Privacy Impact Assessment

Human Resource-GSS (formerly HRC-GSS)

- Version: 8.1
- Date: September 9, 2020
- Prepared for: USDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Human Resource General Support System (HR-GSS)

September 9, 2020

Contact Point

Joseph T. Abbott – System Owner

Human Resource Office (HRO)

(202) 690-0279

Reviewing Official

Emmanuel Olufotebi

FSIS Privacy Office

(202) 205-0144

United States Department of Agriculture

Revision History

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.1	03/26/2014	Kathryn Stuart	Updated to new template and prepared for Annual Review by SO.
2.0	04/14/2014	Kathryn Stuart	Finalized changes for signature.
3.1	11/17/2014	Kathryn Stuart	Updated to latest template and prepared for Annual Review by SO.
4.0	12/1/2014	Kathryn Stuart	Finalized changes and obtained Annual Review Memo signature from SO.
4.1	01/12/2016	Uche Okeoma	Updated for ATO
5.0	06/03/2016	Uche Okeoma	Finalized changes and to obtain Annual Review signatures.
5.1	01/17/2017	Uche Okeoma	Update for FY 17
6.0	03/30/2017	Uche Okeoma	Finalized for FY 17
6.1	03/15/2018	Yvette Petrescu	Updated to latest template and prepared for Annual Review by SO.
7.0	09/18/2018	Yvette Petrescu	Finalized document and obtained Annual Review Memo Signature from SO.
7.1	11/19/2018	Olugbenga Sogbetun	Updated document to satisfy POAM ID 27972 and 28079

7.2	03/27/2019	Olugbenga Sogbetun	Updated information in preparation for ATO
8.0	07/23/2019	Olugbenga Sogbetun	Document Finalized for ATO.
8.1	09/9/2020	Safae Alaoui	Updated for FY20

Abstract

This Privacy Impact Assessment is being conducted since HR-GSS was identified during the Privacy Threshold Assessment as using Personally Identifiable Information (PII).

The Food Safety and Inspection Service (FSIS) historically utilized a set of "Mini-Applications" to manage various HR functions. Development of these applications occurred independently without an overarching enterprise architecture or product vision in place. This created an environment over time where mission-critical tools were disparate, unsecure, lacking key functionality and outdated. This set of tools required significant cost to both time and resources to support and maintain.

The HR-GSS platform replaces the previous systems with a single, modern, centralized web application using the Python/Django framework improving intra-application and external system communication and data integrity.

HR-GSS is a web-based system that allows program managers and users to rapidly identify, respond to, and track the Agency's response to significant incidents. These include suspected tampering of products, threats to facilities, natural disasters, and Class 1 recalls that involve illness

Overview

- HR-GSS is managed by FSIS. The system is housed at the FSIS Enterprise Data Center (EDC) located in Kansas City, MO.
- HR-GSS is integrated into the FSIS Enterprise Network and is not available to the general public; it is only available to those with access to the FSIS intranet and with an e-Authentication (e-Auth) username and password.
- HR-GSS is not located in a harsh environment that would be detrimental to the hardware or to the system's performance and availability.
- There are numerous roles in HR-GSS. The key role is the HR-GSS Application Administrator. The functionality he is responsible for include: managing users within the system, and creating/updating the information related to Incident Reports (IRs).
- The legal authority to operate the program or system is provided by the signed ATO letter dated 08/13/2019.

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?

The types of information stored within HR-GSS include:

- Employee Information
- Position Information
- Personnel Action History

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

NFC and user input are the sources of the information.

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

HR-GSS is a Human Resource system and requires HR information in order to function. Anything created in HR-GSS references a specific employee along with their current or historical employment information.

1.4 How is the information collected?

On a nightly basis, an automated job is run that connect to NFC's reporting tool, Insight. This job authenticates with an account created specifically for this purpose and retrieves all the data configured for use by HR-GSS and inserts or updates it in the application's database.

1.5 How will the information be checked for accuracy?

NFC data is considered authoritative. When errors are found, employees can request corrections by contacting HROD.

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

The authorities for USDA to collect, maintain, use and disseminate information through this system are: 5 U.S.C.301 (government organization and employees); Title 5 USC 552a (Records Maintained on Individuals (Privacy Act)); Title 41 CFR 201-6.1 (Federal Information Resources Management Regulation); 44 U.S.C.3101 (Records Management); OMB Circular No. A-108 (Responsibilities for the Maintenance of Records About Individuals by Federal Agencies); OMB Circular No. A-130 (Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals); and Authorization to Operate (ATO), dated 22-07-14,

In addition, USDA is generally authorized to collect information to support its mission under: Title 7, Chapter 55-2205 (7 U.S.C 2204) (which authorizes the Secretary of Agriculture to collect information and employ any sampling or other statistical method deemed appropriate); 21 U.S.C. 679c(a)(1)-(3) (which expressly authorizes the Secretary to give high priority to enhancing the ability of FSIS to conduct its mission); the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, et seq.), the Poultry Product Inspection Act (PPIA) (21 U.S.C., et seq.), the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, et seq.), and the Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901-1906).

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

Access to data is strictly controlled.

HR-GSS System Administrators and general users access the system using unique, authorized accounts. HR-GSS cannot be accessed without an authorized account and it cannot be accessed by external users. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions at the application level. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

There are firewalls and other security precautions in place. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of Behavior (ROB) and consequences, and system use notifications are in accordance with the Privacy Act (5 U.S.C. § 552, subsection [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every 3 years.

When anyone is granted access to the FSIS environment, they are issued a USDA email account and an FSIS user account (managed in Active Directory). To access HR-GSS, the user must first login to the FSIS network environment by using their Active Directory account to login.

Additionally FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to having system access. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer (OCIO).

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Any contractors who may be authorized to access the system (e.g., software developers) are governed by contracts identifying ROBs for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel who are expert in such matters.

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.

- Tracking the lifecycle of SF-52 (Personnel Action) Forms.
- Tracking and reporting on the annual bargaining unit performance awards.
- Tracking the lifecycle of worker compensation claims

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

Data is accessed via web interface and can display in web pages or export to reports in CSV or PDF format.

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

The system does not use any 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.

HR-GSS System Administrators and general users access the system using unique, authorized accounts. HR-GSS cannot be accessed without an authorized account and it cannot be accessed by external users. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions at the application level. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

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?

Maximum of 5 Years based on the type of information.

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

Yes.

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

Possible risks associated with the system data include exposure of personal data due to unauthorized access to the users' profile, unauthorized users modifying a valid user's profile, and non-privileged users gaining access to database management functions.

Controls exist to manage and mitigate all these risks. Extended retention periods increase the probability of a control failure and the volume of data that might be exposed. FSIS, EDC, and HRO continuously monitor the security controls for the HR-GSS applications to respond to changing security threat conditions and actual/potential security relevant events.

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?

All internal organizations have access to the information is some capacity.

Any information shared is deemed necessary for managing their own employee populations.

4.2 How is the information transmitted or disclosed?

Data is accessed via web interface and can display in web pages or export to reports in CSV or PDF format.

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 OHR takes privacy very seriously. HR provides routine privacy reminders to their users and ensures their users take part in the FSIS annual security awareness training.

In addition, they are trained to handle sensitive and confidential information. All user data is accessible and used only by FSIS personnel who are authorized by their local security officer, and then by the HR-GSS administrator.

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?

No Information containing PII is shared with organizations external to the USDA.

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.

HR-GSS does not share PII outside of the Department.

HR-GSS has a SORN with ID OPM/GOVT-1 published on 12/11/2012 titled -General Personnel Records, System of Records.

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

Should HR-GSS information need to be shared externally, departmental guidelines for providing information to such organizations will be followed. This includes the redacting of PII, unless the information is required under law.

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

As long as employee PII data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee PII is not shared externally. Such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed.

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 Does this system require a SORN and if so, please provide SORN name and URL.

Yes.

OPM/GOVT-1

https://www.opm.gov/

https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf

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

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System users. Plant vendors are provided notification during business agreement processes.

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

Yes. However, the information is required as a condition of employment.

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

No.

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

HR GSS does not obtain information from employees.

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 who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2166, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109 - Fax (202) 690-3023 – E-mail: fsis.foia@usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-information-act/foia-requests

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

The FOIA requestor must specify that they would like the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) that gives the individual cause to believe that this system has records pertaining to them.

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

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice, on both the Form 7234-1 and Form 8822-4. The individual's acknowledgement of the Privacy Act Notice and the proffer of information signify the individual's consent to the use of the information. The purpose, use, and authority for collection of information are described in the Privacy Act Notice.

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

N/A

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

Corrections to the data are securely maintained in the same manner as the original data therefore, there is no privacy risk associated with redress available to individuals.

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?

1) First, a user must be in a specific group/department that can justify use of the application. The Network ID/IP address ranges of user groups that can justify using the application are already defined. The HR-GSS admin performs this task.

2) A justifiable user would then have to go to the new user request page for HR-GSS and apply.

3) After the user submits the form, the security officer for that user's department must approve/decline the request. The officer is notified via email.

4) Should the security officer approve, the request is then sent to the HR-GSS administrator.

5) Once approved, the user will have access to the system. The password that the user initially used to submit their request will become their main password to access the application.

8.2 Will Department contractors have access to the system?

Ordinarily no, however should a contractor be authorized to access the system; they will be governed by the contract's identifying ROB for USDA and FSIS systems and security. These types of contracts are routinely reviewed upon renewal by management and contract personnel expert in such matters.

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

USDA Security Awareness and Privacy Training are provided to all users. As a condition of system access, users must successfully complete security training on a regular basis or lose system access rights.

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

Yes, this system was granted an ATO on 08/13/2019.

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

Audits are performed at both the hardware operation system (OS) level and at the application level. At the hardware level, the Engineering Branch (EB) uses auditing tools, such as EventTracker, to monitor server logs, including user logins (failure and success), network connections, system processes, etc.

Audits on the application include:

- Daily reports in which data from the NFC is compared to data within the application to ensure that an employee's overall federal information is accurate
- Actions by the users are logged by the system

The technical safeguards in place include regular vulnerability scans, which scan for vulnerabilities, irregular patch levels, and possible web application vulnerabilities. These scans are performed by the SOC (System Operation Center) and fixes are implemented by the engineering branch. Any security incidents that could possibly compromise the server or application are managed by the SOC Incident Response team.

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?

The risk is that personal information might be shared with individuals who should not have access to the information and who might misuse the information. Therefore, the HR-GSS has mitigated these risks by granting access only to authorized persons. Further, all USDA employees have undergone a background investigation and contractor access is governed by contracts identifying rules of behavior for USDA and FSIS systems and security.

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?

Python Django

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

No

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. Both M-10-22 and M-10-23 have been reviewed by the SO and ISSPM.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

If so, is it done automatically?

N/A - Third party websites are not being used.

If so, is it done on a recurring basis?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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)?

N/A - Third party websites are not being used.

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A.

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.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

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.

N/A - Third party websites are not being used.

Responsible Officials

Joseph T. Abbott
System Owner
1400 Independence Avenue,
SW Washington, DC 20250

Marvin Lykes
Chief Information Security Officer
1400 Independence Ave., SW
Washington, DC 20250

Carl A. Mayes
Chief Information Officer
1400 Independence Ave., SW
Washington, DC 20250

Arianne Perkins
Emmanuel Olufotebi
Privacy Office
Room 2164, South Building
Washington, DC 20250

- **Barring any major updates, no signatures are required until ATO Expiration Date on 08/13/2022**