Privacy Impact Assessment

EmpowHR - Human Capital Management System

- Version: 3.0
- Date: March 2019
- USDA, OCFO, National Finance Center

United States Department of Agriculture

Privacy Impact Assessment for the

Human Capital Management System (EmpowHR)

March 2019

Contact Point
Debby Tatum
System Owner/Project Manager
504-426-7664

Reviewing Official
Gail Alonzo-Shorts
Information Systems Security Program Manager
504-228-3867

USDA National Finance Center
United States Department of Agriculture

Abstract

NFC is a Shared Service Center (SSC) under the OPM Human Resources Line of Business (HRLOB). The Human Capital Management System offering, EmpowHR, is a web based human resources information system. EmpowHR allows the USDA and its customers to access employment information from a centralized database maintained by their human resources departments. This Privacy Impact Assessment (PIA) is being conducted to fulfill the requirements of Section 208 of Public Law 107-347 (the E-Government Act of 2002).

Overview

EmpowHR is a commercially provided Oracle/PeopleSoft Human Resources Management System (HRMS) that provides web based management functions to allow USDA and its customers to access Federal employee, applicant, contractor and affiliate information from a centralized database maintained by their human resources and/or contracting departments. System functionality includes recruitment, position classification, HR processing, strategic workforce reporting, training and employee development, employee and labor relations, employee benefits administration, succession planning, employee performance and accountability and organizational management. Employees can view their own personal information, and supervisors can review useful information about their employees.

EmpowHR (formerly known as I*CAMS) has been in operation since 1999 and provides maximum flexibility in meeting new customer requirements, maintaining the core vendor software, and performing system upgrades and enhancements. EmpowHR was successfully upgraded to the PeopleSoft HRMS version release 8.8 SP1 in September 2004 and then to PeopleSoft HRMS version release 9.0 in September 2008.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

EmpowHR collects uses and maintains Federal employee, applicant, contractor and affiliate information that includes personally identifiable information (PII) (social security numbers (SSN), name, address, date of birth, phone number, email address, performance rating, etc.). It offers the option to enter the employee's personal home or personal cell telephone number – this collection is optional and is done as a service to EmpowHR customers. It also includes submitted voluntary self-identification of race and national origin identification data and

disability designation. EmpowHR has the capability to store photographs of employees, but this feature is not currently in use.

1.2 What are the sources of the information in the system?

Applicants, employees, contractors, managers and agency human resources offices provide information for EmpowHR.

1.3 Why is the information being collected, used, disseminated, or maintained?

EmpowHR serves as a repository to store job applications, personnel, and payroll data for the purpose of performing HR operations and administration of employee and contractor records.

1.4 How is the information collected?

Information is collected via a web based application directly from employees, applicants, contractors and affiliates. HR staff may enter information on an individual's behalf through the web based application.

1.5 How will the information be checked for accuracy?

Users are responsible for the accuracy and completeness of any personal data provided. Users will be able to access, review, and update or correct their PII, unless access is prohibited by law or regulation, or the burden or expense of providing access is disproportionate to any data protection risks at stake.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

5 U.S.C. Sec. 552a governs the collection, use and safeguarding of data collected on individuals.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

NFC complies with the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), to ensure that data is protected from unauthorized access, malicious or inadvertent modification, disclosure, and disruption

NFC also works diligently to secure Personally Identifiable Information (PII) by requiring adequate training to employees and contractors that have access to the data.

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. Section 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. Section 552, Privacy act of 1974, as amended and applicable to agency regulations. All employees and contractors adhere to security requirements for handling and storing of Federal data as directed by the Electronic Government Act Title III, also known as the Federal Information security Management Act (FISMA). Only role-based access is granted. Employees have access only to their own records; managers have access only to employees they supervise; and agency human resources staff have access only to their agency employee information (as determined by the agency). PeopleSoft through its PeopleTools manages the end user security. PeopleSoft has strong role-based security controls in place.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Employee information is used to process personnel actions and monitor employees to include: hiring, separating, promoting, training, disciplinary, awards, work status, employee locator, performance evaluation, pay and leave calculation, health benefits, retirement, etc. The information collected is used to assist applicants and potential applicants with the process of seeking employment with the Federal government. Contractor and affiliate information is used to track non-employee personnel within an organization.

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

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.

Customer agencies may run pre-prepared and custom reports against the database and have the ability to access all data elements depending on access privileges requested by authorized agency personnel.

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

EmpowHR does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

EmpowHR uses role-based access and UserID/password to protect access to all information. Employees only have access to their own records; managers have access only to employees they supervise; and agency human resources staff have access only to their agency employee information (as determined by the agency). Access to information is provided on a need-to-know basis and follows our "least privilege" policy. PeopleSoft through its PeopleTools is used to manage the end user security. PeopleSoft has strong role-based security controls in place.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The retention periods of data contained in this system are covered by NARA General Records Schedules. Civilian Personnel Records have various retention periods for specific types of data. These retention periods are adhered to per customer agency requirements and memorandum of understanding. NFC retains information in EmpowHR in accordance with NFC Record Schedule N1-106-10-7, which states a retention period of 56 years.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. NFC Record Schedule N1-106-10-7 has been approved.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The purpose of retaining the information is to provide customers the capability to serve the human resources needs of their OCHCOs. The data will be used to respond to any human resources issues including but not limited to time attendance, recruitment, payroll, Equal Employment Opportunity (EEO) issues or law suits, and disciplinary actions. To mitigate risks associated with unauthorized release of EmpowHR data, NFC removes data from online systems when appropriate, and stores it offline at a federal records center or other authorized location, for the minimum amount of time required. NFC destroys data on paper and microfiche following the guidance and timelines in accordance with the NFC Record Schedule N1-106-10-7.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

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

Information collected by the EmpowHR system is owned by each customer agency. The customer agency determines the use and sharing of the information. NFC maintains and secures the information on behalf of our customers. The system/agency security officers handle all requests for any information pertaining to user accounts/access based on supervisory requests. Access is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties/access their data. Access is requested/determined by personnel/payroll offices who submit the data. NFC grants authority to use/access EmpowHR to individual users at the request of the agencies approved by the user's ASO.

NFC provides agencies their own HR data from EmpowHR to (at their request), or to a service provider on their behalf. The agencies use the information as they deem necessary. NFC sends the requested data to the NFC SFTP File Server, and from there it is transmitted to the agencies or their designated service providers via SFTP. The agencies are responsible for protecting and securing the data once it reaches its destination. Currently, data is being transmitted to these USDA agencies:

- USDA Forest Service
- USDA National Resources Conservation Service
- USDA Office of the Chief Information Officer

NFC shares our customers' EmpowHR data with other NFC MAs (Major Applications), as described below.

- PPS: EmpowHR provides HR data to the NFC Payroll Personnel System (PPS) MA, for those agencies that use EmpowHR, via internal FTP/SFTP.

- Insight: EmpowHR provides HR data to the NFC Insight MA, which is hosted at USDA NITC. Source information within flat files is transmitted via SFTP over a secure VPN, and loaded into the Insight database, and is made available to Insight users with appropriate access.

- Reporting Center: EmpowHR provides HR data to the NFC Reporting Center application (a subcomponent of the NFC WebApps MA) via internal FTP/SFTP. EmpowHR creates files on the EmpowHR application servers which are then sent via FTP to the Mainframe component of the NFC EIP. Reporting Center pulls the files

from the Mainframe and generates reports that are available to Reporting Center users with appropriate access.

- USDA/OCIO eAuthentication (eAuth) system: EmpowHR data is made available to USDA OCIO for use in the eAuthentication Application, Enterprise Entitlements Management Service (EEMS) for EmpowHR users who use eAuth for identification and authentication to EmpowHR.

- USDA Data Lake system: Information may be shared with senior leadership across USDA through a series of Tableau dashboards and reports for the purpose of promoting data-driven decisions. The information shared will span data from different various administrative domains including IT, Finance, HR, Property, Operations, Homeland Security, and Property & Fleet.

4.2 How is the information transmitted or disclosed?

The NFC EmpowHR MA is a Web-based application and uses 128-bit encryption HTTPS that is accessed by applicants, employees, contractors, managers and HR staff. The NFC EmpowHR MA requires file transfer that use secure file transfer protocol (SFTP) over a VPN or other secure transmission methods, as listed in 4.1 above. To obtain EmpowHR data for eAuthentication EEMS, OCIO users login using DBConnect over IPsec.

The information will be transmitted to the USDA Data Lake via secure file transfer methods such as SFTP, API, and Web Service. Once in the USDA Data Lake, data will be shared via a series of Tableau dashboards.

Information is shared with other USDA systems as described in 4.1 above.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The system security officer handles all requests for and information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is requested/determined by personnel/payroll offices who submit the data. NFC will grant authority to use/access EmpowHR to individual users at the request of OPM and the requesting user's agency security officer. Data transmission risks are mitigated by the required use of secure file transmission methods for all information that is exchanged between EmpowHR and another system, agency, or organization.

Risk when sharing within USDA is considered low-moderate. Should data sharing include sources of the network, encryption protocols ensure PII is not inadvertently shared in an

unencrypted format. Data is encrypted in motion and at rest. In addition, access to data is limited to only those persons with need-to-know through the use of internal, granular governance process. Dissemination of information is governed by internal policy. Access to information is monitored, tracked, logged and audited using tools such as Cloudera Navigator and Cloudera Manager.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

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

Information collected by the EmpowHR system is owned by each customer agency. The customer agency determines the use and sharing of the information. At their request, NFC provides some internal organizations (customer agencies) or their designated service providers with their data, as listed below, via secure transmission methods. The agencies use the information as they deem necessary, and they are responsible for protecting and securing the data once it reaches its destination.

- EmpowHR data owned by Forest Service is provided to them, at their request, for use in their Human Resource Management/Customer Relationship Management (HRM/CRM) system (hosted by DOC) and for Time and Attendance processing (hosted by GDCII). Files are transmitted via XML Messaging over VPN.

- NFC provides Forest Service' (FS) HR data from EmpowHR to the GDCI Integration, Inc. (GDCII) data center in St. Louis MO, at FS' request, for use in FS' Time and Attendance processing system (Paycheck8) which is hosted by GDCII. NFC saves the requested FS data to the NFC SFTP File Server, and from there it is transmitted to GDCII via SFTP.

- NFC provides USDA's HR data from EmpowHR to the GDCI Integration, Inc. (GDCII) data center in St. Louis MO, at USDA's request, for use by the ConnectHR application that GDCII hosts for USDA. NFC saves the requested USDA data to the NFC SFTP File Server, and from there it is transmitted to GDCII via SFTP.

- NFC provides USDA HR data, at their request, to eRecruit and Onboarding (third party applications) provided to USDA as SaaS (Software as a Service). These applications are hosted at the Department of Commerce (DOC data center located in Alexandria, VA; and managed by the National Technical Information Service (NTIS). Data transmission from NFC to eRecruit and Onboarding is via SOAP/XML based Web Service messaging over HTTPS, using Oracle Integration Broker Server.

- NFC provides DOJ HR data to USA Staffing (third party application) at their request. This application is hosted at the Office of Personnel Management (OPM). Data transmission from NFC to USA Staffing is via SOAP/XML based Web Service messaging over HTTPS, using Oracle Integration Broker Server.

- NFC provides HR data to Monster Government Services (MGS), a third party application. This application is hosted at the Equinix Data Center in Ashburn, VA. Data transmission from NFC to MGS is via SOAP/XML based Web Service messaging over HTTPS, using Oracle Integration Broker Server.

- NFC provides agencies their own HR data from EmpowHR to (at their request), or to a service provider on their behalf. The agencies use the information as they deem necessary. NFC sends the requested data to the NFC SFTP File Server, and from there it is transmitted to the agencies or their designated service providers via SFTP. Currently, data is being provided to the Library of Congress (LOC), DHS Federal Emergency Management Agency (FEMA), and Natural Resources Conservation Service (NRCS).

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

Yes, the sharing of PII outside the Department is compatible with the original collection, and covered by a SORN. See USDA/OP-1, Personnel and Payroll System for USDA Employees Customer agency SORN as reference.

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

Information is accessed by customer agencies via a Web-based application and uses 128-bit encryption HTTPS. Disclosure of information is restricted through the use of passwords and sign-on protocols. Data is restricted through a profiled access approach. Only individuals with an established "need-to-know" may access their specific profiled data.

Any information transmitted from EmpowHR to an external agency (or their designated provider) must be transmitted via secure transmission, such as SFTP, over a Virtual Private Network (VPN) or other secure transmission protocols, as described in 5.1 above

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Only authorized individuals can access information under the "need-to-know" authorities. The proper controls are in place to protect the data and prevent unauthorized access. Data transmission risks are mitigated by the required use of secure file transmission methods for all information that is transmitted from EmpowHR to another agency or organization. Data transmission methods currently used by EmpowHR are described in 5.1 above.

Section 6.0 Notice

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

6.1 Was notice provided to the individual prior to collection of information?

The agencies that employ individuals are responsible for obtaining authorization to collect use, maintain and share PII. NFC provides the agencies with the System of Record Notice (SORN) that is associated with EmpowHR. The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The individual employees must coordinate directly with their employing agency regarding these rights.

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

The agencies that employ individuals are responsible for providing individuals with the opportunity and/or right to decline to provide information, and also the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII. NFC provides the agencies with the SORN that is associated with EmpowHR. The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The individual employees must coordinate directly with their employing agency regarding these rights.

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

NFC provides the agencies with the SORN that is associated with EmpowHR. The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The agencies are responsible for informing their employees of their rights to consent to particular uses of their information,

as described in the SORN. The individual employees must coordinate directly with their employing agency regarding these rights.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

NFC coordinates and communicates with the agencies that employ individuals, not directly with the employees. NFC provides the agencies with the SORN that is associated with EmpowHR. The agencies that use EmpowHR are responsible for making their employees aware of, and consent to, uses of their information for legitimate uses described in the SORN. The agencies are responsible for informing their employees of their rights to consent to particular uses of their information, as described in the SORN. The individual employees must coordinate directly with their employing agency regarding these rights.

From a regulatory and management controls perspective, a copy of the redacted PIA is available on USDA's Office of the Chief Information Officer web site.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

At the customer agency's discretion and according to the agency's security policies, individuals may be assigned a unique user id and password that allows them access to their own data in the system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals with the proper assigned user role would be able to correct specific information themselves. However, most information in the system must be corrected by authorized users from the agency's human resources department at the request of the individual or at agency direction.

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

Each agency using the system would provide this information to employees.

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

Each agency using the system would provide this information to employees.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

It is the responsibility of each individual agency to ensure that personnel with access to correct data on employees have the proper clearances, position sensitivity designations, and appropriate system access to the data. NFC access control procedures, role-based security of the application, and agency reporting of employee access and utilization aid agency officials to mitigate the risks of agency individuals with improper access to employee data.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

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

Only role-based access is granted. PeopleSoft through its PeopleTools manages the end user security, which is determined by the agencies. PeopleSoft has strong role-based security controls in place. NFC follows Title VII, Chapter 11 Directive 58, Information Systems Security Program, and Directive 2, Access Management.

8.2 Will Department contractors have access to the system?

Yes if authorized a valid role.

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

Privacy and PII training is included in the Security Awareness and Rules of Behavior training that is required for all federal employees and contractors annually. An exam is provided following the training and the user must receive 70% or better to maintain or receive access to the information system. Some NFC staff members receive additional privacy training according to their role within NFC. Contractors must complete annual security training and be properly trained on the system.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes

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

EmpowHR provides auditing at the application, database and network/operating system levels.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

A Risk Assessment was performed on EmpowHR and security controls have been documented in the System Security Plan. These controls are tested annually under the continuous monitoring, SSAE 18, and A-123 programs.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

EmpowHR uses a Commercial off-the-shelf (COTS) application.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

There are no privacy concerns with the technology employed. EmpowHR is hosted at the NFC data center. EmpowHR has undergone a detailed security vulnerability assessment and has been certified and authorized.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

N/A

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

EmpowHR receives PII data from eRecruit, Onboarding, USA Staffing, and Monster that includes social security number (SSN), name, address, date of birth, phone number, email address, performance rating, etc., of employees, as well as voluntary self identification of race and national origin identification data and disability designation.

EmpowHR sends USDA PII data to GDCII to use in ConnectHR that includes that includes social security number (SSN), name, address, date of birth, phone number, and email address.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

NFC uses the PII data from eRecruit, Onboarding, USA Staffing, and Monster to populate EmpowHR with payroll and personnel data about the person who has been selected for a position, for the purpose of performing HR operations and administration of employee and contractor records.

The information collected from eRecruit, Onboarding, USA Staffing, and Monster is used in EmpowHR to assist applicants and potential applicants with the process of seeking employment with the Federal government. Employee information is used to process personnel actions and monitor employees to include; hiring, separating, promoting, training, disciplinary, awards, work status, employee locator, performance evaluation, pay and leave calculation, health benefits, retirement, etc. Contractor and affiliate information is used to track non-employee personnel within an organization.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database, and is maintained and secured as part of EmpowHR. EmpowHR uses role-based access to all information. Employees only have access to their own records. PeopleSoft through its PeopleTools manages the end user security. PeopleSoft has strong role-based security controls in place.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database, and is maintained and secured as part of EmpowHR. The retention periods of data contained in this system are covered by NFC Record Schedule N1-106-10-7. Civilian Personnel Records have various retention periods for specific types of data. These retention periods are adhered to per customer agency requirements and memorandum of understanding.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database, and is maintained and secured as part of EmpowHR. EmpowHR uses role-based access to all information. Employees only have access to their own records. PeopleSoft through its PeopleTools manages the end user security. PeopleSoft has strong role-based security controls in place.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Data received from eRecruit, Onboarding,USA Staffing, and Monster is stored within the EmpowHR application and database, and is maintained and secured as part of EmpowHR. HR data stored in EmpowHR is owned by each customer agency. The customer agency determines the use and sharing of the information. At their request, NFC provides some internal/external organizations (customer agencies) or their external designated service providers with their data, as listed above in 4.1 and 5.1, via secure transmission methods.

The agencies use the information as they deem necessary, and they are responsible for protecting and securing the data once it reaches its destination.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

No; the data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database, and is maintained and secured as part of EmpowHR. See USDA/OP-1, Personnel and Payroll System for USDA Employees Customer agency SORN as reference.

10.10 Does the system use web measurement and customization technology?

No, it does not.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Data received from eRecruit, Onboarding, USA Staffing, and Monster is stored within the EmpowHR application and database, and is maintained and secured as part of EmpowHR.

The system security officer handles all requests for and information pertaining to user accounts. Access control is based on the principle of least privilege, which refers to granting the minimum required system resources to a user that enables them to perform their duties. Access is requested/determined by personnel/payroll offices who submit the data. NFC will grant authority to use/access EmpowHR to individual users at the request of OPM and the requesting user's agency security officer.

Agency Responsible Officials

DEBORAH TATUM

Digitally signed by DEBORAH TATUM
Date: 2019.05.01 10:54:49 -05'00'

System Manager/Owner
Debby Tatum, Associate Director
Web Applications Directorate
Government Employees Services Division
USDA National Finance Center

GAIL ALONZO SHORTS

Digitally signed by GAIL ALONZO SHORTS
Date: 2019.08.21 17:54:41 -05'00'

NFC Privacy Officer/ISSPM/CISO
Gail Alonzo-Shorts
Access Management Branch
Information Technology Services Division
USDA National Finance Center

Agency Approval Signature

ANITA ADKINS

Digitally signed by ANITA ADKINS
Date: 2019.09.23 16:23:47 -05'00'

Authorizing Official Designated Representative
Anita Adkins, Acting Director
Government Employees Services Division
USDA National Finance Center