Privacy Impact Assessment
APHIS Enterprise Infrastructure General Support System (AEI GSS)

- Version: 1.9
- Date: July 10, 2018
- Prepared for: USDA OCIO TPA&E

Technology, Planning, Architecture, & E-Government

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Animal and Plant Health Inspection Service Enterprise Infrastructure General Support System (AEI GSS). The AEI GSS provides the connectivity platform for APHIS which is charged with protecting U.S. agriculture, regulating genetically engineered organisms, administering the Animal Welfare Act and carrying out wildlife damage management activities. This PIA was conducted because the AEI GSS has the potential to store personally identifiable information within the file servers.

Overview

APHIS is charged with protecting U.S. agriculture, regulating genetically engineered organisms, administering the Animal Welfare Act and carrying out wildlife damage management activities. These efforts support the overall mission to protect and promote food, agriculture and natural resources. The purpose of the AEI GSS to provide complete IT support services to employees and contractors working to fulfill the mission of inspecting and protecting animal and plant materials within the United States.

In all computing facilities, the AEI GSS utilizes the USDA NET for Wide Area Network (WAN) connection to the rest of USDA. The GSS is comprised of major components providing a multitude of services to APHIS employees; including Blackberry, wireless, VoIP, trouble ticket system, border protection devices and other critical centralized services. In order to provide the technical backbone to host these major components the AEI GSS utilizes multiple components, both hardware and software, located at its 3 hosting facilities. These major components include products from CISCO, Microsoft, HP, Dell, Oracle, IBM and many others. The AEI GSS includes all firewalls, routers, switches, storage devices, and servers (this includes file and print servers). This includes the desktops and laptops that attach to the LANS within each computing center. For a complete list of components in the GSS, please see the narratives in the SSP.

1 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 AEI potentially stores data used and processed by a number of desktop applications based on user preference and saved on the file/printer servers. The boundary of the data

stored is the responsibility of the application/investment including the SORNs and privacy impacts. The AEI maintains the data and is responsible for the security of the stored data.

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

The source of the information on AEI file servers containing data that users have extracted from other major applications for which a PTA/PIA has been written. In addition, the AEI stored information is for the USDA APHIS employees/contractors for support of the mission of the agency.

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

For the mission work of APHIS to include internal and external sources. Contractor numbers, employee name, home telephone numbers. May also include the potential for users to store documents on file servers with data that they extract from other applications.

1.4 How is the information collected?

The information is obtained through the course of fulfilling the mission of the agency.

1.5 How will the information be checked for accuracy?

The data is checked for accuracy by the APHIS employees collecting the information. The AEI GSS maintains information through the file servers and applications maintained on the system. Each application system owner is responsible for documenting the data about their system within their own boundary documents. The AEI GSS maintains the security of the file and application servers. The AEI does not collect information instead it maintains the information needed to support the mission of the agency.

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

The legal authorities defined in the collection of information include but not limited to: Animal Welfare Act; Plant Protection Act; Animal Protection Act; and Virus Serum Toxin Act.

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

It has been found that some privacy data has been saved on the infrastructure unprotected. The agency has since implemented encryption and currently has a scanning tool in place to quarantine unprotected data.

There is a possible risk that data could be out of date and stored on the infrastructure beyond the data retention at this time the network is being scanned and the Records Management Liaison will work to ensure that the data is still current and needed.

2 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 information is used to carry out the mission of the agency.

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

Not Applicable

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

Not Applicable

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.

The AEI does not collect however; it is the platform used to save data. The infrastructure has implemented technical controls to secure the data stored locally for the support of the mission of APHIS.

3 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?

Items are retained per the General Records Schedule 24: Information Technology Operations and Management Records, records are destroyed based on the subject matter. The data is retained as per specified for system backup and tape libraries. Data is backed up as a monthly full backup, with daily incremental backups, and then superseded by the next full backup. Data is retained for 3 years.

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

Each of the program offices that collect data will schedule the records as required.

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 have been no risk identified.

4 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?

This is based on the programs use of the data and this would be documented in the appropriate PIA and/SORN.

4.2 How is the information transmitted or disclosed?

This is based on the programs use of the data and this would be documented in the appropriate PIA and/or SORN.

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.

Not applicable

5 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?

This is based on the programs use of the data and this would be documented in the appropriate PIA and/or SORN.

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.

Not applicable. Each program will create and publish a SORN for the data they are responsible for.

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

This is based on the programs use of the data and this would be documented in the appropriate PIA and/or SORN.

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

Not Applicable

6 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?

No PII is collect by the AEI. The infrastructure stores the information collected by the programs. Notice is the responsibility of the programs.

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

N/A

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

Not Applicable

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.

There is no risk identified with individuals not being unaware of the collection of data.

7 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 procedures to allow individuals to gain access to their information is documented in the appropriate PIA and or SORN. That is the responsibility of the programs.

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

Procedures are established within the programs.

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

The information is provided in the appropriate PIA and/or SORN. This is the responsibility of the programs.

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

Not Applicable

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 identified risks associated with the redress.

8 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?

APHIS implements a Rules of Behavior (ROB) for which all AEI GSS users must consent prior to being granted system credentials for access. The AEI GSS inherits the USDA implementation of User Security Awareness training which is provided annually by the Department. APHIS has created access control lists (ACLs) on network shares that

determine who within APHIS can access a specific share. Authorization for access to these secured shares must be obtained before a user is granted access.

8.2 Will Department contractors have access to the system?

Yes

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

The Department's IT Security Awareness Training Program is provided on an annual base and is mandatory for all APHIS employees. All users are required to sign a ROB that addresses privacy related responsibilities.

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

Yes, the AEI GSS currently operates under an ATO granted August 11, 2015. In addition, AEI GSS is currently undergoing continuous monitoring, with the next security authorization due in August 11, 2018.

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

All users are required to have an individual user account to access the AEI GSS. Firewalls and intrusion detection systems prevent unscrupulous parties from accessing the AEI GSS.

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?

Not Applicable

9 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 system is a General Support System (GSS).

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

No, the AEI GSS does not employ technology which may raise privacy concerns.

10 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

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

Not Applicable

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

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

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

Not Applicable

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

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

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

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