Privacy Impact Assessment

Insight

- Version: 3.1
- Date: November 2018
- Prepared for: USDA OCFO, National Finance Center

United States Department of Agriculture

Privacy Impact Assessment for

Insight

November 7, 2018

Contact Point
Debby Tatum, Associate Director
Web Applications Directorate
504-426-1102

Reviewing Official
Ivan Jackson, Associate Director
Information Technology Security Directorate
(504) 426-7551

USDA National Finance Center
United States Department of Agriculture

Abstract Note:

The information system is the National Finance Center (NFC) Insight, providing human resource reports. Insight contains Human Resource (HR) Privacy Identification Information (PII).

Overview

Insight provides workforce information with metrics and attributes to allow HR to analyze workforce staffing and productivity. The responsible organization is the National Finance Center, 13800 Old Gentilly Road, New Orleans, Louisiana. The System Owner is Debby Tatum. Insight contains Human Resource (HR) sensitive data that includes salary, health benefit deduction, health benefits, social security number and bank account information. A typical query would be a client requiring a report on how many employees are in a specific location. The client would log into *Insight* seeing only information he has been authorized to see. The report would show the number of employees within the specified location. The Source information originally comes from the Payroll/Personnel System (PPS), EmpowHR, and Administrative Billings and Collections System (ABCO). These internal systems have the same Authorizing Official (AO) as Insight. Insight does not permit users to input data or change data.

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?

Insight contains Human Resource (HR) sensitive data that includes name, social security number, DOB/POB, address, employment history, salary, health benefit deduction, health benefits, miscellaneous identification numbers, financial data, and bank account information.

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

Source data comes from flat files from the Payroll/Personnel System, the EmpowHR system, and ABCO. These systems contain data for USDA employees and non-USDA federal employees for whom NFC provides Payroll and Personnel services.

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

The system provides workforce information with metrics and attributes to allow HR to analyze workforce staffing and productivity.

1.4 How is the information collected?

Source data comes into the Insight Database via standard FTP (file transfer protocol) over USDA encrypted Virtual Private Network (VPN) tunnel between NFC and NITC data centers, from Payroll/Personnel System, EmpowHR flat files, and ABCO system.

1.5 How will the information be checked for accuracy?

Insight data reflects what is in the source system and will not be changed.

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. "

The SORN is USDA/OP-1

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

Unauthorized disclosure of salary, health benefit deduction, health benefits, social security number or bank account could adversely affect employees of USDA. Insight is an internal USDA web application protected through border protections in place at the National Information Technology Center (NITC), where Insight is hosted.

The NITC controls all physical access points (including designated entry/exit points) to the facility where the information system resides through the use of armed security officers and the Facility Security System. The Facility Security System requires that an individual be in possession of their assigned badge containing the appropriate access levels. The NITC verifies individual access authorizations before granting access to the facility by performing a security background clearance check prior to granting access. The NITC also controls access to areas officially designated as publicly accessible by requiring all visitors to enter through a single entry point. Once access to the facility is granted, the visitor must be escorted at all times.

The NITC controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides. Visitors

must present proper ID, sign a log, and wear a visitor's badge. The visitor must sign for the visitor's badge on the appropriate sign in/out sheet, located in the east lobby. The NITC may issue "Limited Access" visitor's badges for authorized visitors needing access to NITC internal doors, excluding the operations area. However, visitors must remain with their escort throughout their visit. Persons found in the building without an employee or visitor badge will be immediately escorted to the building guard. All visitors to the facility must pass through the magnetometer at the east lobby. All visitor parcels, briefcases, purses, and similar materials are x-rayed at the east lobby. Visitor badges do not provide access through the parking lot entry gates.

Each network zone is protected by a controlled number of interfaces to firewall pairs that concentrate external traffic into a manageable number of interfaces. Ingress is controlled and monitored through firewall and IDS system that are configured, provisioned, and managed to provide effective protection of the confidentiality and integrity of ingress data to each network stack or zone.

Access by web interface requires a valid user identification and password. Once authenticated, the user receives only access to information for which the user account has permission. Accounts are created with least privilege determined by job responsibilities. Account access is restricted to system administrators with privileged accounts.

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.

Reporting information allows HR to analyze workforce staffing and productivity.

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

Business Intelligence by Oracle. The product provides workforce information with metrics and attributes to allow HR to analyze workforce staffing and productivity. A typical report would provide the number of employees in a specific location.

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

Commercial or publicly available data is not used.

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.

Accounts are created with least privilege determined by job responsibilities. Account access is restricted to system administrators with privileged accounts. USDA personnel and contractors go through NACI background checks. Web interface users do not have permissions to access the database. Physical access to the database is restricted through automated mechanisms to recognize potential intrusions, which includes video monitoring and recording, badge readers, biometric scanners and audible alarms.

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 Operational Data Store (ODS) and the Dimensional Data Marts (DM) store current as well as prior information for the life cycle of the employee.

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

National Archives and Records Administration (NARA) General Records Schedules (GRS) provide mandatory disposal authorization for temporary administrative records common to several or all agencies of the Federal Government. They are issued by the Archivist of the United States under the authority of 44 U.S.C. 3303a (d).

General Records Schedule 2, Payrolling and Pay Administration Records N1-GRS-92-4 item 22b for reports and data used for agency workload and/or personnel management purposes states to destroy when two years old. For reports providing fiscal information on agency payroll, N1-GRS-92-4 item 22c states to destroy after GAO audit or when three years old, whichever is sooner.

Insight retention plans are within the guidelines.

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

A long retention of data increases the risk that the information will go out of date and use of outdated information will cause errors. The sources used to populate the Insight database repository are for reporting purposes only and will not be updated, changed or

information returned to the source. Use of the data will not cause errors in the source. The retention dates planned for Insight are within acceptable best practices. Risk of out of date data is negligible.

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?

The source data is loaded into the Insight database and not subsequently shared, transmitted, or exported to any other internal applications or internal organizations; except to be viewed by the federal agency which owns and originally provided the data. Insight provides reporting information to allow HR to analyze workforce staffing and productivity.

4.2 How is the information transmitted or disclosed?

Source information within flat files is transmitted using standard FTP over USDA encrypted Virtual Private Network (VPN) tunnel between NFC and NITC data centers and loaded into the database. Reporting information is disclosed via secure Oracle HTTPS Server (OHS) based web access to authorized users requiring a valid user identification and password to access Insight.

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.

Unauthorized disclosure of salary, health benefit deduction, health benefits, social security number or bank account could adversely affect employees of USDA. Source data comes into Insight from three internal NFC applications under the same Authorizing Official (AO). The internal systems have been authorized to operate and follow USDA Risk Management Framework guidelines, processes and procedures which are compliant to OMB directives, FISMA and NIST requirements. NFC personnel go through NACI background checks and receive annual security awareness training with Rules of Behavior required acknowledgement. Source information within flat files is transmitted via standard file transfer protocol (FTP) over USDA encrypted Virtual Private Network (PVN) tunnel between NFC and NITC data centers, and loaded into the database. Reporting information is disclosed via secure Oracle HTTPS Server (OHS) based web access to authorized users requiring a valid user identification and password to access Insight. The database is not accessible by the web interface user. Physical access to the database is restricted through automated mechanisms to recognize

potential intrusions, which includes video monitoring and recording, badge readers, biometric scanners and audible alarms.

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?

Insight does not export or transmit data to any external organizations or other applications. The source data is loaded into the Insight database and not subsequently shared with any other external applications or external organizations; except to be viewed by the federal agency which owns and originally provided the data. Insight stores federal agencies' workforce information, and provides reporting capabilities that allows federal agencies' HR staff to analyze their agency's workforce staffing and productivity data. Organizations are only allowed to view their own agency's information, at the level of their account, approved by their agency, based on least privilege.

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.

Display and viewing of the information contained in Insight is compatible with the original collection of the information in the NFC applications from which the data is obtained. NFC follows the 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 in Insight is accessed by the agencies via a web-based application that uses 128-bit encryption HTTPS. Access to Insight is through a web interface requiring a valid user identification and password. User accounts are created using the least privilege

with access permissions determined by job responsibilities. There is no logical access to the database for users outside the Department. Physical access to the database is restricted through automated mechanisms to recognize potential intrusions, which includes video monitoring and recording, badge readers, biometric scanners and audible alarms.

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

Unauthorized disclosure of salary, health benefit deduction, health benefits, social security number or bank account could adversely affect employees of USDA. There is no access to the physical database, which is hosted by NITC. Physical access to the database is restricted through automated mechanisms to recognize potential intrusions, which includes video monitoring and recording, badge readers, biometric scanners and audible alarms. Logical access is through a web interface to the reporting module is controlled by least privilege determined by job responsibilities of the user. The web interface does not allow the user to directly access the database.

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?

Notice is provided during normal HR new hire processes for all federal employees.

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

Information is gathered as part of the normal hiring activity for all federal employees, and required to provide compensation and benefits to the employee.

Individuals have the opportunity to decline to provide the information and are informed that the data is required to complete routine business functions.

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

No. This information is required to provide compensation and benefits to the employee, and collected as part of the NFC legal authority. This applies to all federal employees.

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.

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. Individuals are notified several ways such as; by their agency, during online registration, during application use, etc. From the standpoint of an individual using the application, they are made aware of the collection of data and potential uses and must consent to both prior to accessing the system.

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?

Individuals do not have access to the information within Insight.

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

Individuals would contact their HR representative and the corrections would be made within the source Payroll/Personnel System. Corrections would not be made directly within Insight. Updates to the source systems will be loaded into Insight as they occur.

The procedures to correct information in the source system as stated in the SORN USDA/OP-1 for Payroll/Personnel System are:

Notification procedure: Employees may request information from this system from the appropriate personnel office having custody of his/her records. A request for information should be addressed to the Director, Personnel Division (name of appropriate Agency), USDA, at the address shown under Location and should contain the name of requestor, employing agency in USDA or agency to which information was furnished, address of agency and particular information requested.

Record access procedures: Any individual may obtain information as to the procedures for gaining access to and contesting a record in the system which pertains to him/her by submitting a written request to the appropriate office referred to in the preceding paragraph.

Contesting record procedures: Same as Record access procedures.

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

As stated in the SORN USDA/OP-1 for Payroll/Personnel System:

Notification procedure: Employees may request information from this system from the appropriate personnel office having custody of his/her records. A request for information should be addressed to the Director, Personnel Division (name of appropriate Agency), USDA, at the address shown under Location and should contain the name of requestor, employing agency in USDA or agency to which information was furnished, address of agency and particular information requested.

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

There are no alternatives available through Insight. The redress would be through the source systems.

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

Source data is provided from the NFC Payroll/Personnel System, EmpowHR, and ABCO; Insight does not return data to the source systems. There is no privacy risk associated with redress to Insight.

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?

The agencies determine user access. NFC follows Title VII, Chapter 11, Directive 2, Access Management, and Directive 58, Information Systems Security Program. User account creation goes through a defined process for any access to any of systems

within NFC. The end users' agency security officers (ASOs) submit request to the NFC Access Management Branch to add users in a defined role. Procedures are documented within NFC. The ASOs are the point of contact between the system users and NFC Access Management Branch. The ASOs are responsible for ensuring that Insight users have completed the required training (e.g., PII, SAT, ROB) and clearance process prior to requesting access for these users. This applies to all federal employees.

8.2 Will Department contractors have access to the system?

USDA NFC contractors will have access to the system, if properly authorized a valid role. They are subject to the same privacy training and security clearance requirements as the federal employees.

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.

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?

NITC hosts Insight. The operating system tracks system specific information, such as database, antivirus, and application-level events as determined by the COTS software. Oracle tracks SYS account login activity. Access to the database is only by system administrators with privileged accounts. Users do not have access to the database. Physical access to the database is restricted through automated mechanisms to recognize potential intrusions, which includes video monitoring and recording, badge readers, biometric scanners and audible alarms.

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 Insight and security controls have been documented in the System Security Plan. These security controls are tested annually under the continuous monitoring, SSAE 16, 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?

Insight is a reporting tool that 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. Insight is hosted in an internal USDA data center (NITC). A Service Level Agreement is in place for NITC's Infrastructure as a Service (IaaS). NITC hosts Insight and follows USDA's RMF processes and procedures. NITC has a current Authority To Operate (ATO).

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?

Insight does not use 3rd party websites/applications.

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

No Insight PII will be available through use of 3rd party websites/applications.

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

No Insight PII will be available through use of 3rd party websites/applications.

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?

No Insight PII will be available through use of 3rd party websites/applications.

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

No Insight PII will be available through use of 3rd party websites/applications.

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

No Insight PII will be available through use of 3rd party websites/applications.

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?

No Insight PII will be available through use of 3rd party websites/applications.

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 Insight PII will be available through use of 3rd party websites/applications.

10.10 Does the system use web measurement and customization technology?

No Insight PII will be available through use of 3rd party websites/applications. No web measurement and customization technology is used.

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?

No web measurement and customization technology is used.

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.

No Insight PII will be available through use of 3rd party websites/applications. There is no risk from 3rd party websites.

Agency Responsible Officials

DEBORAH TATUM

Digitally signed by DEBORAH TATUM
Date: 2018.11.28 06:55:32 -06'00'

System Manager/Owner
Debby Tatum, Associate Director
Applications Development
Government Employees Services Division (GESD)
USDA National Finance Center

IVAN JACKSON

Digitally signed by IVAN JACKSON
Date: 2018.12.10 13:12:56 -06'00'

NFC Privacy Officer/ISSPM/CISO
Ivan R. Jackson, Associate Director
Information Technology Security
Information Technology Services Division (ITSD)
USDA National Finance Center

Agency Approval Signature

Adrianne F. Riviere, acting for Cristina Chiappe

Digitally signed by Adrianne F. Riviere, acting for Cristina Chiappe
Date: 2018.12.12 11:57:10 -06'00'

Authorizing Official Designated Representative
Cristina Chiappe, Director
Government Employees Services Division (GESD)
USDA National Finance Center