

Privacy Impact Assessment NASS Infrastructure (INF) GSS

National Agricultural Statistics Service

- Template Version: 1.0
- Date: June 16, 2016
- Prepared for: USDA NASS





Privacy Impact Assessment for the NASS Infrastructure (INF) GSS

June 16, 2016

Contact Point

Dave Brooks
National Agricultural Statistics Service
(202)720-6019

Reviewing Official

Renato Chan
Chief, NASS Security
National Agricultural Statistics Service
United States Department of Agriculture
(202)720-4068

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

This PIA is for the NASS Infrastructure (INF) General Support System. It serves as the default repository of data used and processed by various Agency desktop applications, and provides NASS employees local access to file and print sharing services to the Agency enterprise network. It also provides client access to various desktop applications, including email. The PIA is being conducted to maintain a record of time and attendance for every NASS employee, and maintain records necessary to perform routine personnel actions.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

This PIA is for NASS Infrastructure (INF) General Support System (GSS). The System Owners for NASS INF GSS are Tesfa Gebreamlak and Aida Aguilar. The NASS INF GSS was granted authority to operate on 4/27/2015 (as the NASS WAN GSS). Its functionalities include file sharing, printing, communication, e-mail, security, and application deployment services.

The NASS INF GSS serves as the backbone and primary GSS for the agency and is responsible for supporting all other NASS systems and applications. The NASS INF GSS architecture consists primarily of a Citrix virtual environment for all its endpoint computing, as well as

Cisco switches, routers, firewalls, and Microsoft servers providing file sharing, printing, communication, e-mail, security, and application deployment services.

The NASS INF GSS serves as the backbone and primary GSS for the agency and is responsible for supporting all other NASS systems and applications. The NASS INF GSS architecture consists primarily of a Citrix virtual environment for all its endpoint computing, Microsoft servers providing file sharing, printing, communication, e-mail, security, and application deployment services, and UNIX/Linux servers that host the NASS Data and Applications Major Application.

The Headquarters LAN in Washington, D.C. consists of Windows desktops, laptops, as well as Wyse thin clients, providing office automation needs for over 400 users. These endpoints are primarily used to host virtual sessions off the NASS Citrix platform housed at the USDA National Information Technology Center (NITC) in Kansas City, MO.

The NASS UNIX platform consists of UNIX-based systems running Linux and AIX. These servers provide critical support to the mission of NASS to produce and disseminate timely, accurate, and useful statistical information to its clients (i.e., farmers and agriculture business, commodity markets, government, and the general public). Headquarters staff are distributed across four wings and two floors. LAN is connected via a core switch and separate switches located in the various wings. There are approximately 400 staff members in HQ all of which have a personal computer on their desktop and a small percentage have two computers. Printers are shared at around one printer for every five employees.

The NASS INF GSS has migrated the majority of its remote Field Offices (FO) to a virtual environment; servers are now hosted at the USDA National Information Technology Center (NITC) in Kansas City. Citrix is employed for thin client computing, though machines can still be used as thick clients if desired.

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?

Information on NASS employees include: (1) name, (2) home address, (3) telephone number, (4) Social Security Number, and (5) employment history.

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

Information is collected from employees and the National Finance Center (NFC).

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

To maintain a record of time and attendance for every NASS employee, and maintain records necessary to perform routine personnel actions.

1.4 How is the information collected?

Information is collected from employee paper records as well as from NFC electronic records.

1.5 How will the information be checked for accuracy?

There are no additional checks for accuracy as information is assumed accurate

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

5 U.S.C. 301. In addition, information in the system for NASS employees are collected routinely for administrative functions such as time and attendance, and travel reimbursements.

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

There are risks of unauthorized users potentially accessing privacy data. These are mitigated by policy, and employing various security measures such as access control, auditing, encryption where possible.

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.

Information in the system for NASS employees are used routinely for administrative functions such as time and attendance, and travel reimbursements.

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

NASS uses primarily the Time and Attendance (T&A) system for NASS employee records. No additional tools are used.

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

N/A. NASS INF GSS is not directly available to public.

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.

N/A. NASS INF GSS is not directly available to public.

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?

Retention of data follows schedules approved by the U.S. National Archives and Records Administration (NARA).

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 brought about by the length of time data is retained.

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?

None, access to data is limited only to NASS users who have a need to modify, maintain and review the data.

4.2 How is the information transmitted or disclosed?

Access to data is limited only to NASS users who have a need to modify, maintain and review the data. Each user also signs a pledge of confidentiality that carries severe legal penalties for violating the pledge.

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.

N/A. Access to data is limited only to NASS.

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 any external organization.

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.

N/A

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

N/A

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

N/A

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, details and scope of the data collected is discussed when the individual comes on board.

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

Yes, individuals have the opportunity and/or right to decline to provide information, and are told potential issues of not having enough information.

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

Yes, individuals have the right to consent to information. This is explained to individuals while given the option to whether give information on or not when they first come onboard.

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.

This system is covered by both OPM/GOVT-1, "General Personnel Records," and USDA/OP-1, "Personnel and Payroll System for USDA Employees." which are published on the Federal Register.

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?

Access to data is limited only to NASS users who have a need to modify, maintain and review the data. Access to the data is determined by the system manager of the

underlying application or system. Each user also signs a pledge of confidentiality that carries severe legal penalties for violating the pledge.

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

Inaccurate or erroneous information are corrected by NASS staff responsible for maintaining the records.

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

To correct erroneous information, individuals are notified by the NASS Human Resources and Services Officer (HRSO) either through email or phone call on how to go about correcting their information.

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

N/A, 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.

There are no known privacy risks.

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?

Access to the data is determined by the system manager of the underlying application or system. Each LAN user is assigned a network account. Appropriate rights are assigned to these accounts which control what users can access within the system. Access request as well as approval is documented accordingly by management and the Technical Services Branch. The Computer Security Staff audits access routinely.

8.2 Will Department contractors have access to the system?

No.

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

Privacy training is provided generally through the required annual USDA security awareness and role-based training. In addition, personnel with significant information security responsibility are required to complete role-based training.

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

Yes.

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

The NASS Computer Security staff audits access routinely.

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?

Due to the nature of the information processed within the system, there are privacy risks involved. NASS employs several security controls, including: proper network rights assignments (access control), auditing, and data masking/encryption to lower risks to a level acceptable to NASS and in compliance with Privacy Act of 1974 provisions.

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?

NASS General Support System (GSS).

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.

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

There is no 3rd party websites and/or applications in use.

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

N/A

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

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

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

N/A

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

N/A

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

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

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

10.10 Does the system use web measurement and customization technology?

N/A

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



Responsible Officials

Dave Brooks
PII Information Owner
National Agricultural Statistics Service
United States Department of Agriculture

Approval Signature

RENATO CHAN Digitally signed by RENATO CHAN
DN: c=US, o=U.S. Government, ou=Department of
Agriculture, cn=RENATO CHAN,
0.9.2342.19200300.100.1.1=12001000002672
Date: 2017.04.21 09:58:45 -0400'

Name: Renato Chan
Title: Chief NASS Security
Agency: NASS
United States Department of Agriculture