Privacy Impact Assessment
National Bio and Agro-Defense Facility (NBAF) Laboratory System (NLS)

Policy, E-Government and Fair Information Practices

- Version: 3.0
- Date: April 14, 2022
- Prepared for: Marketing and Regulatory Programs

United States Department of Agriculture

Privacy Impact Assessment for the

NBAF Laboratory System

Contact Point

Eric Fong
Information Systems Security Manager
APHIS/NBAF

Reviewing Official

Angela Cole
Chief Privacy Officer - APHIS
United States Department of Agriculture

Tonya Woods
Privacy Act Director
United States Department of Agriculture

Dr Elizabeth A. Lautner
System Owner
United States Department of Agriculture

Abstract

This Privacy Impact Assessment (PIA) is for the USDA, Animal and Plant Health Inspection Service (APHIS), Veterinary Services (VS), National Bio-Agro Defense Facility (NBAF) Laboratory System (NLS). NLS is a collection of virtualized Windows Application/ Database servers operating in APHIS platform. The servers provide mission specific stack of commercial off the shelf software (COTS).

This PIA was conducted because the NBAF NLS has the potential to store personally identifiable information within the file servers that contains access control.

Overview

The primary mission of the NBAF is the protection of animal health for the livestock industry in the United States. Capabilities for the NBAF include laboratories designed, constructed, and equipped for Biosafety. The NBAF NLS aims to provide automation support to employees and contractors working to fulfill the mission of inspecting and protecting animal and plant materials within the United States.

NLS consists of the following subsystems:

- Asset Management System software is an asset maintenance management program staff use to collect information about warehouse inventory. No PII is contained in this software.
- Laboratory Wireless Communication System (LWCS) enables scientists and staff to communicate hands-free and provides a secure, scalable, and integrated communication platform. LWCS consists of two key components: the software controlling and managing call activity and the communication badges. Together, they allow users to communicate with others inside and outside the laboratory instantly. The LWCS maintains information regarding the communication devices, groups, user assignments, and usage information. The badge is a small, wearable device that provides a voice-controlled user interface to the LWCS. The badge contains a speaker, microphone, wireless radio, and high contrast display showing caller ID, text messages, and alerts. Staff name and phone contact information are stored in a badge in a call tree that knows which number, and which order the staff members or service should be notified.
- Temperature Monitoring System (TMS) is a temperature monitoring system NBAF used to collect information about laboratory equipment. No PII is contained in this software.

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 laboratory wireless communication system maintains user contact information such as username, caller ID, text messages, and alerts. NBAF 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?

NBAF and USDA employees make up the PII data captured, stored, and processed in the analytic server.

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

The information is being collected for the purpose of storage, audit, and retrieval of business needs.

Laboratory wireless communication system may collect employees' PII, which is strictly maintained for audit purposes, retrieval of devices, and storage.

• System summary —Snapshots of system call volume and speech recognition rates.
• Call logs—Information about calls made and received by users, groups, etc.
• Recognition—Pinpoints equipment or users experiencing speech recognition problems.
• Device management —Reports based on the device management feature that includes new device attributes such as label, owner, and device status.
• Audit —Creates an audit trail of the changes.
• Badge asset tracking —Provides tracking of device.

1.4 How is the information collected?

Pertinent PII data may be collected from laboratory wireless communication systems such as username, caller ID, text messages, and alert stored in the analytic server.

1.5 How will the information be checked for accuracy?

Laboratory wireless communication system collects data associated with employees that use the system. The administrator has full access to the user’s profile. The users

can verify and update the data through the administrator to ensure data remains current and accurate.

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

- Executive orders 10450, 10577, 12968, 12968; 5 CFR Parts 5, 731, 732, 736
- Public Health Security and Bioterrorism Preparedness and Response Act of 2002
- The Homeland Security Presidential Directive 7 and 9

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

Privacy risks are the loss of Vocera usage information such as the name of the individual regarding the badge information such as group, user assignment, and usage information.

Mitigations to minimize privacy risks are:

- Access is limited to NBAF, USDA employees, access is approved by supervisor and to be reviewed periodically
- Only Administrators can add, modify, remove users
- Practice of least privilege and separation of duty; access rights to only for the duty assigned
- Encryption for data at rest and during transition
- Screen Timeout
- Software enabled Audits
- Limits on PII visibility
- No public access to NLS

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 collected will be strictly used for the NBAF facility wireless communication system. The use of data includes the individual identifiers or user profile, caller ID, and alerts and is not shared outside of NBAF.

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

The server and the associated report console interface provide administrators, managers, and decision makers the ability to monitor system performance and generate reports for analysis.

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

NA.

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.

NLS follows all required security controls deemed applicable by NIST-800-53 Rev. 5

Type of controls include:

- Access to the data in the system is controlled and documented by formal authorization
- All access to the system is limited by account identification and password
- Users have formal training in how to use the system
- Users have formal training on how to properly manage PII
- A warning banner must be acknowledged at login
- Only authorized users have access to the data
- Practice of least privilege and separation of duty; access rights to only for the duty assigned
- Encryption for data at rest and during transmission

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?

All information systems are retained in accordance with Information Systems Security General Records schedule - 3.1 and 3.2.
https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf
https://www.archives.gov/files/records-mgmt/grs/grs03-1.pdf

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

All component records are using general record schedules. Refer to 3.1.

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

Retention of application-specific data is required to meet business and organizational requirements for this information system. The risks associated with retaining application-specific information are mitigated by the controls in Section 2.1 discussed above.

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?

Information is not shared outside of NBAF.

4.2 How is the information transmitted or disclosed?

Not applicable.

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.

Information is not shared outside of NBAF.

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 transmitted or disclosed to organizations external to the USDA.

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.

PII Information is not shared outside of NBAF except in the event of investigative and enforcement from outside agencies that requires records regarding regulatory activities in USDA-APHIS-1: Investigative and Enforcement Records Regarding Regulatory Activities, USDA/APHIS
See SORN: https://www.federalregister.gov/documents/2001/11/16/01-28727/privacy-act-of-1974-as-amended-systems-of-records

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

NBAF does not share with external organizations except those required by law or routine uses under the Privacy Act. Encryption will be applied to the transmission through VPN or media encryption to safeguard its transmission.

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

USDA/APHIS/NBAF provide safeguards against invasions of privacy by limiting the collection of personal data to authorized personnel only. The data collection must be relevant for the purposes for which it is collected and shall not be used for any other purpose. External sharing is restricted to federal law enforcement agencies.

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

Yes, APHIS- 1 Investigative and Enforcement Records Regarding Regulatory Activities, USDA/APHIS.

https://www.federalregister.gov/documents/2001/11/16/01-28727/privacy-act-of-1974-as-amended-systems-of-records

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

Yes, prior to logging into laboratory wireless communication system, the administrator has to acknowledge a privacy and security notice.

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

No.

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

No. The information is used for internal purposes only. All information is required to track incoming and outgoing visitors in NBAF faculty. All PII information is collected and to be used with NBAF internal use only. Individuals can decline to provide their data into visitor management system, however their access to NBAF may be declined.

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.

Individuals are notified about their information processing during the initial system registration process. System users have appropriate training and Rules of Behavior to access the visitor management system. These measures have been implemented to prevent individuals from being unaware of the collection and processing of information. Failure to agree to the registration process may deny the individual access to NBAF.

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 requesting information under the Privacy Act must follow the procedures set forth in the regulations of the U.S. Department of Agriculture published in 7 CFR Part 1, subpart G.

All requests for access to records must be in writing and should be submitted to the APHIS Privacy Act Officer, 4700 River Road, Unit 50, Riverdale, MD 20737; or by facsimile (301) 734–5941; or by email APHISPrivacy@usda.gov. In accordance with 7 CFR 1.112 (Procedures for requests pertaining to individual records in a record system), the request must include the full name of the individual making the request; the name of the system of records; and preference of inspection, in person or by mail. In accordance with 7 CFR 1.113, prior to inspection of the records, the requester shall present sufficient identification (e.g., driver's license, employee identification card) to establish that the requester is the individual to whom the records pertain. In addition, if an individual submitting a request for access wishes to be supplied with copies of the records by mail, the requester must include with his or her request sufficient data for the agency to verify the requester's identity. Personnel who wish to view the data used to grant their facility access should contact the NBAF IT directly

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

Personnel who wish to correct the inaccurate or erroneous should contact the NBAF Security office directly or email NBAFSecurity@usda.gov or by following the procedures identified in Section 7.1.

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

Individuals are notified at the point of collection of information, through this PIA and applicable SORNs identified in Section 6.2.

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

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.

The primary risk associated with the redress process include unintentional release of proof of identification information required to access records. Any PII collected to prove identity will be sent through secured and

encrypted communication. The information will be destroyed once the identification has been confirmed.

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?

User access is initiated by an USDA NBAF employee's supervisor request, is approved by the system owner, and is recorded in the automated system UMS that resembles APHIS form 513. System owners can approve, add, remove, and terminate roles.

8.2 Will Department contractors have access to the system?

Contractors who are hired to work on-site at NBAF will be granted access commensurate with their roles and responsibilities.

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

APHIS requires all system users to complete annual Information Security Awareness Training. The records are stored electronically for verification purposes. If an individual does not take training, he/she will lose access.
.

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

Yes. A&A is valid from 6/3/2021 – 6/3/2024.

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

System security logs and system event logs from all facility security and badging systems will be reviewed on the systems that generate them by trained facility and system security staff. Archived log files will be protected by data at rest and encrypted for long term storage with limited system access.

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?

Risk: Unauthorized disclosure of PII

Mitigations:

- Least Privilege: Data can be retrieved only by personnel with authorized badge and who have logged in with their e-Authentication PIV or eAuthentication username/password credential role.
- Separation of Duties/Only authorized personnel have access: System owner can approve and denied access with periodic review.
- Audit Trail: All system access, badge request, have chain of custody form are used for audits.
- Training: PII training is mandatory for all users, as well as periodic review of SOP from the security personnel that are handling the data.

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 visitor management system operates under a moderate categorization per FIPS 199. The system is to support NBAF efforts for visitor tracking to comply with HSPD-12 regulations while meeting requirements defined by FIPS 201-1 and PIV compliance.

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

No. NLS uses USDA-approved technologies and these technology choices do not raise privacy concerns.

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?

No 3rd party web sites are used.

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?

No.

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

ELIZABETH LAUTNER
Digitally signed by ELIZABETH LAUTNER
Date: 2022.04.17 20:43:01 -05'00'

Dr Elizabeth A. Lautner
System Owner
United States Department of Agriculture

JANELLE JORDAN
Digitally signed by JANELLE JORDAN
Date: 2022.04.20 10:07:47 -04'00'

Tonya G. Woods
APHIS Privacy Act Officer
Animal and Plant Health Inspection Service
United States Department of Agriculture

ANGELA COLE
Digitally signed by ANGELA COLE
Date: 2022.04.29 11:34:49 -04'00'

Angela Cole
Chief Privacy Officer/Deputy Assistant Chief Information Security Officer
Marketing and Regulatory Programs
United States Department of Agriculture