U.S. Office of Personnel Management

Privacy Impact Assessment for

Axon Cloud Services (ACS)

October 31, 2025

Contact Point
Robin Thottungal
Chief Information Officer
Office of the Inspector General

Reviewing Official
Becky Ronayne
Senior Agency Official for Privacy

Abstract

The Office of the Inspector General (OIG) is an independent office within the U.S. Office of Personnel Management (OPM) and has a statutory mission to provide objective oversight of OPM programs and operations. The Axon Cloud Services (ACS) system is administered and operated by the OIG Office of Investigations. ACS provides on-officer video capture, secure digital media storage and management, and paperless tracking and reporting. This Privacy Impact Assessment (PIA) is required because the ACS system maintains personal information in identifiable form.

Overview

In accordance with Executive Order 14074, Advancing Effective, Accountable Policing, and Criminal Justice Practices to Enhance Public Trust, Special agents of the U.S. OPM OIG, Office of Investigations (OI) must utilize body-worn cameras to record their actions during the tactical portion of enforcement operations (i.e., arrest and search warrants). The ACS system provides two interconnected technology solutions to satisfy this requirement: the camera devices and the associated information system. The cameras that OI agents wear are Axon Enterprise, Inc (Axon) cameras, and the associated information system is the FedRAMP-authorized Software as a Service (SaaS) Axon cloud platform Evidence.com. Axon cameras allow video to be directly uploaded to the cloud platform via a docking station where the video footage can be accessed in accordance with access control policies.

The Axon Digital Evidence Management System (DEMS) is an enterprise, commercial-off-the-shelf, end-to-end law enforcement camera and digital evidence management system. The DEMS provides an integrated system of cameras, compatible software, and mobile applications to enable OPM OIG

law enforcement officers to download, catalog, tag, manage, and store associated digital evidence.

The OIG implemented specific technical design, access control, and audit logging controls that provide enhanced protection for the sensitive data stored in the system. The ACS system is hosted at a secure data center managed by the vendor. The evidence management application for ACS is administered by OPM OIG IT personnel in coordination with vendor support. Information in ACS is restricted and only permits OIG employees to access information required in the performance of the employees' duties. OIG management uses reports from the system internally to track, evaluate, and manage program operations, and as a basis for reporting investigative results and statistics internally and externally. Limited reports on investigative activities are shared as required by law or as otherwise appropriate to support the OIG's mission, including with the U.S. Congress, DOJ, other law enforcement partners, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE). CIGIE is a federal entity that was created by the Inspector General Act of 1978 to, among other purposes, respond to allegations of wrongdoing that are made against Inspectors General and certain staff.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The IG Act, 5 U.S.C. § 401 et seq., establishes the OIG and sets forth its purpose, duties, and authorities. Most pertinently, the IG Act authorizes the OIG, in the course of carrying out its statutory responsibilities, "to have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available to [OPM] which relate to [OPM] programs and operations," (5 U.S.C. § 406(a)(1)); "to make such investigations and reports relating to the administration of the programs and

operations of the applicable establishment" as the Inspector General determines to be "necessary or desirable," (5 U.S.C. § 406(a)(2)); "to make an arrest without a warrant while engaged in official duties as authorized under this chapter or other statute, or as expressly authorized by the Attorney General, for any offense against the United States committed in the presence of such Inspector General, Assistant Inspector General, or agent, or for any felony cognizable under the laws of the United States if such Inspector General, Assistant Inspector General, or agent has reasonable grounds to believe that the person to be arrested has committed or is committing such felony" (5 U.S.C. § 406(f)(1)(b)); to "seek and execute warrants for arrest, search of a premises, or seizure of evidence issued under the authority of the United States upon probable cause to believe that a violation has been committed" (5 U.S.C. § 406(f)(1)(C)) and "to administer to or take from any person an oath, affirmation, or affidavit," (5 U.S.C. § 406(a)(5)).

Executive Order 14074, "Advancing Effective, Accountable Policing, and Criminal Justice Practices to Enhance Public Trust and Public Safety," requires that federal law enforcement agencies ensure the appropriate use of body-worn cameras and advanced law enforcement technologies.

Executive Order 9397, as amended by Executive Order 13478, permits the collection and use of Social Security Numbers (SSNs).

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

SORN, OPM/CENTRAL-4 Inspector General Investigations Case Files, applies to information maintained in this system.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes, ACS system security plan was updated in January 2025.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. DAA-0478-2019-0002, Records of the Office of the Inspector General for the United States Office of Personnel Management.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The PRA does not apply to the collection of information during the conduct of an audit, investigation, inspection, evaluation, or other review conducted by any Office of Inspector General per the IG Act, 5. U.S.C. § 406(k).

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, or maintains.

ACS contains investigative, personnel (support), and administrative data collected by the OIG. The system includes numerous types of information about individuals, including name, address, SSN, telephone number, e-mail address, photograph, or other unique identifying number, code, or characteristic, gender, race, date of birth, place of birth, geographic indicator, license number, vehicle identifier including license plate, and other descriptors. Other information about individuals, such as financial account numbers, medical, educational, or personal records, may be incidentally captured by body-worn cameras used during OIG operations. Any disclosure of information from ACS to external parties will be reviewed and redacted in accordance with applicable authorities if necessary.

Information contained in ACS may be about U.S. citizens, current or former Federal employees, Federal contractors and contractor employees, complainants, witnesses, subject matter experts, law enforcement partners,

and other persons relating to OPM programs and operations. Information may be about living or deceased individuals.

2.2. What are the sources of the information and how is the information collected for the project?

Information in ACS is collected primarily through the body-worn cameras OIG employees use. All OPM OIG special agents complete initial and recurring training related to body-worn camera deployment, use, and operation. Body-worn cameras will be activated at the beginning of a law enforcement action. Activation will generally be when approaching the persons or premises that is the subject of the operation for preplanned arrests or searches. Body-worn cameras will be programmed to record for a specified period upon activation and after deactivation.

Metadata and other information necessary for evidence management may also be stored within ACS. The sources of this information include direct collection from the individual record subjects, complainants, or third parties with information pertinent to OIG investigative activities (including witnesses and other entities having some relationship with the record subject); the files of OPM offices and their systems of records; other Federal, state, and local agencies; and non-government record sources; including commercial databases that provide public records search and link analysis capabilities.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ACS does not directly connect with any commercial or publicly available data sources; however, OIG investigative staff utilize commercial and publicly available data sources during their investigative activities. These data sources may be used to obtain information that is used to corroborate evidence and to identify and locate potential subjects, witnesses, and record sources. The source of the information is generally noted when the

incorporation of the information is recorded pursuant to standard OIG procedures regarding the evidential documenting of investigative activities.

2.4. Discuss how accuracy of the data is ensured.

Information obtained during OIG investigative activities is verified through the investigative process; information is subject to evaluation and scrutiny by OIG investigative staff and verified against information collected from other records sources. Accuracy is further ensured by supervisory reviews of investigative activity.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the information in ACS will be inaccurate or incomplete.

Mitigation: This risk is mitigated by standard investigative procedures whereby OIG investigative staff validates information obtained by verifying the information against other records sources. These procedures are reinforced by internal policies, external guidelines (including the CIGIE Quality Standards for Investigations), and supervisory reviews of investigative activities.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

Information collected and maintained in ACS is used to comply with Executive Order 14074 and the OIG policies implementing that executive order's requirements. The audio and video information collected by OIG body-worn cameras is collected to improve public trust, transparency, and accountability, as well as to provide an additional layer of safety for OPM OIG special agents.

Body-worn camera recordings may be accessed by OPM OIG special agents when it is reasonable and necessary to document activities, conduct internal investigations, facilitate training, or for public disclosure in certain instances.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

ACS employs a search function that enables OIG staff to identify commonalities between different investigative activities, thereby allowing for the identification and consolidation of duplicative activities and the efficient assignment of duties. ACS is also capable of producing reports, which are used internally to track, evaluate, and manage OIG program operations and externally to convey OIG investigative statistics, as required by law, or as otherwise appropriate to support the OIG's mission.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

No. ACS access is limited to OIG personnel. No other OPM offices or programs have a need to access the system's information.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that an authorized person may access the information for an unauthorized purpose and that PII may be accessed or used inappropriately or in a manner not consistent with the original program's purpose or the user's specific mission area and authority.

Mitigation: This risk is mitigated by limiting access according to user roles and work assignments, by documenting disclosures, and using built-in audit logs that document users' access to information. This risk is further mitigated by supervisory investigative staff reviews. Additionally, all OIG employees authorized ACS access must take prerequisite OPM OIG training, including an ethics briefing. Users are also required to comply with and

acknowledge OIG-specific rules of behavior to access ACS and other OIG IT resources.

Privacy Risk: There is a risk that individuals who do not have a need to know the information in the investigative process will access and use the information for unauthorized purposes.

Mitigation: This risk is mitigated by limiting access according to user roles and work assignments, by documenting disclosures, and using built-in audit logs that document users' access to information. These logs are checked to ensure that the system is not accessed inappropriately. User access is based on express permission and the OPM OIG limits access to those employees with a need-to-know basis. There are also multiple layers of physical and IT protections that are used to safeguard the information in ACS. Physical security on the premises ensures that only authorized individuals have access to OIG offices and ACS hardware. Firewalls and data encryption methods ensure the data can only be accessed by authorized OIG personnel. Limiting access to only those cases for which there is a need to know further prevents against unauthorized access or use.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

ACS is primarily a tool used during the conduct of investigations by OIG investigators. Executive Order 14074 requires OIG investigators to activate body-worn cameras in various situations where it would not be feasible from an operational or security perspective to provide notice prior to activation. However, notice is provided in the SORN identified in section 1.2. Additionally, body-worn cameras will be conspicuously worn, and polices regarding the collection, maintenance, and use of body-worn camera footage (including the OIG's body-worn camera policy, this PIA, and the SORN identified in section 1.2) will be provided on request.

With respect to certain categories of information, such as that contained in administrative and personnel records of OPM or other Federal agencies, notice is provided at the initial point of collection.

4.2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Insofar as information is obtained directly from the record subject, individuals may have the opportunity to decline to provide information. OIG criminal investigators are trained as to investigative subjects' rights and obligations when responding to OIG inquiries, and the OIG has policies in place to ensure that subjects are made aware of those rights, as appropriate.

In instances where information is obtained by the OIG from other record sources (including witnesses, commercial or publicly available databases, and Federal systems of records) the individual generally is not provided the opportunity to consent or object to the OIG's collection. Providing individuals additional specific notice at the point of collection of information could negatively impact the investigative activities of the OIG by, for example, alerting the subjects of criminal investigations as to the Government's prosecutorial strategies or the nature of evidence collected.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not receive adequate notice concerning how their information is used in ACS and individuals may not be aware that the system collects and uses their information.

Mitigation: This risk is partially mitigated with the notification regarding the collection, maintenance, and use of information contained in this system is provided through publication of this PIA and the SORN listed in section 1.2, above. Individuals wishing to learn whether this system contains

information about them may contact the system manager. However, notice and consent may not be possible in certain circumstances, due to the risk of alerting the subjects of investigations as to the Government's prosecutorial strategies or the nature of evidence collected, which could inhibit or detrimentally affect the OIG's capacity to detect unlawful activity.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

Information in ACS is retained in accordance with the NARA retention schedule noted in section 1.4, above.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by adherence to the established retention schedule and documented guidance from NARA, which clearly defines retention requirements by record type and agency.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Any information sharing from ACS comports with the statutory responsibilities of the IG Act, 5 U.S.C. § 401 et seq., which authorizes the audit, investigation, and evaluation of OPM programs and operations and the collection of related information.

Information in ACS is regularly shared with DOJ pursuant to the IG Act, 5 U.S.C. § 404(d), which requires the OIG to "report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal criminal law;" and to otherwise support the criminal and civil prosecution of violations of law impacting or relating to OPM programs and operations.

Information is also shared, as appropriate, with other Federal, state, and local agencies (including other Federal Offices of Inspectors General) pursuant to joint investigations involving OPM programs and operations or where the OPM OIG becomes aware of an indication of a violation or potential violation of law falling within the jurisdiction of the agency.

Information in ACS is also shared to comply with various reporting requirements, including the annual report required by the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority and the semiannual report to Congress required by the IG Act, 5 U.S.C. § 405.

Finally, information is subject to release in response to Freedom of Information Act requests, Privacy Act Requests, or in accordance with the requirements of Executive Order 14074, as implemented by OPM OIG policies.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Insofar as the information sharing described in section 6.1 implicates Privacy Act-protected information and is not otherwise permitted by the conditions for disclosure enumerated at 5 U.S.C. § 552a(b), it is permitted by the routine uses listed in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files, or incorporated by reference from the Prefatory Statement of Routine Uses for OPM's Internal and Central Systems of Records. The predominant routine uses include:

- For Law Enforcement Purposes--To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where OPM becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

- For Litigation--To disclose information to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which OPM is authorized to appear, when: (1) OPM, or any component thereof; or (2) Any employee of OPM in his or her official capacity; or (3) Any employee of OPM in his or her individual capacity where the Department of Justice or OPM has agreed to represent the employee; or (4) The United States, when OPM determines that litigation is likely to affect OPM or any of its components; is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice or OPM is deemed by OPM to be relevant and necessary to the litigation provided, however, that the disclosure is compatible with the purpose for which records were collected.

- For the Merit Systems Protection Board--To disclose information to officials of the Merit Systems Protection Board or the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions, e.g., as promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

- To any source from which information is requested in the course of an investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

6.3. Does the project place limitations on re-dissemination?

Disclosures from ACS may be accompanied by a notice advising against further release without the prior authorization of the OPM OIG. It is also possible to give someone access to information in ACS, but not give them the ability to reshare that information.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

Disclosures outside the OIG are recorded in ACS pursuant to the OIG's standard investigative procedures, which require OIG investigative staff to timely document actions taken pursuant to an investigative activity within the ACS entry associated with that investigative activity. Records of disclosures note the information disclosed, the individual effecting the disclosure, the entity to whom the information was disclosed, and the date on which the disclosure was made.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in OIG ACS will be shared with a third party and used or disseminated for a purpose that is not consistent with the purpose for which it was collected.

Mitigation: This risk is mitigated by the implementation of internal OPM and OIG guidance and policies on the release of information, and by limiting releases to the extent necessary to facilitate OPM OIG investigative activities; to support civil, criminal, or administrative prosecutions resulting from or related to OIG investigative activities; to meet reporting requirements; and to comply with various information-disclosure authorities. This risk is further mitigated by limiting OIG employees' access to information in ACS according to the duties of their positions.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

Access to ACS information is limited because investigative information and certain records in ACS are exempt from access (including access to an accounting of disclosures) provisions of the Privacy Act, 5 U.S.C. § 552a(c)(3) and (d). 5 C.F.R. § 297.501(b)(1), OPM's rule implementing the Privacy Act within OPM, further discusses these limitations. Certain information may be released in accordance with Executive Order 14074, which provides for expedited public release of footage depicting death or serious bodily injury. Individuals seeking to access records in ACS pertaining to themselves may contact the ACS system manager, as noted in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

There is limited opportunity to amend investigative information and certain records in ACS because they have been exempted from the amendment provisions of the Privacy Act, 5 U.S.C. § 552a(d). 5 C.F.R. § 297.501(b). Individuals seeking to amend records in ACS pertaining to themselves may contact the ACS system manager, as noted in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files.

7.3. How does the project notify individuals about the procedures for correcting their information?

The procedures for individuals to correct information are described in the SORN for OPM/CENTRAL-4, Inspector General Investigations Case Files and in this PIA.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have the opportunity to access or amend inaccurate information maintained by other agencies and

submitted to ACS. Furthermore, there is a risk that individuals may not be able to access or amend video recordings captured by body-worn cameras and stored in ACS.

Mitigation: Furthermore, to the extent that body-worn camera footage becomes part of a legal proceeding (e.g., as an exhibit in a court of law) or is publicly released, the individuals depicted in the footage may have the ability to provide their interpretation of the events captured by the footage. This risk cannot be completely mitigated since providing individuals the opportunity to access or amend information in ACS could negatively impact the investigative activities of the OIG by, for example, alerting the subjects of criminal investigations as to the Government's prosecutorial strategies or the nature of evidence collected. Further, the accuracy or relevance of information obtained during an investigation may not be readily apparent at the time of collection. Accordingly, allowing the premature amendment of information could inhibit or detrimentally affect the OIG's capacity to detect unlawful activity. Finally, given that video, audio recordings, and metadata captured by body-worn cameras are intended to provide an accurate recording of an event, individuals' ability to amend this type of information is necessarily limited. However, these risks are partially mitigated by the publication of instructions on the OPM website, in this PIA, and in the SORN listed in section 1.2, above, to inform individuals about how to request access to and amendment of their records, notwithstanding that certain records in this system have been exempted from the access and amendment provisions of the Privacy Act.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

ACS user access is based on express permission and the OPM OIG limits access to information to those employees with a need to know the information in the performance of their duties. Users are assigned roles, which have access privileges according to the user's duties and assigned investigative activities. There are also multiple layers of physical and IT protections that are used to safeguard the information in ACS. Physical security on the premises ensures that only authorized individuals have unaccompanied access to OIG offices. Firewalls and data encryption methods ensure the data can only be accessed by authorized OIG personnel.

ACS employs built-in audit logs that document users' access to information. These logs are checked to ensure that the system is not accessed inappropriately.

Adherence to the stated practices in this PIA is further ensured by internal OIG policies describing employees' responsibilities with respect to the maintenance and use of information, and by the provision of privacy training described in section 8.2, below. Additionally, not less than once every three years, the OIG Office of Investigations is subject to peer review by another Federal Office of Inspector General, which evaluates adherence to the CIGIE Quality Standards for Investigations. OIG records management practices may be assessed as part of this triennial peer review, the results of which are made publicly available on the OIG's website.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees receive annual training on IT security and privacy awareness, which includes instruction on the proper handling of PII. All OIG employees authorized ACS access are required to have certain OIG training,

including an ethics briefing as a prerequisite. Users are further required to learn and acknowledge specific rules of behavior governing access to ACS and other OIG IT resources. Once granted access to ACS, employees are provided additional training on their user roles.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

ACS user access is based on express permission and access to information is limited to those OPM OIG employees with a need to know the information in the performance of their duties. Access is limited solely to OIG employees, who are granted access to ACS and assigned roles by system administrators only after receiving the instruction described in section 8.2, above. ACS users' access is further limited within the system to information pertaining to their assigned duties during the pendency of those duties. Firewalls and data encryption methods ensure the data can be accessed by authorized OIG personnel only.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

The OIG does not have any information sharing agreements that pertain to the disclosure of information from this system, nor is access to ACS granted to non-OIG employees. Any new uses of the information, memoranda of understanding, information sharing agreements, or provisions of access would be reviewed by OIG senior level management, to ensure that the contemplated change aligns with the OIG's mission, that necessary technical safeguards are in place, and that all legal requirements are met.

Responsible Officials

Krista Boyd

Inspector General

U.S. Office of Personnel Management

Approval Signature

Becky Ronayne

Senior Agency Official for Privacy