Privacy Impact Assessment

Policy, E-Government and Fair Information Practices

- Version: 4.5
- Date: May 6, 2020
- Prepared for: SDA OCIO TPA&E

United States Department of Agriculture

Privacy Impact Assessment for the

Enterprise General Support System

May 6, 2020

Contact Point

Frances Byrd

Food Safety and Inspection Service (FSIS)

202-708-8758

Reviewing Official

Emmanuel Olufotebi

Privacy Office

United States Department of Agriculture

Revision History*

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	08/07/2012	Kenneth Hopson	Annual update
2.0	5/30/2013	James Kurucz	Incorporated Department Concurrency Review board
2.1	7/28/2013	Theresa Ottery	Privacy Office Comments
2.2	8/5/2013	James Kurucz	Applied Privacy Office Comments
2.3	8/8/2013	Charles Thompson	Systems Infrastructure Branch Review
2.4	8/15/2013	James Kurucz	Applied comments from the Systems Infrastructure Branch
2.5	8/28/2013	Christopher Douglas	Information Systems Security Branch Review
2.6	9/10/2013	James Kurucz	Applied Edits from ISSB Branch Chief
3.0	8/5/2014	James Kurucz	Annual Update/Template Transfer
3.1	8/5/2014	Robin Wagner	Quality Check
3.2	8/6/2014	James Kurucz	Incorporated Quality Check Comments
3.3	8/7/2014	Mark Brook	Privacy Office Review
3.4	8/12/2014	James Kurucz	Incorporated Privacy Office Comments
3.5	4/23/2015	Rohan A. Heath	Annual Update
3.6	4/1/2016	Rohan A. Heath	Annual Update

3.7	1/3/2017	Rohan A. Heath	ATO
3.8	3/13/2017	Rohan A. Heath	Updates based on Privacy Review
3.9	3/31/2017	Rohan A. Heath	Updates based on Privacy Review
4.0	7/13/2017	Rohan A. Heath	Final
4.1	2/1/2018	Rohan A. Heath	Annual Review
4.2	6/24/2018	Rohan A. Heath	Final
4.3	4/17/2019	Rohan A. Heath	Annual Update
4.4	2/14/2020	Rohan A. Heath	Annual Update (ATO Year)
4.5	5/6/2020	Rohan A. Heath	Updated the AO’s signature block (page 22)

Abstract

This document serves as the Privacy Impact Assessment for the Enterprise General Support System (E-GSS). The Food Safety and Inspection Service (FSIS) E-GSS is the vehicle providing Active Directory and Operating System (OS) infrastructure services to FSIS applications. This PIA is being conducted in conjunction with the March 23, 2017 Privacy Threshold Analysis (PTA), which determined that E-GSS stores information that is considered Personally Identifiable Information (PII) at FSIS.

Overview

The FSIS Enterprise General Support System (E-GSS) is a general support system (GSS) that provides hardware and operating system software support for FSIS major applications. In addition, E-GSS provides Enterprise- wide desktop/laptop, directory, and printer services support.

The FSIS Enterprise General Support System (E-GSS) is the vehicle upon which the FSIS infrastructure depends for all messaging and application capabilities for all FSIS personnel. The information processed in FSIS applications produces reports and information for FSIS staff and for the nation’s meat and poultry suppliers in the United States and abroad.

The FSIS E-GSS is a single domain consisting of over 400 servers in the Enterprise Data Center (EDC) located in Kansas City and St. Louis Metropolitan Areas, and Financial Processing Center (FPC). These servers use the Microsoft, Windows 2008 R2, Windows Server 2012 R2, and Windows Server 2016 operating systems. In addition, at the EDC there are a number of Major Applications that are supported by Linux servers running different flavors of the RedHat Enterprise Linux (RHEL) operating system.

The servers at the EDC and FPC include all servers in the USDA domain provided by Enterprise Active Directory (EAD) with a FSIS Organizational Unit (OU) except for the Laboratory Information Management System (LIMS) servers.

The E-GSS also includes within its boundary, a Windows Imaging Server located in Hanover MD. The Windows Imaging Server is used to image laptops with the FSIS standard Windows workstation baseline and is connected to the FSIS Network.

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 E-GSS collects the following privacy information on government employees, contractors and state inspectors in a state meat and poultry inspection (MPI) program as part of the E-GSS account creation process:

- First and last name
- Work phone number
- Work address
- USDA Enterprise Active Directory Login ID

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

A Footprints ticket is created when an Enterprise Active Directory account needs to be initiated. This ticket must be accompanied by a Quick Issue End User New Account Form which requests the following PII data:

- First and last name
- Work phone number
- Work address

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

The E-GSS supports the FSIS mission by providing network access and infrastructure support for all FSIS systems. Therefore, E-GSS establishes and maintains a process for creating and deleting user accounts in Enterprise Active directory as a means to providing secure network access.

1.4 How is the information collected?

Once employees, contractors successfully complete the appropriate security background check, they are then eligible to receive a network account. A Footprints ticket is then created by the new employee’s supervisor or contracting officer’s representative to request an account be created. This ticket must be accompanied by a Quick Issue End User New Account Form, which requests information noted in section 1.2.

1.5 How will the information be checked for accuracy?

The E-GSS uses EAD domain controllers that respond to security authentication requests, such as users signing-on and checking user permissions. As a result, the EAD domain controllers helps ensure identification and authentication accuracy.

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.

As long as employee data identified in section 1.2 is collected and retained, there is the risk that it may be disclosed to unauthorized individuals. However, PII risks are mitigated by the least possible amount of information being collected by E-GSS. E-GSS servers are maintained in access-controlled facilities, and logical access to FSIS data is restricted to only personnel authorized to view it. Security auditing is enabled on E-GSS operating systems to provide accountability for all personnel by tracking and monitoring system activity.

Network monitoring is also performed daily and provides alerts and defense mechanisms on suspicious or malicious traffic. E-GSS System Administrators and general users access the system using unique accounts. E-GSS cannot be accessed without an authorized account. There are no anonymous user accounts. 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.

All FSIS employees that use the E-GSS must comply with the Agency's general use policy for information technology. Rules of Behavior (ROB), consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. FSIS employees must pass a Government National Agency Check with Inquiries (NACI) background check prior to being granted system access. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

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.

The USDA's Enterprise Active Directory account information for E-GSS is only used for identification and authentication purposes. Once authenticated to the FSIS network, no additional PII information is processed at the E-GSS level.

There are FSIS systems that use the same E-GSS Active Directory credentials to grant access to specific systems. However, this account information is managed at the system level.

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

The USDA's EAD uses domain controllers that respond to security authentication requests, such as user sign-on and checking user permissions. As a result, identification and authentication accuracy is effectively determined.

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

N/A – USDA's Enterprise Active Directory 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.

E-GSS systems are continuously monitored by the FSIS Security Operation Center (SOC) and by the Infrastructure Operations Division (IOD) Engineering Branch using a number of automated tools to ensure that information is handled in accordance with the above described uses in section 2.1.

In addition, each year the Office of the Chief Information Officer (OCIO) conducts Security Awareness Training (SAT) for all FSIS employees and contractors. Users, including state MPI users that do not take and pass this required annual training will have their access to the FSIS environment (network and applications) revoked. Additionally, FSIS employees and contractors are briefed on the acceptable system and communications Rules of Behavior as part of the SAT training,

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?

Information is retained for as long as the user is active. The E-GSS Asig Account Operators receive “Report of Separations” and/or and Footprints ticket notifications on a regular basis for users that have separated from the agency. Thereafter, the user’s Enterprise Active Directory account is immediately deleted. In addition, E-GSS OU administrators perform routine checks regarding the reported separated staff to ensure their accounts are no longer active.

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.

There are no additional risks associated with the length of time data is stored. The actions taken to mitigate risk (noted in section 1.7) address any ongoing risks appropriately.

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?

Since E-GSS is a GSS within FSIS, there are applications that have authentication mechanisms to check whether the user has a valid Enterprise Active Directory account. Systems use this authentication method instead of creating their own unique user login ID for each user.

4.2 How is the information transmitted or disclosed?

PII data is not use for reporting or retrieval purposes.

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 information collected by E-GSS is available to all USDA agencies in the GAL and only contains basic information, such as username, email address, work phone number, and office address. The sharing of this information is critical in allowing FSIS to accomplish its mission of protecting public health. The risks and mitigating actions taken are discussed in section 1.7 above.

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 is not 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.

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

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

Not Applicable. E-GSS does not share PII outside of the Department.

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

Not Applicable. E-GSS does not share PII outside of the Department.

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.

No. The E-GSS does not require a SORN.

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, having access to USDA's Enterprise Active Directory is required for an employee to perform their responsibilities. Employees and contractors that fail to complete the appropriate background checks, which include providing PII, are denied access to USDA facilities and information systems.

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.

All employees and contractors are required to read and consent to the AD-1188 and NACI forms prior to being granted access to E-GSS. Therefore, there are no risks of individuals being unaware of their PII being collected.

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?

Individuals can correct inaccurate or erroneous information by contacting the FSIS' Office of the Chief Human Resource Officer.

Non-FSIS employees can contact the technical services center within the Office of Policy and Program Development.

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

The FSIS Human Resources (HR) would contact an individual via email if it believes that the individual's information is incorrect, and provide the individual with the procedures to correct their information.

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

Formal redress is provided.

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 PII data are securely maintained in the same manner as the original data. Therefore, there is no privacy risk associated with redress procedures 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?

The successful completion of the AD-1188 or NACI security background check is the first step in users gain access to E-GSS. In addition, SAT must be passed, which delineates the acceptable Rules of Behavior when accessing the FSIS network. SAT records are then retained by the FSIS Information Assurance Branch (IAD) to monitor user compliance and tracked in AgLearn, USDA eLearning platform. System Administrators must sign a Privilege Rules of Behavior form before being granted elevated system access.

8.2 Will Department contractors have access to the system?

Yes, USDA contractors are authorized to access E-GSS through an Enterprise Active Directory account and are able to view employee information available in the Microsoft Outlook Global Address List (GAL).

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

All users are required to undergo Security Awareness Training (SAT) prior to accessing E-GSS, as well as complete annual refresher training to retain access.

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

The E-GSS ATO was granted on July 13, 2017.

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

The E-GSS system is continuously monitored by the FSIS Security Operations Center (SOC) and by the Innovation and Operations Division (IOD) Engineering Branch, using a number of automated tools to ensure FSIS data is handled in accordance with the FSIS security policies. In addition, encryption software is installed on all FSIS servers to protect their data.

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 primary risks are that the employee information may be incorrect or that it may be disclosed to unauthorized individuals. Risks are mitigated by granting access only to authorized persons, and by ensuring regular security training is required and taken by all users.

All USDA employees undergo thorough background investigations. In addition, E-GSS resides on a secure USDA FSIS network that is continuously monitored by the FSIS SOC and the IOD Engineering Branch for suspicious or unauthorized activity. See Section 1.7 above for a description of the controls that have been put in place for the FSIS environment.

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?

E-GSS is a General Support System.

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/or applications.

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

Frances Byrd
System Owner
1400 Independence Ave., SW
Washington, DC 20250

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

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

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

Approval Signatures

Agreed: FRANCES BYRD Digitally signed by FRANCES BYRD Date: 2020.05.11 14:26:01 -04'00'

Frances Byrd Date
System Owner

Agreed: MARVIN LYKES Digitally signed by MARVIN LYKES Date: 2020.05.11 16:14:07 -04'00'

Marvin Lykes Date
Chief Information Security Officer

Agreed: CARL MAYES Digitally signed by CARL MAYES Date: 2020.05.12 13:01:50 -04'00'

Carl A. Mayes Date
Chief Information Officer

Agreed: EMMANUEL OLUFOTEBI Digitally signed by EMMANUEL OLUFOTEBI Date: 2020.05.12 09:58:09 -04'00'

Emmanuel Olufotebi Date
Privacy Office