United States Department of Justice
Justice Management Division

Privacy Impact Assessment

for the
EmpowHR System

Issued by:

John E. Thompson
Acting General Counsel

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

Date approved: January 9, 2026

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the 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.)

EmpowHR is a government-to-government software as a service (SaaS) solution provided by the National Finance Center (NFC) to other government agencies. The SaaS solution is built on a technology suite of Oracle/PeopleSoft products and services. EmpowHR serves as a human resources (HR) information system and provides a web-based interface to NFC-hosted data processing and reporting tools. EmpowHR provides for the full processing capabilities for all personnel actions, payroll transactions, and benefits management.

The goal of EmpowHR is to offer a streamlined and integrated set of business processes within the NFC-hosted technology suite. DOJ currently uses a subset of the available products and services in EmpowHR, including HR, Employee Self Service, and Manager Self-Service. DOJ leverages EmpowHR to automate common administrative tasks associated with HR management and to reduce internal operational costs by using the NFC-hosted service that incorporates industry best-practices. The HR functions of the EmpowHR system are used by HR offices from DOJ Headquarters (OIG, EOIR, USMS, USA) and the U.S. Drug Enforcement Administration (DEA). The Manager Self-Service portion of the system is utilized by JMD's Finance Staff (FS).

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, 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.

DOJ HR professionals use EmpowHR for administrative matters to enter all employee personnel actions, performance appraisals, awards, and addresses for accessions and payroll documents such as selected health benefits. For staff managers and supervisors, there is an option to use EmpowHR to initiate personnel actions (i.e., promotions, awards, etc.). EmpowHR offers a workflow system that defines HR request process flows and routes process actions accordingly. HR Requests are initiated by both the employee or by the HR Liaison for a particular office. The HR Liaison would be the individual responsible for initiating personnel actions such as processing of awards, reassignments, promotions, etc., on behalf of the employees of that office. Once approved, HR requests are forwarded to the HR staff that is responsible for that office/component for processing. Last in the approval process is generally the individual in the office with the highest authority or their delegate. This level of access is used by HR liaisons and managers from whom signatures are required for personnel action approvals and is limited in scope to the employee's name; no other PII is accessible. All information for new employees is manually entered into EmpowHR by HR Specialists.

The primary technical, IT security, and administrative responsibilities for the EmpowHR system resides with NFC as they are the service provider with an Authority to Operate (ATO) managed by United States Department of Agriculture (USDA).

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	Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541, et seq. 5 U.S.C. 2951: Reports to the Office of Personnel Management
Executive Order	Executive Orders 9397, as amended by 13478, 9830, and 12107
Federal regulation	28 C. F. R. Part .0 Subpart 0
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	**Names of personnel/family**
Date of birth or age	X	A, B, C & D	**Personnel and relevant employee spouse/partner information may also be included**
Place of birth	X	A, B, C & D	**Personnel and relevant employee spouse/partner information may also be included**
Gender	X	A, B, C & D	**Personnel and relevant employee spouse/partner information may also be included**
Race, ethnicity, or citizenship	X	A, B, C & D	**Personnel and relevant employee spouse/partner information may also be included**
Religion	X	A, B, C & D	**Personnel and relevant employee spouse/partner information may also be included**
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C & D	**SSNs for all personnel; relevant spouse/partner/dependents (full or truncated based on need-to-know)**
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C & D	**Personal - home/residence address(es) for all personnel; relevant spouse/partner/ emergency-contact information**
Personal e-mail address	X	A, B, C & D	**Personal - Email addresses for all personnel; relevant spouse/partner/ emergency-contact information**
Personal phone number	X	A, B, C & D	**Personal - home/cell phone #'s for all personnel; relevant spouse/ partner/emergency-contact information**
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	A	**Financial accounts**
Applicant information			
Education records	X	A	**Personnel and relevant employee spouse/partner information may also be included**

(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
Military status or other information	X	A, B, C & D	**Personnel and relevant employee spouse/partner information may also be included**
Employment status, history, or similar information	X	A	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A	**Personnel performance plans, evaluations, disciplinary actions, and awards for all personnel**
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	A	**Government-issued mobile devices assigned to personnel**
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			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**	X	A	**All personnel**
- **Palm prints**			
- **Iris image**			

(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
- **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:	X	A	
- **User ID**	X	A	**System admins and general users accessing the system**
- **User passwords/codes**	X	A	**System admins and general users accessing the system**
- **IP address**	X	A	**System admins and general users accessing the system**
- **Date/time of access**	X	A	**System admins and general users accessing the system**
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A	Other categories of PII: **Combined Federal Campaign (CFC) contributions for participating personnel**

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	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components		Other federal entities: NFC only	X
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		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	Internal Processing. HR professionals use the system to enter all employee personnel actions, performance appraisals, awards, and addresses for accessions and payroll documents such as selected health benefits. Managers and supervisors also have the option to initiate personnel actions.
DOJ Components				
Federal entities	X			NFC provides demographic data to the Office of Personnel Management (OPM) periodically and on an as needed basis.
State, local, tribal gov't entities				
Public	X			EmpowHR is only used to transmit employee personnel data to NFC's mainframe. Any data pulled would come from NFC's database.

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Only the SF-52 document is shared to authorize a termination action and the end result will appear in NFC's mainframe. NFC's mainframe is considered the Department's personnel system of record. EmpowHR is just the vehicle for populating that database.
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.

The information in EmpowHR is not released to the public for "Open Data" purposes and/or for research or statistical analysis purposes.

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.

Employee information in EmpowHR is not collected directly from the individual. Information is collected during the employee onboarding process on such forms as the SF-0306, which contains a Privacy Act notice provided by OPM. NFC provides user agencies with generalized notice via the applicable public SORN for EmpowHR (identified in Section 7.2). JMD FS is responsible for ensuring EmpowHR users sign a Rules of Behavior acknowledging their responsibility to access, collect, use, maintain, and protect PII. Additionally, NFC utilizes certain banners on the EmpowHR NFC access site, which inform EmpowHR users of their rights to consent to the use of their information.

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.

JMD FS provides EmpowHR users (such as system account managers, HR professionals, and staff managers and supervisors) with the opportunity and/or right to decline to participate in the collection of PII in the system, along with information about the consequences of declining authorization of the collection, use, dissemination, and retention of their PII in EmpowHR. However, failure to provide certain types of PII (i.e. Social Security number) will result in JMD's inability to provide human resources functions such as payroll processing.

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.

Employees do not have access to EmpowHR. Each personnel action processed for an employee generates a SF-50 document. Employees have access to their eOPF which houses the SF-50s that document any actions processed on their behalf. In addition, the employees have access to the NFC Employee Personal Page (EPP), which stores other relevant personnel/payroll data (i.e. tax information, address, allotments, etc.) Employees have the ability to update their information in EPP.

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): August 12, 2025, through August 12, 2028. 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: N/A
	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:

	NFC has determined the EmpowHR security categorization as "Moderate" for each Confidentiality, Integrity and Availability properties per NIST 800-60.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: NFC provides the degree of protection (administrative, technical, and physical safeguards) for the data collected as prescribed by the Privacy Act of 1974, 5 U.S.C. § 552a. NFC ensures all data included in data file transmissions are provided, received, and stored in a secure manner. NFC protects, labels, and handles the data in accordance with the Privacy Act, and applicable agency regulations.
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: NFC regularly audits EmpowHR software, including an annual SOC compliance report that's available to EmpowHR customers. USDA/NFC provides auditing for EmpowHR at the application, database and network/operating system levels, and will notify DOJ of any unusual user activity. Internal JMD auditors audit DOJ's usage of EmpowHR / DOJ's EmpowHR instance. EmpowHR is periodically audited by both OPM and USDA OIG, which are focused on personnel actions being keyed based on signed source documents authorizing such actions, i.e. SF-52, selected health benefits and life insurance forms, etc.
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: Privacy and PII training, including Rules of Behavior, are included in the Cybersecurity Awareness Training (CSAT) that is required for all DOJ federal employees and contractors annually.

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?

EmpowHR is a web-based application and uses 128-bit encryption over hypertext transfer protocol secure (HTTPS) that is accessed by applicants, employees, contractors, managers and HR staff. Additionally, EmpowHR requires file transfer that uses secure file transfer protocol (SFTP) over a secure virtual private network (VPN). EmpowHR uses electronic authentication to protect access to all information. EmpowHR establishes defined roles to allow "Separation of Duties" and employs the principal of "Least Privileges" both designed to reduce the risk of unauthorized access and disclosure of privacy information. Auditing of role-based access is conducted by the Financial Systems Payroll Systems Group (within JMD Finance) in accordance with DOJ Access Management Policies and

Procedures.

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.)

EmpowHR data retention is managed by NFC and governed by National Archives and Records Administration (NARA) General Records Schedules. NFC retains information in EmpowHR in accordance with NFC Record Schedule N1-016-10-7, which provides for a retention period of 56 years (Individual Employee Pay Records (archives.gov)).

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.

Specific employee records are retrieved via a search on the employee's first and/or last name, their SSN, or the EmpowHR generated employee ID.

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:

USDA/OP-1, Personnel and Payroll System for USDA Employees & Customer Agency; renamed Office of the Chief Financial Officer (OCFO), NFC, Systems for Personnel, Payroll, and Time & Attendance (OCFO/NFC-1) (2024-01680.pdf (govinfo.gov)).

JUSTICE/JMD–003, Department of Justice Payroll System. Federal Register /Vol. 82, No. 100 /Thursday, May 25, 2017 /Notices.

JUSTICE/DOJ-006, "Personnel Investigation and Security Clearance Records for the Department of Justice" 67 FR 59864 (9-24-2002), 69 FR 65224 (11-10-2004) 72 FR 3410 (1-25-2007) (rescinded by 82 FR 24147), 82 FR 24147 (5-25-2017)

OPM/GOVT-1, "General Personnel Records" December 11, 2012, 77 FR 79694; modifications published November 30, 2015, 80 FR 74815 and February 2, 2022, 87 FR 5874.

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?

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):*** EmpowHR has data validation routines built into the interface that checks for required fields, data types, and data ranges. Additionally, the business logic layer processes data before it is committed to the database, checking the data against business logic for accuracy and consistency. The retention periods of data contained in the system are covered by NARA General Records Schedules.
- ***Sources of the information:*** EmpowHR stores personnel and payroll data for the purpose of performing HR operations and administration of employee and contractor records. While EmpowHR can store contractor information, DOJ currently does not utilize this feature. The source of the personnel/payroll data stored in EmpowHR are the data documented on the Form SF-52, which authorizes the completion of personnel actions and payroll forms completed by employees.
- ***Specific uses or sharing***: With the exception of NFC providing demographic data to OPM periodically, there is no sharing of the personnel/payroll data housed within EmpowHR. This data is only accessed by HR staff in performance of their duties.
- ***Privacy notices to individuals:*** Information is collected during the employee onboarding process on such forms as the SF-0306, which contains a Privacy Act notice provided by OPM. JMD FS is responsible for making DOJ employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. EmpowHR users must sign a Rules of Behavior prior to system access. Additionally, NFC utilizes banners in which EmpowHR users can either "agree" or "not agree" of their rights to consent to the use of their privacy information.
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information:*** NFC provides the degree of protection (administrative, technical, and physical safeguards) for the data collected as prescribed by the Privacy Act of 1974, 5 U.S.C. § 552a. NFC ensures all data included in data file transmissions are provided, received, and stored in a secure manner. NFC protects, labels, and handles the data in accordance with 5 U.S.C. § 552, Privacy act of 1974, as amended and applicable to agency regulations.