Privacy Impact Assessment

Network General Support System (N-GSS)

- Version: 2.3
- Date: June 25,2012
- Prepared for: Food Safety and Inspection Service (FSIS), Office of the Administrator, Office of the Chief Information System Officer

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
2.0	January 2007		Reformatted and reorganized
2.1	January 2008		Changed title page to match official name
2.2	January 2008		Changed system name within document to match official name
2.3	June 25, 2012	Mark Whitaker	Updated to reflect new department template (from August 2010).

Abstract

This document serves as the Privacy Impact Assessment for the FSIS Network General Support System (N-GSS). The purpose of the system is to provide communication services to FSIS personnel (employees and contractors) and the FSIS applications.

Overview

The United States Department of Agriculture (USDA) FSIS Network is a general support system (GSS). It represents the core components of the FSIS communication infrastructure and is therefore essential to the FSIS mission of ensuring a safe and wholesome food supply for the nation's population. The N-GSS does not store information other than information technology data relating to the administration of network devices, however, it does provide communications support for other FSIS GSS systems that do. The N-GSS data is maintained on the devices that comprise the network infrastructure (routers, switches, intrusion detection system (IDS)/intrusion prevention system (IPS), etc.) or dedicated workstations that provide device management functions.

The FSIS primary backbone consists of the FSIS Universal Telecommunications Network (UTN), which is connected to USDA UTN, which provides access to the Internet for all USDA agencies. The USDA UTN keeps each Agency's data logically separated.

The FSIS UTN relies on three access points (also known as the OCIO backbone) to connect to the USDA UTN and the Internet. They are:

- the FSIS Beltsville Stack, located in Beltsville, MD.
- the FSIS Ft. Collins Stack, located in Fort Collins, CO;
- the FSIS Headquarters Stack, located in Washington, DC; and

Some traffic comes into the FSIS UTN Headquarters Stack directly from the Internet (not via the USDA UTN). In these cases, secure VPNs are established using Advanced Encryption Standard (AES). The categories of traffic that enter the FSIS UTN this way are:

- individual user client machines (remote VPN);
- Very Small Aperture Terminal (VSAT) Users; and
- site-to-site connections.

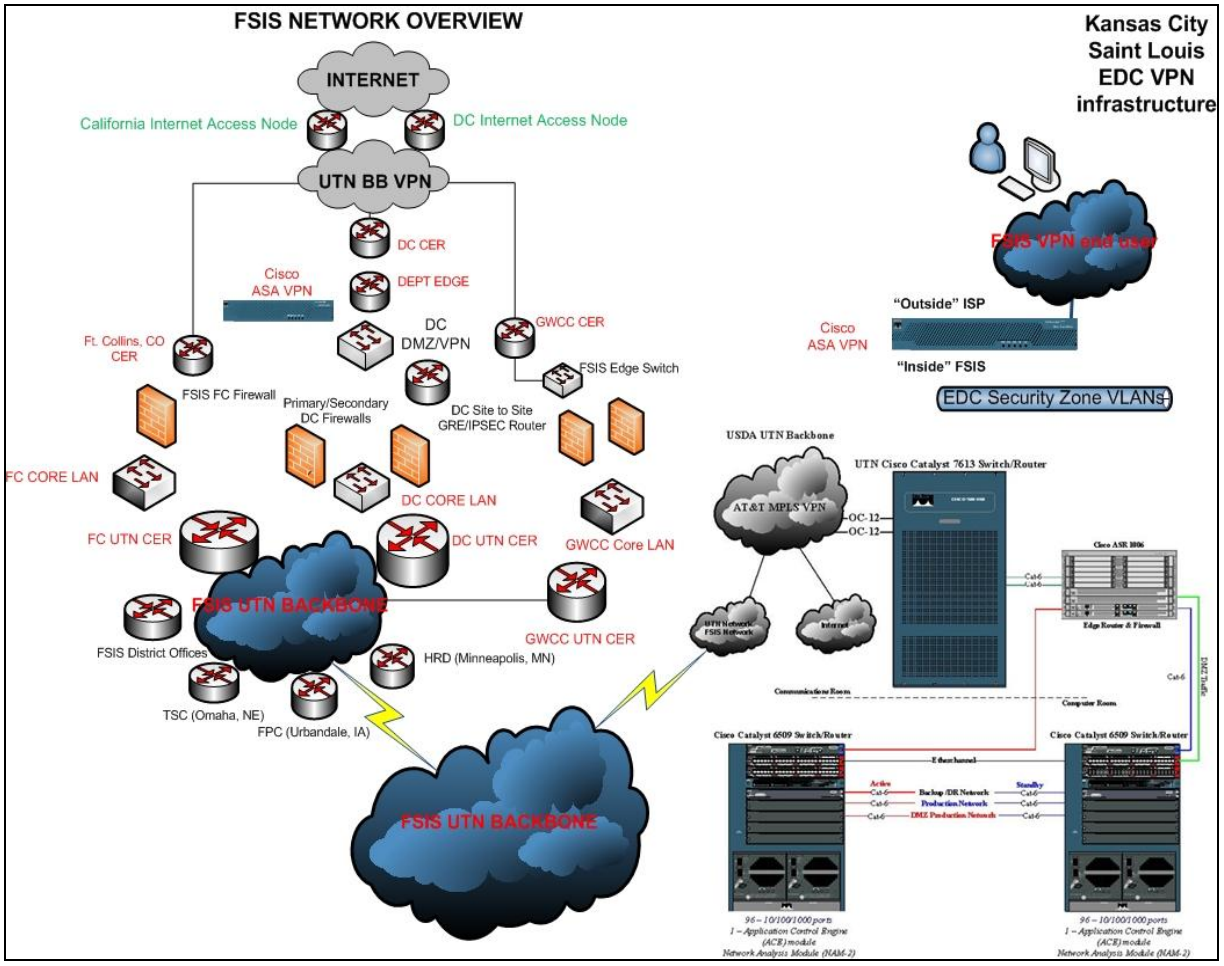
All individual and VSAT users come into the FSIS network via Cisco VPN connections. The site-to-site connections are currently using either Cisco or Juniper VPN connections.

Other remote locations needing to access the FSIS UTN use a variety of different communication technologies, including dial-up. In an effort to eliminate dial-up service, FSIS has undergone a transition to convert as many sites as possible to broadband. As part of the

transition, AT&T is providing (unencrypted) VPN using Multi-protocol Label Switching (MPLS[1]) to district offices, labs, and various other core offices.

Processing Flow

System diagrams illustrating data flow and component interconnections are provided below:



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] Multi-protocol Label Switching (MPLS) gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.

1.1 What information is collected, used, disseminated, or maintained in the system?

The N-GSS system collects the following information for Network Administrators (federal employees and contractors that provide operations and maintenance support): First Name and Last Name.

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

Network Adminstrator accounts. The Active Directory user accounts that are maintained in the Enterprise GSS are a source of information used, but not maintained, by the N-GSS.

The Network Administrators have to obtain administrator accounts in order to access the actual network components (e.g., routers and switches). First and Last Names are also provided for these accounts, which are maintained by the FSIS Network.

Like all users of the FSIS environment (FSIS employees and contractors), Network Administrators must have an FSIS Active Directory user account. When an individual applies for an FSIS Active Directory account, their First and Last Name are provided as part of the request. Though the FSIS Active Directory information is maintained by the FSIS Enterprise GSS, the FSIS Network ensures that the Active Directory information provided is accurate before permitting a user to establish a network session.

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

First Name and Last Name are used for authenticating the user to the N-GSS VPN and authenticating Network Administrators to network devices and network management tools.

1.4 How is the information collected?

All users of the FSIS environment (FSIS employees and contractors) must have an FSIS Active Directory user account. When an individual applies for an FSIS Active Directory account, their First and Last Name are provided as part of the request. When a Network Administrator applies for a privileged administrator account, the information is provided in the request.

1.5 How will the information be checked for accuracy?

The employee's First and Last Name are vetted at the time an employee is hired. The Employee Number from Active Directory is generated at the time the employee's FSIS Active Directory user account is created. If an employee's information is incorrect, they will not be able to access the FSIS Network.

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 mandates federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful/unauthorized use.

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

The risk is that Network Administrator's (federal employee and contractors) First and Last Names are collected and stored in the N-GSS system.

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

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology and Network Administrators must comply with the Agency's Privileged User Rules of Behavior. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. Active Directory and AIIS role-based security is used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory.

When anyone is granted access to the FSIS environment, they are issued a USDA email account and an FSIS user account. In addition, they may have to obtain a USDA eAuthentication account (e.g., to access a specific FSIS application). By having these accounts, the user's network login credentials are checked against authorized system user role membership, and access privileges are restricted accordingly. FSIS system users must pass a Government NACI (National Agency Check with Inquiries) background check prior to

having system access. Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

All attempts to login to the FSIS network are logged and the FSI Security Operations Center uses the information to monitor access to the network and tracks the top 10 users with the most failed attempts. In addition, all Network Administrator activity is logged.

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.

First Name and Last Name are used for authenticating the user to the N-GSS VPN and authenticating Network Administrators to network devices and network management tools.

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

The FSIS Security Operations Center (SOC) uses numerous tools to monitor the health of and access to the FSIS Network on continuous real-time (24x7) basis. These tools include, but are not limited to, ArcSight, Bluecoat, Event Tracker, SourceFire, and Symantec Endpoint Protection. These tools provide information about attempts to logon to the network, failed logon attempts, most popular website, known malicious websites, intrusion detection information, equipment problems, the distribution of anti-virus data, etc.

The FSIS Data Center Operations Branch (DCOB) team (i.e., Network Administrators) utilizes the Cisco Secure ACS View interface and CiscoWorks. Via this interface, the DCOB team can run reports to review Network Administrator activity. The Cisco Secure ACS View interface provides numerous canned reports that show log on activity, account creation events, changes to the network devices, etc.

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

The SOC monitors the health of and activity on the FSIS Network. As part of the monitoring effort, the SOC tools displays names of Web Sites to show the most frequently visited sites. The SOC monitoring tools also display the names of known malicious Web Sites to which FSIS is actively blocking access.

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.

See Section 1.7 above for a description of the controls that have been put in place for the FSIS Network.

The risk is that Network Administrator's (federal employee and contractors) First and Last Names are collected and stored in the N-GSS system.

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?

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for five (5) years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request.

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.

The risk is that Network Administrator's (federal employee and contractors) First and Last Names are collected and stored in the N-GSS system. As long as they are maintained, there is a risk that the information could be exposed to unauthorized individuals. The length of time data is retained does not change the level or type of risk associated with retaining the data. Therefore, the same methods to reduce risk are used throughout the life of the data.

See Section 1.7 above for a description of the controls that have been put in place for the FSIS Network.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the USDA.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Per the PTA, N-GSS confirms that users attempting to logon to the network do have an FSIS authorized Active Directory account (which is maintained by the FSIS Enterprise GSS). Otherwise, the N-GSS does not share information with other organizations.

4.2 How is the information transmitted or disclosed?

The handshake to confirm that someone is using an authorized FSIS account is encrypted over an access controlled network, so there is little privacy risk.

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 Network Administrator First Name and Last Names information is not shared with any internal organizations and it is maintained on access controlled tools, so there is little privacy risk.

The general user FSIS Active Directory account information is not maintained by the N-GSS. The handshake to confirm that someone is using an authorized account is encrypted over an access controlled network, so there is little privacy risk.

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?

Generally, the N-GSS information is not shared with external organizations.

If necessary, information may be disclosed to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for

records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.

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.

Under normal circumstances, the N-GSS does not share PII outside the department. However, routine use for disclosure to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.

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

Should N-GSSS information need to be shared with NARA, Congress, or Department of Justice, standard FSIS guidelines for providing information to such organizations will be followed.

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

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

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

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

Yes. Employee name information is collected at the point of hiring.

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information.

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

Yes.

However, the information is required in order to be hired.

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.

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information.

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?

The employee's name is important to the correct authentication of FSIS employees when they attempt to logon to FSIS equipment. If an employee's name is not correct, they will not be able to login to an FSIS laptop or the N-GSS application. Furthermore, if their name is not correct, that will affect payroll and other functions. If an employee's information is not being processed correctly, they would work with Human Resources to ensure that the information is correct.

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

The employee would contact Human Resources and follow the standard HR procedures for addressing incorrect employee information.

In addition, users can contact the FSIS Service Desk at 1-(800) 473-9135.

If a Network Administrator's name is incorrect in his or her Network Administrator account, the Network Administrator would bring to the attention of N-GSS management to have the information corrected.

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

New employees are provided with such information at the time they are hired.

In addition, users can contact the FSIS Service Desk at 1-(800) 473-9135.

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.

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

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

To gain access to the N-GSSS system, a general user must have 1) an account on the FSIS Active Directory, 2) an FSIS issued laptop, and 3) they must be working from an FSIS authorized IP address. Network Administrators must also have a privileged network account in order to access actual network devices (e.g., routers and switches).

Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. 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.

8.2 Will Department contractors have access to the system?

Yes.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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

Annual, recurring security trainings practiced and conducted through the Office of the Chief Information Officer. Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect of incomplete data as recorded in the system. Contractors who may be authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. An access agreement describes prohibited activities (such as browsing) by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access.

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

Yes, the ATO was granted on 23 April 2010.

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

Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department, and agency policies and procedures are safeguards implemented to mitigate the risks to any information technology.

The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The risk is that Network Administrator's (federal employee and contractors) First and Last Names are collected and stored in the N-GSS system.

See Section 1.7 above for a description of the controls that have been put in place for the FSIS Network.

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?

N-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, the ISSPM team has reviewed both documents.

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.

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?

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 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

Miguel Rivera – Chief Technical 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
Food Safety and Inspection Service
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: _____ 10 July 2012
Miguel Rivera — Date
Chief Technical Officer (CTO) / System Owner

Agreed: _____ 6-28-12
Alicemary Leach — Date
Privacy Officer

Agreed: _____ 7/23/12
Elamin Osman — Date
Chief Information Security Officer (CISO)

Agreed: _____ 7/30/12
Janet Stevens — Date
Chief Information Officer