

# Privacy Impact Assessment

Enterprise General Support System (E-GSS)

- Version: 1.0
- Date: *August 07, 2012*
- Prepared for: USDA OCIO





## Privacy Impact Assessment – E-GSS

---

Document Revision and History			
Revision	Date	Author	Comments
1.0	08/07/2012	Kenneth Hopson	Annual update

## 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 a single-domain vehicle providing Active Directory and Operating System (OS) infrastructure services to FSIS applications. This PIA is being conducted in conjunction with February 2012 Privacy Threshold Analysis conducted (PTA), which determined that E-GSS stores information that can be considered Personally Identifiable Information (PII).

## Overview

The FSIS E-GSS is the vehicle upon which the FSIS infrastructure depends for all messaging and application capabilities for all FSIS personnel. The FSIS E-GSS is an Active Directory domain with servers distributed across the Enterprise Data Centers (EDC) located in Kansas City and St. Louis Metropolitan Areas, as well as among the district offices, laboratories, Technical Service Center (TSC), Human Resources Division (HRD) and Financial Processing Center (FPC).

The E-GSS user base is comprised of USDA secretaries, program/management analysts, veterinary medical officers, food technologists, compliance officers, consumer safety inspectors, food inspectors, as well as state inspectors with State Meat and Poultry Inspection personnel.

## 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 program as part of the E-GSS account creation process:

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

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

A Footprints ticket is created when a FSIS 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 Active directory, as a means to providing secure network access.

### **1.4 How is the information collected?**

Once employees, contractors and state employees successfully complete the appropriate security background check, they are then eligible to receive a network account. A Footprints ticket is then created by E-GSS administrators to request that 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 domain controllers that respond to security authentication requests, such as users signing-on and checking user permissions. As a result, the E-GSS domain controllers helps ensure identification and authentication accuracy.

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

US Code TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate.

The November 18, 2008, amendment to the Executive Order 9397 directs Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unauthorized use.

44 U.S.C. 3101 states that each USDA mission area, agency, and staff office shall create and maintain proper and adequate documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the Department of Agriculture (Department) to protect the legal and financial rights of the Government and of persons directly affected by the Department's activities.

Also see: 5 U.S.C. Chapter 552, 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071, 44 U.S.C. 3101 et seq., 44 U.S.C. 3506, Title 7 CFR 2.37, 36 CFR Chapter 12, Subchapter B, 36 CFR Part 1234, eGovernment Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36), OMB Circular A-130, NARA - Disposition of Federal Records: A Records Management Handbook, NARA General Records Schedules.

**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 fact that a very minimal amount of information is collected by E-GSS. Also E-GSS servers are maintained in access-controlled facilities, and logical access to FSIS data is restricted to only authorized personnel. 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.

**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 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 systems within FSIS that use the same E-GSS Active Directory credentials to grant access to their 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 E-GSS 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 - FSIS 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 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, annual Computer Security Awareness Training (CSAT) is conducted by the Office of the Chief Information Officer (OCIO). Users that do not take and pass this required annual training will have their access to the FSIS environment (network and applications) revoked. Every year users are required to sign a Rules of Behavior form every year and administrators, a Privilege Rules of Behavior form.

## **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 Account Operators receive “Report of Separations” and/or and a Footprints ticket notifications on a regular basis for users that have separated from the agency. Thereafter, the user’s Active Directory account is immediately deleted. In addition, E-GSS 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 General Support System (GSS) within FSIS, there are applications that have authentication mechanisms to check whether the user has a valid 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?**

System personnel can perform user account validation using the FSIS Global Address Lookup (GAL) in Microsoft Outlook, which is visible to all USDA agencies. In addition, calls can also be made by department managers to the Footprints Help Desk to verify that a user account is active.

### **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?**

FSIS network accounts are created, as needed for State Meat and Poultry Inspection Program personnel. As a result information is shared as it relates to the inspection duties assigned to the individual.

- 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.**

The GAL information collected by E-GSS is available to all employees, as well as approved contractor state employees and it is required system functionality. However, the GAL only contains basic information, such as username, email address, work phone number, and office address as discussed in section 1 above. Therefore, the sharing of E-GSS PII data is similar for internal and approved external account users. No SORN is required.

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

State employees must access the FSIS network through a designated FSIS facility or connect through the FSIS VPN using a valid user account to accomplish their duties in support of FSIS. Therefore, state employees are exposed to the same security safeguards as internal FSIS users.

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

As mentioned in section 5.3, state employees must adhere to the same security mechanisms as internal FSIS users. In addition, The Agriculture Learning (AgLearn) system is USDA's department-wide system for managing training records and activity at USDA. As part of the FSIS Security Awareness Training Program, all FSIS employees, contractors and state employees are required to take the AgLearn Information Security Awareness training annually. During training, personnel are briefed on the acceptable "Rules of Behavior" as required by law when accessing the FSIS network. At the end of the training, personnel must sign a Rules of Behavior acknowledgement form and successfully pass the exam at the end of the training. System administrators are required to sign a Privilege Rules of Behavior form.

## 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?**

Yes. Federal employees must complete an AD-1188 justification as part of the FSIS security clearance process before being granted access to USDA facilities and information systems (i.e. E-GSS). Contained therein is the following comprehensive notice (Note that the Active Directory does not contain the Social Security Number):

*“ The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN is needed to keep records accurate because other people many have the same name and birth date. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you need to have access as indicated above or 2) determine that your access to such information is no longer needed. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.”*

Contractors are required to complete a National Agency Check with Inquiries (NACI) prior to being granted access to USDA facilities and information systems (i.e. E-GSS). In the NACI, users are provided the following disclaimer in regards to their personal information:

*“The information collected will be protected from disclosure under the Privacy Act of 1974. We do not retain or distribute collected information to any parties outside the USDA, except as necessary to conduct official U.S. Government business, and we do not distribute this data to non-Government entities. Information collected will be retained at our discretion in a readable form for as long as necessary to complete the investigation. The information may be retained in an archival form as required by Federal laws and regulations governing the retention of historical records of Government agencies.”*

PII notifications for state employees are performed at the state level through formally approved state trusted liaisons. These trusted liaisons work with the FSIS OCIO coordinators when requesting FSIS network accounts for state employees.

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

Yes. However, having access to 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.

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

No.

**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.**

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.

All Notices to state personnel are provided at the state level. E-GSS works with state trusted liaisons to ensure that state employees have been properly vetted according to federal requirements and provided with the appropriate PII notices.

## **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?**

USDA employees and contractors may contact FSIS Human Resources (HR) to gain access to their PII information.

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

Individuals who have reason to believe that E-GSS might have inaccurate or erroneous PII records pertaining to them should write to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 690-3882 Fax (202) 690-3023 - Email: [fsis.foia@usda.gov](mailto:fsis.foia@usda.gov).

The FOIA requestor must specify that he or she wishes 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) which gives the individual cause to believe that this system has records pertaining to him or her.

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

Individuals seeking to contest their PII being collected may submit a request in writing to the Headquarters or component's FOIA officer, whose contact information can be found at <http://www.da.usda.gov/foia.htm> under "contacts".

**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, Computer Security Awareness Training (CSAT) must be passed which delineates the acceptable Rules of Behavior when accessing the FSIS network. CSAT records are then retained by the FSIS Information Assurance Branch (IAD) to monitor user compliance. 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 Active Directory account and are able to view employee information available in the Microsoft Outlook 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 Computer Security Awareness Training prior to accessing E-GSS, as well as complete annual refresher training in order 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 27-July-2011.

**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 SOC and by the IOD Engineering Branch using a number of automated tools to ensure that FSIS data is handled in accordance with the FSIS security policies.

**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 that regular security training is required by all users. All employees of USDA 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”?**

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

**10.2 What is the specific purpose of the agency’s use of 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> party websites and/or applications purged periodically?**

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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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?**

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 -

**10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3<sup>rd</sup> 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

**Miguel Rivera**—System Owner, E-GSS  
Chief Technology Officer  
Office of the Chief Information Officer  
Office of the Administrator  
Food Safety and Inspection Service  
United States Department of Agriculture

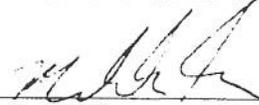
**Alicemary Leach** – Director, ECIMS  
Office of Public Affairs and Consumer Education  
Food Safety and Inspection Service  
United States Department of Agriculture

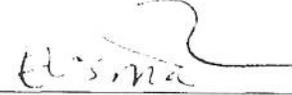
**Elamin Osman** – Chief Information Security Officer  
Office of the Chief Information Officer  
Office of the Administrator  
United States Department of Agriculture

**Janet Stevens** - Chief Information Officer  
Office of the Chief Information Officer  
Office of the Administrator  
Food Safety and Inspection Service  
United States Department of Agriculture

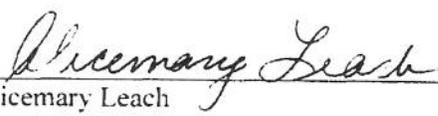


**PRIVACY IMPACT ASSESSMENT APPROVALS**

Agreed:  8-7-12  
Miguel Rivera  
System Owner Date

Agreed:  09/17/12  
Elamin Osman  
Chief Information Security Officer (CISO) Date

Agreed:  9/25/12  
Janet Stevens  
Chief Information Officer (CIO) Date

Agreed:  8-7-12  
Alicemary Leach  
Privacy Officer Date