United States Department of Justice

Justice Management Division

Privacy Impact Assessment
for the
Justice Enterprise Data Integration & Business Intelligence Portal – Next Generation

Issued by:

John E. Thompson
Deputy General Counsel

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: May 27, 2026

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Justice Enterprise Data Integration & Business Intelligence Portal – Next Generation (JEDI-NG) system stores and processes payroll, financial, and procurement data from Unified Financial Management System (UFMS)/Momentum, which is the official accounting and procurement system of the Offices, Boards and Divisions OBDs), Office of Justice Programs (OJP), Bureau of Prisons (BOP), and the United States Marshals Service (USMS). The system provides analysis services built from a cloud-based software solution that loads, stores, manages, and reports on data. UFMS provides core reporting, based on Momentum, while JEDI provides more detailed reporting. The system utilizes an Extract, Transform, Load (ETL) tool and database that extracts core data fields from UFMS/Momentum ODS (Operational Data Store) and structures the data in a columnar data warehouse, making reporting and analysis more efficient. This data mart provides the Financial Systems Support Group of JMD with ad hoc data and may feed other systems with UFMS data as needed. The JEDI-NG team will continue to build upon establishing direct data connections to external data sources, for example, Treasury's Governmentwide Treasury Account Symbol (GTAS), G-Invoicing, and Central Accounting Reporting System (CARS). JMD may utilize this database for advanced analytics and automated reporting; therefore, the solution must be capable of developing and delivering reports. The PIA was conducted because JEDI-NG reports payroll and financial data that includes personally identifiable information (PII).

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

JEDI-NG stores payroll, financial, and procurement data from UFMS, hosted via Amazon Web Services (AWS), also referred to as UFMS-AWS or /Momentum). UFMS-AWS is the official financial and acquisitions management system for the Department of Justice (Department or DOJ), excluding the Federal Bureau of Investigation (FBI) and Federal Prison Industries (UNICOR). The system is used for data analysis, budget analysis, and business forecasting, and is built from a cloud-based software solution that

will load, store, manage, and optionally report data. JEDI-NG utilizes an ETL tool and database, which extracts core data fields from UFMS/Momentum ODS and structures the data in a columnar data warehouse that will make it easier to report on and analyze the data.

2.2 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	*The Chief Financial Officers Act of 1990, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990);Anti-Deficiency Act*, Pub. L. 97–258, 96 Stat. 923 (Sept. 13, 1982); *The Federal Financial Managers Integrity Act*, Pub. L. No. 97-255, 96 Stat. 814 (Sept. 8, 1982). The Federal Information Security Modernization Act of 2014 (FISMA), 31 U.S.C. § 3512; 44 U.S.C. § 3101; 44 U.S.C. § 3551 et seq.;
Executive Order	Executive Order No. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (2011); Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017)
Federal regulation	OMB Circular A– 130, Managing Information as a Strategic Resource (2016); OMB Memorandum M–17–12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017); OMB Memorandum M–20–32, Improving Vulnerability Identification, Management, and Remediation (Sept. 2, 2020).
Agreement, memorandum of understanding, or other documented arrangement	*Preparation, Submission, and Execution of the Budget*, OMB Circular A-11; *Management's Responsibility for Enterprise Risk Management and Internal Control*, OMB Circular A-123; and *Financial Reporting Requirements*, OMB Circular A-136.
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	First Name, Last Name
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A	Truncated via UFMS
Tax Identification Number (TIN)	X	A, B & C	Tax Identification Numbers processed via UFMS.
Driver's license			
Alien registration number			
Passport number	X	A, B	
Mother's maiden name			
Vehicle identifiers			
Business contact information, e.g. email address, phone number, business address	X	A, B	DOJ email addresses used to forward JEDI-NG reports to users.
Personal contact information, e.g., email address, phone number, home address			
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	A, B	Credit Card and Taxpayer information processed via UFMS
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar 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
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	X	A, B	Basic information regarding DOJ issued contracts to vendors who DOJ
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			

(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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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		Hard copy: mail/fax		Online	
Phone		Email			
Other (specify): Not applicable. Data is not collected directly from individuals; instead, it is transferred from UFMS to JEDI-NG on a daily basis. JEDI-NG does not maintain records of this data.					

Government sources:					
Within the Component	X	Other DOJ Components		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): Data is transferred from UFMS (a DOJ system) to JEDI-NG on a daily basis. JEDI-NG does not maintain records of this data.					

Non-government sources:					
Members of the public		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	Access is limited to the roles requested and approved on the user access request form.
DOJ Components			X	Data is transferred from UFMS-AWS to JEDI-NG on a daily basis. JEDI-NG does not create or permanently store separate copies of the data; it functions as a reporting and analysis layer that reflects UFMS-AWS information.
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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.

No information is released or shared with the public for open data, research, or statistical purposes.

Section 5: Notice, Consent, Access, and Amendment

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

JEDI-NG does not collect information directly from individuals. Individualized notice will be provided by the source systems that feed into JEDI-NG. The publication of this PIA and the SORNs listed in section 7.2 provide general notice of the collection, use, and maintenance of UFMS information to include PII.

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.

As a Department-wide financial/procurement reporting system, JEDI-NG does not collect information directly from individuals. Therefore, any opportunities to voluntarily participate in the collection of PII will be handled by the source system.

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.

JEDI-NG does not collect information directly from individuals; therefore, requests for access and amendment of PII contained in JEDI-NG must be made to the source system. JEDI-NG users have access to the information in the system pertaining to their JEDI-NG role (as noted per the access request), which could contain their own PII. User profile data can only be updated by a system administrator. A system administrator cannot update their own profile. System administrators are required to submit an approved access request for updates to be made by another system administrator other than themselves.

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) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** 12/7/2023 – 12/7/2026. **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 information or information 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 NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** JEDI-NG was assigned a moderate security categorization rating and security control baseline based on identified information types, AWS GovCloud customer controls, SAP NS2's complementary user entity controls (CUECs), DOJ common controls program, and Justice Unified Telecommunications Network (JUTNet) offered controls.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The Finance Staff provides oversight and monitoring of the security controls on an ongoing basis and informs the Information System Security Officer when changes occur that impact the security of the system.
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:** JEDI-NG utilizes SPLUNK or similar agents as per JMD requirements as a mechanism to audit review, analysis, and reporting on a weekly basis. This is key for identifying suspicious activities. Each EC2 instance will be configured with the Splunk Universal Forwarder or similar agents to send audit logs to JMD Finance Staff Cybersecurity Services for review, analysis, and reporting processes. Audit logs will be integrated as per JMD guidelines to provide ability to review, analyze , and report on suspicious activities.

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**.
X	**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:** Within the UFMS training, there is a portion that covers JEDI-NG, as well as a self-guided training overview and job aids available on the JMD Financial System Support page.

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?

Federal employees are required to review and acknowledge a consent and system use notice before accessing the system. DOJ Login[1] displays a notice to users prior to granting system access. The system uses a notification message that provides appropriate privacy and security notices (consistent with DOJ privacy and security policies) and remains on the screen until the user takes explicit action to log onto the financial reporting system. Users are granted access based on least privileged role permissions necessary to perform their job functions and requests are scrutinized to ensure there are no segregation of duties (SoD) conflicts. Accounts are monitored weekly to identify any conflicts and recertified annually to determine whether least privilege and SoD security principles are followed. Per security control, Protection of Information at Rest, customer data is encrypted during transmission. System-related information that requires protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information.

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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

Retention requirements cover the full life cycle of information, extending beyond system disposal in some cases. Information to be retained may also include policies, procedures, plans, reports, data output from control implementation, and other types of administrative

[1] DOJ Login is covered by separate privacy documentation here: https://www.justice.gov/opcl/media/1347416/dl?inline.

information. The National Archives and Records Administration (NARA) provides federal policy and guidance on records retention and schedules.

The data retention period for UFMS data follows the NARA approved General Records Schedule (GRS), and is as follows:

- Accounting data: 6 years (GRS 1.1)
- Procurement records: 3 years (GRS 1.1)
- Personnel records: 1 year (GRS 2.4)
- System Access Records 6 years (GRS 3.2)

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.

7.2 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:

DOJ-002, DOJ Information Technology, Information System, and Network Activity and Access Records (86 FR 37188) (7-14-2021)

DOJ-001, Accounting Systems for the Department of Justice, 69 FR 31406 (6-03-2004),

JMD-003, Department of Justice Payroll System, 69 FR 107 (1-02-2004).

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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules):***
- ***Sources of the information:***
- ***Type of technology employed (e.g. AI/ML):***
- ***Specific uses or sharing:***
- ***Privacy notices to individuals***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information:***

Data minimization: UFMS has data validation routines built into the interface that check for required fields, data types, and data ranges. JEDI utilizes an ETL tool and database that extracts core data fields from UFMS/Momentum ODS and structures the data in a columnar data warehouse, facilitating more efficient reporting and analysis. The business logic layer processes data before it is committed to the database, checking the data against business logic for accuracy and consistency. NARA General Records Schedules cover the data retention periods contained in the system.

Lifecycle Security: Requirements regarding integrity, privacy, and security were assessed throughout the system development lifecycle, including product selection, acceptance testing, system categorization, risk assessment, requirements analysis, security testing and evaluation, independent certification, and other tasks developed and described within the system architecture and configuration(s). The Program's security team participated in creating each of these tasks to ensure compliance with Federal and DOJ security policies. The security team ensures that the Certification & Accreditation (C&A) lifecycle progresses parallel to the UFMS system development lifecycle so that integrity, privacy, and security are analyzed and continuously monitored.

JEDI stores payroll, financial, and procurement data from UFMS/Momentum, JMD's official accounting system. To reduce privacy risks, JEDI-NG follows the same privacy and security administrative, technical, and physical controls as UFMS-AWS. JEDI-NG has no immediate plans to implement artificial intelligence or machine learning.

JEDI stores and transmits PII used for financial and payroll administration and reporting. DOJ's comprehensive security program minimizes privacy risks associated with JEDI by employing management, operational, and technical controls. JEDI maintains privacy and security protections consistent with Department and industry standards.

Finance Staff ensures that DOJ employees are aware of and consent to the use of their information. JEDI displays privacy and security notices before granting system access, consistent with federal laws, executive orders, and DOJ policies. The notification message remains on the screen until the user acknowledges the notice and chooses to either "agree" or "not agree" before proceeding.

JEDI provides administrative, technical, and physical safeguards for the data it processes, as required by the Privacy Act of 1974 (5 U.S.C. § 552a). All data transmitted, received, and stored by JEDI is secured, labeled, and handled in accordance with DOJ regulations and the Privacy Act.