained?

Name, Date of Birth, Social Security Number, Physical characteristics, and law enforcement credentials There may be other categories of PII collected incidentally when recording is activated (See, e.g., other possible information identified in Appendix A).

How is the PII collected?

Any PII that is collected will be captured on the DEMS BWC device when video recording is activated.

How will the information collected from individuals or derived from the system be checked for accuracy?

The nature of the device (video) is to capture Law enforcement interactions with citizens. Because the collection is done by video, the collection is considered an accurate reflection of the interactions.

What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?

- Inspector General Act of 1978, as amended, 5 U.S.C. App. 3.
- Executive Order 14074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety

Privacy Impact Analysis

The DEMS BWC device is restricted for authorized law enforcement agents, their direct managers, and DEMS administrators only. Firewall monitors are in place to prevent unauthorized users from accessing OIG's internal network from the internet and there are no public access accounts to the system. Special Agents with a need to know must authenticate to the system and have the credentials to gain access to the footage.

3. DESCRIBE THE USES OF THE PII

Describe all the uses of the PII

When recording is activated, law enforcement agents will state their name and/or credentials for identification during law enforcement activities. Other physical characteristics of individuals may also be captured in the footage collected. Additionally, body worn camera footage review may be necessary after the recording on a case-by-case basis, depending on investigative needs and type of request being made for footage.

What types of tools are used to analyze data and what type of data may be produced?

Tools are not used to analyze the data.

Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?

No.

If the system uses commercial or publicly available data, please explain why and how it is

used.

The system does not use commercial or publicly available data.

Will the use of PII create or modify a "system of records notification" under the Privacy Act?

Yes. It will modify DOL/OIG-11 due to new video recordings being added to the system that are identified by the name of the Special Agent who recorded the video.

Privacy Impact Analysis

To protect the confidentiality and integrity of the data, encryption is implemented on the network, within the computer and storage, and within the application used to access video.

4. RETENTION

What is the retention period for the data in the system?

If a DEMS BWC recording is deemed as evidence, employees will adhere to DOL-OIG's evidence policy. DEMS content deemed non-evidentiary will be maintained on the DEMS secured server for a period of 5 years. On an annual basis, OIG HQ will coordinate with the OIG Records Officer to properly dispose of temporary DEMS BWC files that are greater than 5 years old. DEMS BWC content that is deemed evidentiary in nature should follow retention and destruction instructions provided by the assigned prosecutor. Temporary DEMS Recordings will be retained for no longer than 7 days.

Permanent DEMS BWC Recordings
Evidentiary: Labor Racketeering cases 20 years
DOL Program Fraud cases 10 years
Non-evidentiary: Retain for 5 years, dispose in accordance with BWC policy.

Temporary DEMS BWC Recordings
Accidental, Training, and Inadvertent Recordings: Retain for no longer than 7 days, then delete. Date (12/15/2022 to present)

Is a retention period established to minimize privacy risk?

Yes, these records are considered unscheduled records and will be treated as permanent records until NARA approves final disposition. This approach is designed to satisfy the intended law enforcement purpose of the system but is not designed to minimize the privacy risk. However, OIG utilizes all other necessary controls, such as encryption, to protect privacy while the records are maintained.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

No, the schedule is currently in draft form.

Per M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored, or maintained by the system if it is no longer required?

The directive in M-17-12 to eliminate or reduce PII that is collected, stored, or maintained in a criminal investigative file is contrary to investigative practice which requires a full and complete inquiry and exhaustion of all potential sources of information. See 5 U.S.C. 552a(e)(1). However, the records retention schedule, once approved by NARA will identify the records retention and disposition schedule. Also, U.S. DOL OIG Manual Investigative Notice (IN) 08-1900 (signed and approved August 22, 2022) addresses the storage, access, and review of BWC recordings. IN 08-1900 is included here to this Privacy Impact Analysis.

How is it determined that PII is no longer required?

The requirement to maintain any captured PII by DEMS is determined by how the video is categorized. The video will be maintained based on DOL-OIG's evidence policy, as outlined above.

If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify, or anonymize PII.

The original video would remain as captured. However, if a video is requested to be viewed by the Assistant United States Attorney, a copy can be made and redacted as necessary on a case-by-case basis based on what type of PII is captured, the purpose, and why it is being reviewed. The purpose of the review will determine what will need to be redacted at the time.

5. INTERNAL SHARING AND DISCLOSURE

With which internal organization(s) is the PII shared, what information is shared, and for what purpose?

Data captured on the DEMS BWC device is not shared with other DOL component agencies. This data may be part of an investigative legal case file but is generally not linked specifically to other case files maintained under the system covered by the System of Records Notice for DOL/OIG-11.

How is the PII transmitted or disclosed?

Not applicable. PII is not transmitted or disclosed to other DOL component agencies.

Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?

Not applicable.

Privacy Impact Analysis

There is no impact as data is not being shared with other DOL component agencies.

6. EXTERNAL SHARING AND DISCLOSURE

With which external organization(s) is the PII shared, what information is shared, and for what purpose?

Data may be shared with Assistant United States Attorneys (AUSA) per their request to support law enforcement investigations. In accordance with EO 14074 and applicable law including the Privacy Act, in the event of an incident e.g. involving serious bodily injury or death in custody, the U.S. DOL OIG Manual IN 08-1900 Investigations for Body worn Camera Program policy will cover the release of the footage to promote transparency and accountability, as well as the duty to protect the privacy rights of persons depicted in the footage and any need to protect ongoing law enforcement operations.

Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL?

Yes. While the SORN for Investigative Case Files and Tracking System, Case Development and Intelligence Records, DOL/OIG-11, contains appropriate routine uses and exemptions, the SORN will be updated to account for the DEMS BWC footage.

How is the information shared outside the Department and what security measures safeguard its transmission?

The procedures in U.S. DOL OIG Manual Investigative Notice (IN) 08-1900, section 8: Requests by AUSA will be followed. Additionally, if information is shared with an AUSA, OIG will encrypt the file and the drive and transmit via mobile media.

How is the information transmitted or disclosed?

The information will be transmitted electronically via mobile media from the DEMS server. All Data transmitted will be encrypted.

Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If the answer is yes, be prepared to provide a copy of the agreement in the event of an audit as supporting evidence.

Not at this time. All activities with BWC is governed by the search/arrest warrant approved and signed by the state and/or federal judge which is governed by the U.S. Constitution. There is no separate MOU between DOL-OIG and AUSA parties. The AUSA is a prosecutor for the criminal investigation which is part of the investigative team.

How is the shared information secured by the recipient?

Data shared with AUSA team as part of the criminal investigation will be shared with encryption and secured by the recipient through a case management system on their end.

What type of training is required for users from agencies outside DOL prior to receiving access to the information?

There is no external access to the system.

Privacy Impact Analysis

The privacy impact of the external sharing of DEMS information is consistent with the privacy impact of other external information sharing by OIG for law enforcement purposes. While sharing is limited, encryption of shared information protects PII while transferred between need-to-know personnel.

7. NOTICE

The following questions are directed at notice to the individual of the scope of PII collected, the right to consent to uses of said information, and the right to decline to provide information.

Was notice provided to the individual prior to collection of PII?

Yes. This Privacy Impact Assessment provides notice to individuals. Additionally, notice is provided through publication of a Modified System of Records Notice (SORN) for DOL/OIG-11. All SORNs are published on the DOL's website at: https://www.dol.gov/agencies/sol/privacy.

Do individuals have the opportunity and/or right to decline to provide information?

No.

Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No.

Privacy Impact Analysis

Although individuals are unable to decline to provide information or consent to particular uses, OIG takes the necessary steps to safeguard the information in DEMS, consistent with the uses described in this Privacy Impact Assessment and the SORN for DOL/OIG-11.

8. INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

What are the procedures that allow individuals to gain access to their own information?

The video footage are part of investigative records and individuals have no access to this information. In accordance with 5 U.S.C. 552a(j)(2), information compiled in DEMS is exempt from all of the provisions of the Privacy Act except the following sections: (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i). This material is exempt because the disclosure and other requirements of the Privacy Act would substantially compromise the efficacy and integrity of OIG operations in a number of ways.

What are the procedures for correcting inaccurate or erroneous information?

Because the collected information falls within the "law enforcement" exemption under the Privacy Act with respect to an individual's right to access, there are correspondingly no procedures for individuals to correct inaccurate or erroneous information. See 5 U.S.C. 552a(j)(2).

How are individuals notified of the procedures for correcting their own information?

Individuals are notified through this Privacy Impact Assessment and through the Modified SORN for DOL/OIG-11 that the records are exempted from access, redress, and correction.

If no formal redress is provided, what alternatives are available to the individual?

Due to the law enforcement purpose of the collection, no alternatives are available.

Privacy Impact Analysis

Due to the law enforcement exemption for individual access, redress, and correction provided in the Privacy Act, the privacy impact is consistent with that permitted under the Privacy Act. Appropriate safeguards are in place to protect the information from improper access, as described in other sections of this Privacy Impact Assessment.

9. TECHNICAL ACCESS AND SECURITY

Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Federal OIG law enforcement agents, their direct managers, and DEMS authorized system administrators only. The DEMS server employs a role-based security control to prevent unauthorized access to any media files. Only authorized application administrators can give permission to agents. This granular access control on an individual user level in addition to the encryption of data at rest and in-transmission provides the data protection from unauthorized access by application administrators. All OIG personnel with physical or logical access to these servers are Pre-employment Checks and Inquiries (PECI) cleared prior to obtaining access. All remote access is monitored and controlled by firewalls.

Will contractors to DOL have access to the system? If so, please include a copy of the

contract describing their role to the OCIO Security with this PIA.

No.

Does the system use "roles" to assign privileges to users of the system? If yes, describe the roles.

Yes, privileged user roles are managed through the DEMS Active Directory (AD). User groups are users, admin, managers and Assistant Special Agent-in Charge (ASAC)

What procedures are in place to determine which users may access the system and are they documented?

OIG has documented account management procedures that system administrators follow when assigning users to roles based on a need to know. Users are also terminated when they no longer require access to the system.

How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided? Provide date of last training.

Users are required to complete the OIG's Rules of Behavior training before permission is granted to the system. This training is performed annually by all users. Additionally, per U.S. DOL OIG IN 08-1900, section N Training: All Special Agents must attend an agency approved training to learn how to deploy BWCs properly and to ensure compliance within IN 08-1900. Additional training will be provided to ensure continued proficiency.

Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?

Users must take the DOL Computer Security Awareness Training annually as well as OIG's Rules of Behavior training before access is granted to the system per OIG policy. Privacy Awareness Training is conducted annually.

What auditing measures and technical safeguards are in place to prevent misuse of data?

DEMS has built-in real-time audit capabilities which also feed into OIG's enterprise audit logging system. Every action performed within the application is tracked and reviewed by OIG system administrators to prevent data misuse.

Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?

Yes. This is a new system, and the Security Assessment and Authorization currently is in progress.

Privacy Impact Analysis

OIG uses secure protocols to protect data in transit and at rest. Also, there is no public access to the system. These protection methods minimize the privacy risk to the data.

10. TECHNOLOGY

Was the system built from the ground up or purchased and installed?

Purchased in 2022 and installed by OIG BIT system administrators.

Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

DEMS was built to ensure the following: Must have end to end data at rest and in transit encryption footage, must be capable of uploading DEMS footage and other digital evidence via a tethered connection to an Agency issued laptop with WiFi. The application shall only be accessible by authorized users as designated by DOL-OIG policy.

What design choices were made to enhance privacy?

Access is limited to only connection to OIG network through the VPN. The necessity for encryption was built into the system to account for the possible privacy risks.

For systems in development, what stage of development is the system in, and what project development life cycle was used?

DEMS is not in the development stage.

For systems in development, does the project employ technology which may raise privacy concerns? If so please discuss their implementation?

DEMS is not in development.

11. DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

OIG OI completed the PIA for DEMS.

OIG-OI determined that the safeguards and controls built into DEMS and other DOL controls identified in the SORN for DOL/OIG-11 adequately protect the information.

OIG-OI determined that it is collecting the minimum necessary information for the proper performance of a documented agency function consistent with the mandate expressed in Executive Order 144074, "Advancing Effective, Accountable Policing and Criminal Justice Practices to

Enhance Public Trust and Public Safety." As a general matter, attempting to minimize the collection of PII to be included in a criminal investigative file is contrary to investigative practice which requires a full and complete inquiry and exhaustion of all potential sources of information. See 5 U.S.C. 552a(e)(1).

Signatures

Senior Agency Official for Privacy

Carolyn Angus-Hornbuckle
Digitally signed by Carolyn Angus-Hornbuckle
Date: 2023.12.15 17:51:35 -05'00'

Carolyn Angus-Hornbuckle
Assistant Secretary for Administration and Management

Reviewed by:

MARA BLUMENTHAL
Digitally signed by MARA BLUMENTHAL
Date: 2023.11.21 15:01:31 -05'00'

Mara S. Blumenthal
Manager, DOL Privacy Program
OCIO/OASAM

Prepared by:

EFUA COLECRAFT (Affiliate)
Digitally signed by EFUA COLECRAFT (Affiliate)
Date: 2023.11.13 10:29:11 -05'00'

Efua Colecraft
Privacy Officer, DOL OIG

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

What information about individuals will be collected, generated, shared, and/or retained? Also, note whether the collection is for (Check all that apply):

☒ Federal employees
☒ Contractor staff
☒ Members of the Public

PII Elements

☒Prefix or title, such as Mr., Mrs., Ms., Jr. Sr.
☒First name ☒ Middle initial and/or ☒Last name suffix such as Jr. Sr., etc.
☒Date of birth
☒ Place of birth
☐Mother's maiden name
☒SSN☒SSN [truncated] ☒SSN [elongated]
☒Language spoken
☒Military, immigration, or other government-issued identifier
☒Photographic identifiers (i.e., photograph image, x-rays, video)
☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
☒Other physical identifying information (e.g., tattoo, birthmark)
☒Vehicle identifier (e.g., license place, VIN)
☒Driver's license number
☒Residential address
☒Personal phone numbers (e.g., phone, fax, cell)
☒Mailing address (e.g., P.O. Box)
☐ Personal e-mail address
☐ Business address
☐Business phone number (e.g., phone, fax, cell)
☐ Business e-mail address
☐Medical information including physician's notes
☐ Medical record number
☐Device identifiers (e.g., pacemaker, hearing aid)
☐Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
☐Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
☐Certificates (e.g., birth, death, marriage)
☐Legal documents or notes (e.g., divorce decree, criminal records)
☐ Educational records
☐Network logon credentials (e.g., username and password, public key certificate)

☐Digital signing or encryption certificate
☒Other: _____
☐ None