Office of Justice Programs

Privacy Impact Assessment
for the
OJP Automated Electronic Guard Information System (OJP AEGIS)

Issued by:
Maureen Henneberg

Approved by: Andrew J. McFarland
Senior Counsel, Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 11, 2026

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Office of Justice Programs Automated Electronic Guard Information System (OJP AEGIS) provides integrated supervision of technological functions that provides physical access controls and monitoring for both exterior perimeter and internal access points. The system consists of resilient access control servers, a security guard monitoring station, an administrative and coding workstation, and peripheral access control units, such as badge readers or some other form of secured access readers and motion detectors for both internal and external secured access points. The system includes security surveillance cameras in operation throughout the OJP building which only capture video (no audio is recorded).

This Privacy Impact Assessment (PIA) was undertaken due to the system's collection, maintenance, and dissemination of Personally Identifiable Information (PII). Its purpose is to assess how the system manages user data, ensures secure access controls, and addresses potential privacy concerns related to the use and sharing of personal information within the OJP facility. This assessment is geared towards safeguarding privacy while upholding effective access controls.

Section 2: Purpose and Use of the Information Technology

The OJP AEGIS collects data from individuals with PIV cards who have undergone a secured clearing process. This information, including unique identifiers generated by the National Finance Center (NFC), is used to manage user access to physical access points within the OJP facility located on 999 North Capitol Street, NE Washington, DC, 20002. The purpose of collecting this data is to provide physical control capabilities for the OJP site. The information is utilized through the enrollment workstation, where a user's PIV card authorizes access to various doors within the facility. Access authorizations are stored in the OJP AEGIS database, and logs are generated for successful and unsuccessful access attempts. The primary goal is to enhance security by ensuring that only authorized individuals with proper clearance can access specific areas within the OJP facility. The system aids in criminal and civil law enforcement purposes, and administrative matters related to maintaining a secure environment. The collected data allows for analyses to identify potential concerns or patterns, contributing to the overall security and functionality of the OJP site.

2.1 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	28 U.S.C. § 530C; 34 U.S.C. 10102
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C & D	First Names, Middle Names, and Last Names of Employees and Visitors
Date of birth or age	X	A & B	Dates of Birth (DOB) of Employees
Place of birth			
Gender			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A & B	When the credentialing center enrolls the PIV badge to the OJP AEGIS system, the center adds the employee's SSN to the record in OJP AEGIS.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			

Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			

Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			Company/organization, department (if federal), phone number, and email of staff.
Location information, including continuous or intermittent location tracking capabilities	X	A and B	• Dates and times of entry • Exit and passage through control points
Biometric data:			Security surveillance cameras are in operation throughout the OJP building. Cameras do not record audio. Photo is also on employees' PIV cards, only registered in the memory of the system. There is no data at rest.
- **Photographs or photographic identifiers**	X	A, B, C and D	
- **Video containing biometric data**	X	A, B, C and D	
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			

- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			Users' IDs and passwords will be stored by the system.
- **User ID**	X	A & B	
- **User passwords/codes**	X	A & B	
- **IP address**			
- **Date/time of access**	X	A & B	
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A & B	• Badge number • Unique Identifier for Federal Employees and Non-Social Security ID generated by National Finance Center (NFC) • Company/organization, department (if federal), phone number, and email of staff.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the Component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X	N/A	N/A	Official Investigative Inquiry
DOJ Components	X	N/A	N/A	Official Investigative Inquiry
Federal entities	X	N/A	N/A	Official Investigative Inquiry
State, local, tribal gov't entities	N/A	N/A	N/A	N/A
Public	N/A	N/A	N/A	N/A
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	N/A	N/A	N/A	N/A
Private sector		N/A	N/A	N/A
Foreign governments	N/A	N/A	N/A	N/A
Foreign entities	N/A	N/A	N/A	N/A
Other (specify):	N/A	N/A	N/A	N/A

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

OJP AEGIS utilizes the Federal Register System of Records Notices (SORNs) listed in section 7.2

to offer general notice to the public and provides Privacy Act § 552a(e)(3) notice for individuals visiting the building. No additional notifications or disclaimers are employed by OJP AEGIS.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Although participation in the collection, use or dissemination of information in the system is voluntary, entry to OJP offices is conditioned upon the provision of such information from employees and contractors. Accordingly, to the extent that individuals have a choice in the collection of this information, choosing to not participate will result in a denial of access, and in the case of employees and contractors, a possible termination of employment.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Requests for access or amendment of records must be made in writing, clearly marked as a "Privacy Act Request," and sent to designated address provided in DOJ-011 69 FR 70279 (12-03-2004).

The requester's identity must be verified through notarization or submission under 28 U.S.C. 1746. Additionally, individuals can contest or amend information maintained in the system by directing their request to the appropriate system manager, providing clear reasons for contesting and proposed amendments.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** ATO granted on 12/03/2024 and expires on 12/03/2027. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the Component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** OJP AEGIS is categorized as a Moderate impact system in accordance with guidance provided in FIPS 199 based on the type of information collected and stored to maintain the confidentiality, integrity, and availability of information in the system.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** OJP has integrated IT security continuous monitoring, an essential component of the risk management process. This involves assessing and analyzing security controls and risks through Enterprise Network System (ENS), given that OJP AEGIS operates as a subsystem within ENS. These assessments are validated by OJP at a frequency that ensures support for risk-based security decisions, thus effectively safeguarding the information.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The audit logs are ingested by Splunk and are subject to review in alignment with Department and Component policies and procedures.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
	Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

OJP AEGIS adheres either directly or through inherited and hybrid controls the suite of Access Control (AC), Audit and Accountability (AU), Identification and Authentication (IA), Physical and Environmental Protection (PE), Risk Assessment (RA), System and Communications Protection (SC), and System and Information Integrity (SI).
Of these, the implemented controls are as follows:

AC-03: Access Enforcement
AC-03(14): Individual Access
AC-05: Separation of Duties

AC-06: Least Privilege
AC-11(1): Pattern-hiding Displays
AC-17: Remote Access
AC-17(2): Protection of Confidentiality and Integrity Using Encryption
AU-03(3): Limit Personally Identifiable Information Elements
IA-02(1): Multi-factor Authentication to Privileged Accounts
IA-02(2): Multi-factor Authentication to Non-privileged Accounts
IA-06: Authentication Feedback
IA-07: Cryptographic Module Authentication
IA-08: Identification and Authentication (non-organizational Users)
PE-08(3): Limit Personally Identifiable Information Elements
RA-05: Vulnerability Monitoring and Scanning
RA-08: Privacy Impact Assessments
SC-02: Separation of System and User Functionality
SC-07: Boundary Protection
SC-07(3): Access Points
SC-08: Transmission Confidentiality and Integrity
SC-12: Cryptographic Key Establishment and Management
SC-18: Mobile Code
SC-23: Session Authenticity
SC-39: Process Isolation
SI-02: Flaw Remediation
SI-04(2): Automated Tools and Mechanisms for Real-time Analysis
SI-07(1): Integrity Checks

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Records in this system are retained and disposed of in accordance with the National Archives and Records Administration, General Records Schedule 5.6: Security Management Records "Security Management involves the physical protection of an organization's personnel, assets, and facilities (including security clearance management). Activities include security operations for protecting agency facilities, staff, and property; managing personnel security; and insider threat protection."

OJP AEGIS aligns with item 090: Facility security management operations records. Records about detecting potential security risks, threats, or prohibited items carried onto federal property or impacting assets, including records documenting access control, screening, patrol and response, and control center operations.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records"

maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. X Yes.

7.1 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

(1) DOJ-011, "Access Control System (ACS)," 69 Fed. Reg. 70279 (Dec. 3, 2004), available at https://www.govinfo.gov/content/pkg/FR-2004-12-03/pdf/04-26590.pdf; and

(2) GSA/GOVT-7, "HSPD-12 USAccess," 80 Fed. Reg. 64416 (Oct. 23, 2015), available at https://www.federalregister.gov/documents/2015/10/23/2015-26940/privacyactof-1974-notice-of-an-updated-system-of-records.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

In order to mitigate the risk of over-collection of personal information, the system minimizes the amount of sensitive data stored and accessed. Records are maintained and disposed of in accordance with National Archives and Records Administration guidelines. This ensures that information is retained only for as long as necessary and securely disposed of when no longer needed, reducing the risk of unauthorized access or misuse.

Records are maintained in limited access spaces within DOJ-controlled facilities, and computerized data is password protected. Only authorized DOJ personnel or properly authorized non-DOJ personnel can access the information, reducing the risk of unauthorized access. Administrative, technical, and physical controls are in place to safeguard the information. This includes background investigations for DOJ personnel, security and emergency protocols overseen by the Director of Security and Emergency, and adherence to privacy and security policies and procedures.

Information is disclosed only under specific circumstances outlined in applicable regulations and policies, such as to law enforcement authorities or governmental entities engaged in collecting law enforcement or national security intelligence information. Disclosure to other entities is based on necessity and requires proper authorization, minimizing the risk of unauthorized sharing.