Privacy Impact Assessment

FNS Infrastructure Services General Support System (FNS I-GSS)

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: March 30, 2020
- Prepared for: USDA OCIO-Policy and Directives - Privacy Office

USDA

United States Department of Agriculture

Privacy Impact Assessment for the

FNS Infrastructure Services General Support System (FNS I-GSS)

March 30, 2020

Contact Point
Sonja Farrell
FNS/OIT/TD
703-305-2275

Reviewing Official
Miguel Marling
FNS Privacy Officer
United States Department of Agriculture
(703) 305-1627

Abstract

This document is a Privacy Impact Assessment (PIA) for the FNS Infrastructure Services General Support System (FNS I-GSS). FNS I-GSS provides the general support infrastructure that ties in all Agency users to shared programs and/or applications owned by either the Agency or other government entities. The PIA is being completed due to a Privacy Threshold Analysis (PTA) that indicated a PIA was required for the FNS I-GSS system to meet Federal privacy compliance requirements.

Overview

The FNS Infrastructure Services General Support System (FNS I-GSS) provides telecommunication, networking, and systems support. It encompasses applications, file and print servers and access to the United States Department of Agriculture (USDA) mail system, for Seven Regional Offices (RO), 14 Field Offices (FOs), and the National Office (NO). The FNS I-GSS provides technical and programmatic security support to dedicated FNS applications, and also includes applications hosted at the National Office and on certain Cloud Service Providers (CSPs), as well as those hosted at USDA data centers and FNS facilities.

FNS I-GSS only allows public access for the locator applications that are hosted in the FedRAMP Amazon Web Services (AWS) GovCloud environment. This access is protected via HTTPS, and these applications do not require accounts or require authentication for public users. No other public access is provided. The FNS I-GSS uses Microsoft Active Directory (AD) as the foundation for user access and inherits its AD services from USDA.

The FNS I-GSS ATO boundary includes the following program and applications, along with the FNS-managed web application platforms and database management system (DBMS) platforms that support them:

FNS Program: The FNS Program is a common control program that provides management and operational controls that are common to, and inherited by, FNS systems and applications. Currently the FNS Program addresses common NIST controls for FNS Information Systems for the following control families:

- Access Control (AC)
- Accountability, Audit, and Risk Management (AR) 5
- Awareness and Training Controls (AT)
- Audit and Accountability Controls (AU)
- Security Assessment and Authorization Controls (CA)
- Configuration Management Controls (CM)
- Contingency Planning Controls (CP)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Identification and Authentication Controls (IA)

- Individual Participation Control (IP)
- Incident Response Controls (IR)
- Maintenance Controls (MA)
- Media Protection Controls (MP)
- Physical and Environmental Protection Controls (PE)
- Planning Controls (PL)
- Personnel Security Controls (PS)
- Risk Assessment Controls (RA)
- System and Services Acquisition Controls (SA)
- System and Communications Protection Controls (SC)
- Security (SE)
- System and Information Integrity Controls (SI)
- Transparency (TR)

DISC Colocation-Hosted Applications

The following FNS I-GSS applications are hosted at the Digital Infrastructure Services Center (DISC) Colocation facility in Kansas City, Missouri:

Alloy Navigator (Alloy): Alloy Navigator is a helpdesk tool that is used for managing configuration changes in the FNS OIT environment, including IT infrastructure and IT service support.

ARCHIBUS: ARCHIBUS (https://archibus.fns.usda.gov/archibus) is a total infrastructure and facility management software program that provides various modules for space management, asset management, and other workplace services.

FNS SharePoint (SPGSS): FNS SharePoint is a web platform based on Microsoft SharePoint 2016 Server that provides a communication platform, collaboration space, and application platform used to collect and disseminate information for general interoffice work purposes. It provides FNS staff (employees and vendors) the opportunity for efficiently collaborate with team members; manage documents; find agency resources; search for experts and business information; manage business processes, content and work flow (custom applications); and leverage business insight to make better and informed decisions.

MoveIT Secure Transfer Tool (MoveIT): MoveIT (https://transfer.fns.usda.gov) is a secure file transfer protocol system developed by IPSwitch that provides external/internal connections for uploads/downloads into/from FNS applications/file shares. It also automates the transfer of uploaded/downloaded files to various FNS applications, as well as FNS network shares. It provides seamless connections for transfers to DISC FTPs mainframe and State Agency mainframes.

Optimized Procurement System (OPS): OPS (https://ops.usda.net) provides account and procurement support services, to include a workflow process for submission and approval of AD-700 forms and an integrated reporting on the status of funds.

Peer Awards: Peer Awards (https://maropeerawards/) is a platform enables employees to recognize and reward co-workers with non-monetary awards for specific accomplishments.

States Systems Comprehensive Outlook & Unified Tracker (SCOUT): SCOUT serves as a tracking, document management, and reporting tool used by the State Systems Office (SSO) to track, manage, and forecast activity in all SSO areas of responsibility, including monitoring of State Advance Planning Documents (APD), Agency leadership decisions, and state project risk profiles.

Travel Reporting and Integrated Projections System (TRIPS): TRIPS (http://trips/) is an intranet-based system used by FNS regions to manage travel funds.

Visitor Management System (VMS): VMS is a Microsoft Windows-based system used for digital check in/out. This computer program captures and stores visitor information and creates professional identification badges and visitors' tags.

FNS I-GSS only allows public access for the locator applications that are hosted in the FedRAMP Amazon Web Services (AWS) GovCloud environment. This access is protected via HTTPS, and these applications do not require accounts or require authentication for public users. No other public access is provided. The FNS I-GSS uses Microsoft Active Directory (AD) as the foundation for user access and inherits its AD services from USDA.

FNS also allows public access for the following FNS I-GSS application that is hosted in the GSA Cloud.gov cloud infrastructure:

Data Validation Service (DVS): DVS is a platform-independent, web-based service accessible by design to all State systems. It simplifies the States' role in data validation by passing error messages to SFAs as they are submitting the data to their States.

FNS I-GSS is supported by the USDA Enterprise Active Directory (EAD), which is integrated with existing Department-wide applications and services via the Microsoft Active Directory Federation Service (ADFS). ADFS is a claims-based federation service (authentication) deployed in EAD to support Single Sign-On-Enabled web applications across various domains. This portion of the FNS I-GSS is covered under the USDA EAD PIA.

The information collected by the FNS I-GSS includes names, phone numbers, and business addresses for all FNS employees and contractors that require authentication to the FNS network and EAD. User accounts are created and stored as objects in the USDA AD Domain Services. Each user that accesses resources in the Windows domain must have a user-access-account in the AD. The AD account is used to identify and authenticate the specific user so that the specific user may use a specific network resource. The FNS I-GSS includes end-user workstations, and therefore might contain other Agency-related information.

A typical transaction would include an end user logging into a workstation (whether in the office or remotely), authenticating against an AD domain controller, performing email communications, browsing the Internet, performing document processing, and/or logging into Agency owned applications.

FNS I-GSS includes telecommunications equipment (e.g., switches, routers, VPN devices, etc.); server infrastructure and central storage devices; enterprise applications; and end-user workstations. The enterprise applications include print servers, security appliances/systems, patch management solutions, auditing, remote access systems, and authentication systems.

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?

FNS I-GSS only collects name, business address, and business phone number of the users that authenticate to the system. Users include both Federal employees and contractors. End user workstations and/or end user directories contained within the central storage solution might include other information used in the daily operations of the Agency.

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

FNS I-GSS technical staff obtain end user information via an FNS 674 (User Access Request Form). The requester populates the data. The data is then submitted through a series of approved processes and information verification procedures.

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

FNS I-GSS information is collected to create user accounts that the end user will utilize to authenticate to the system. This ensures that there is a level of security in place to protect the interconnected systems and government assets.

1.4 How is the information collected?

FNS I-GSS technical staff_obtain end user information via an FNS 674 (User Access Request Form). The requester populates the data. The data is then submitted through a series of approved processes and information verification procedures.

1.5 How will the information be checked for accuracy?

As part of the FNS 674 process, the user's name provided is cross-referenced with the background investigation legal name of record. Address and phone numbers are not pertinent to the authentication process and are not verified.

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

This process is driven by privacy laws, regulations, and government requirements, including the following:
Privacy Act (5 U.S.C. 552a(e));
e-Govt. Act, Sec. 208(c) (44 U.S.C. 3501);
Office of Management and Budget (OMB) Circular A-130;
Department Regulation 3515-002;
Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

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

Standard USDA network and information security protocols that protect personally identifiable information (PII) are in place, and records retention requirements will be followed in accordance with FNS Agency Records Retention Schedule and Records Management Policy 270-1. The FNS 674 includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities. Further, users are assigned roles and constraints within the system that limit their access to data and mitigate the risk that PII would be disclosed. eAuthentication is also used by authorized users to access certain FNS I-GSS applications.

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 use of the collected data for FNS I-GSS is strictly to provide a level of authentication for the end user to obtain access to the system as well as to determine what role-based access for resources stored on the FNS I-GSS.

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

The technical staff that support the FNS I-GSS use Splunk, FNS SolarWinds, Microsoft Active Directory, and Windows Operating Systems to analyze data pertaining to user authentication. Data that is produced include audit logs for when users log in, log out, and access resources.

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

FNS I-GSS does not make use of 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.

Access to the FNS I-GSS applications requires a unique user account assigned to the IT administration staff by the use of an FNS 674. Each authorized user must sign a User Access Request Form before given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of his or her official duties. The FNS 674 includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g., curiosity browsing). Users are assigned roles and constraints within the system that limit their access to data.

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 user account is disabled/de-provisioned immediately upon user separation from the Agency and data is retained for 90 days.

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

Yes, GRS 24, Item 6(b) see GRS 20, Item 1(c).

Regular backups are performed and recovery procedures are in place for FNS I-GSS. Access to computerized files is password protected and under the direct supervision of the system manager. Data will be maintained based on the identification records retention for the specific data types for FNS I-GSS applications.

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

One risk identified for user account information being retained for a period of time after the user leaves the Agency is that it could be used by another individual other than that user it was created for. This risk is mitigated by the use of automated de-provisioning processes established that reset the password, remove all group membership and disable the account so that no USDA or FNS resources are accessible. Additionally, the user account logon is disabled by the Enterprise Entitlements Management Service (Identity Manager) for the eAuthentication, which works with the Human Resources system to globally disable the user's credentials via all USDA integrated systems. This prevents reuse of the user account.

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 user's login information is stored in the USDA Federated Enterprise Active Directory (EAD). The information shared is the information collected by the FNS I-GSS pertaining to the user accounts (name, business address, and business phone number). The EAD provides a centralized Active Directory solution across USDA Agencies.

4.2 How is the information transmitted or disclosed?

The information is transmitted via the USDA ENS UTN MPLS cloud. Both USDA FNS and USDA CEC are located on the USDA ENS UTN MPLS cloud. The domain controllers synchronize the user account information among all of the USDA domain controllers.

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.

Standard USDA network and information security protocols that protect personally identifiable information (PII) are in place, and records retention requirements will be followed in accordance with FNS Agency Records Retention Schedule and Records Management Policy 270-1. The FNS 674 includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities. Further, users are assigned roles and constraints within the system that limit their access to data and mitigate the risk that PII would be disclosed. eAuthentication is also used by authorized users to access certain FNS I-GSS applications.

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?

The user login information is shared with the Enterprise Messaging System (EMS) which is hosted by Microsoft (Office 365). The information shared is the information collected by FNS I-GSS pertaining to the user accounts (name, business address, and business phone number). EMS is used to provide end users with messaging (email) and collaboration (SharePoint, Lync/Communicator, and LiveMeeting) capabilities. The shared information is used for authentication purposes.

5.2 Is the sharing of personally identifiable information (PII) 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 PII outside of USDA.

Not applicable. There is no sharing of PII outside of the Department.

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

The EMS is hosted across two Microsoft datacenters. USDA CEC maintains domain controllers at these locations to ensure user authentication is successful; the CEC has a PIA covering the USDA's data sharing for the Federated EAD. All communications to these sites are over the USDA ENS UTN MPLS cloud to the USDA and FNS network. All domain controllers synchronize the user account information.

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

Standard USDA network and information security protocols that protect personally identifiable information (PII) are in place, and records retention requirements will be followed in accordance with FNS Agency Records Retention Schedule and Records Management Policy 270-1. The FNS 674 includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities. Further, users are assigned roles and constraints within the system that limit their access to data and mitigate the risk that PII would be disclosed. eAuthentication is also used by authorized users to access certain FNS I-GSS applications.

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

Not applicable.

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

Only minimal PII is collected to process the FNS 674. Notice is not provided as further information is not collected.

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

There is no information collection beyond use of the FNS 674 to establish user access.

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

Individuals must complete and sign the FNS 674 to gain system access. There is no further information collection.

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.

There is no information collection beyond use of the FNS 674 to establish user access, and records retention requirements will be followed in accordance with FNS Agency Records Retention Schedule and Records Management Policy 270-1.

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 must contact the FNS OIT Service Desk to gain access to their information.

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

Individauls must contact the FNS OIT Service Desk to correct any information.

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

Individuals are informed when completing the FNS 674 and upon completion of the security training.

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

Not Applicable. Individuals would contact the FNS OIT Service Desk to redress the information.

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

There is no information collection beyond use of the FNS 674 to establish user access, and records retention requirements will be followed in accordance with FNS Agency Records Retention Schedule and Records Management Policy 270-1.

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?

Users can gain access to FNS I-GSS upon completion of the FNS 674 process. Once a user completes their portion of the form it goes through and approval process that includes Supervisor, Security Official, and the System Authorizing Official. Anyone that has a fully approved FNS 674 and has passed their Information Security Awareness (ISA) training may obtain access. These procedures are documented as part of the FNS 674 process.

8.2 Will Department contractors have access to the system?

All FNS staff – employees and contractors – have access to the FNS I-GSS upon successful completion of the FNS 674 process.

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

Privacy Training is included in the annual Information Security Awareness (ISA) training provided by the USDA. Every employee and contractor with access to the network is required to complete the annual Computer Security Awareness Training.

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

The last completed A&A for FNS I-GSS was September 2016.

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

The FNS I-GSS users are audited annually through the Recertification process. An FNS 674 is verified as on file for every user that has access to the network. All PII on the FNS 674 is redacted before the form is updated to our documents repository on the network.

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?

There is no information collection beyond use of the FNS 674 to establish user access, and records retention requirements will be followed in accordance with FNS Agency Records Retention Schedule and Records Management Policy 270-1.

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?

The FNS I-GSS is a General Support System (GSS) that provides telecommunication and systems support.

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

Although control weaknesses and vulnerabilities periodically arise in the I-GSS, FNS has established a series of mitigating controls to prevent and detect/correct issues as they occur. These controls include network perimeter controls and network level authentication and auditing controls, as well as IT security and privacy continuous monitoring tools and procedures.

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?

Not applicable. FNS I-GSS does not use third party websites or applications.

10.3 What PII will become available through the agency's use of 3rd party websites and/or applications?

Not applicable. FNS I-GSS does not use third party websites or applications.

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

Not applicable. FNS I-GSS does not use third party websites or 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?

Not applicable. FNS I-GSS does not use third party websites or applications.

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

Not applicable. FNS I-GSS does not use third party websites or applications.

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

Not applicable. FNS I-GSS does not use third party websites or 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?

Not applicable. FNS I-GSS does not use third party websites or 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)?

Not applicable. FNS I-GSS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

Not applicable.

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?

Not applicable.

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.

Not applicable.

Responsible Officials

JOSEPH BINNS Digitally signed by JOSEPH BINNS
Date: 2020.05.05 09:24:48 -04'00'

Joseph Binns
CISO/ISSPM
Information Security Office
Food and Nutrition Service
United States Department of Agriculture

Date

Approval Signature

Sonja Farrell
System Owner
Director, Technology Division
Food and Nutrition Service
United States Department of Agriculture

Date