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

Policy, E-Government and Fair Information Practices

- Version: 5.0
- Date: April 8, 2021
- Prepared for: USDA OCIO-Policy and Directives - Privacy Office

United States Department of Agriculture

Privacy Impact Assessment for the

NBAF Laboratory System

8 April 2021

Contact Point

Eric Fong
Information Systems Security Manager
APHIS/NBAF
(785) 477-3496

Reviewing Official

Tonya Woods
Privacy Act Director
United States Department of Agriculture
(301) 851-4072

Dr. Kenneth Burton
NBAF Coordinator
United States Department of Agriculture
(785) 477-3200

1.1

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 system stores Personally Identifiable Information (PII) within the file servers that contains access control.

Overview

The primary mission of the NBAF is the protection of animal health for the United States livestock industry. Capabilities for the NBAF include laboratories designed, constructed, and equipped for Biosafety. The purpose of the NBAF NLS is 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. With an active USDA user account, USDA employees are then assigned role-based access that has been approved by the supervisor and mission capability owner.

NLS consists of the following subsystems:

- Asset Management System
- Visitor Management System

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 NBAF stores data used and processed by 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 including the SORNs and privacy impacts. The NBAF NLS maintains the data and is responsible for the security of the stored data. The NBAF NLS may potentially contain generate or store PII information on individuals to include:

☒ Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias).

☒ Date and/or place of birth.

☒ Address Information (street or email address).

☒ Personal identification number (e.g. social security number, tax identification number, passport number, driver's license number or a unique identification number, etc)

☐ Financial data (credit card numbers, bank account numbers, etc.).

☐ Health data (including height, weight, blood pressure, etc.).

☒ Biometric data (fingerprints, iris scans, voice signature, facial geometry, DNA, etc.).

☒ Criminal history.

☒ Employment history.

☒ Miscellaneous identification numbers (agency assigned number, case number, accounts, permits, etc.).

☒ Photographic image/identifying characteristics.

☒ Handwriting or an image of the signature.

☒ Other information that may be seen as personal (personal characteristics, etc.).

Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

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

NBAF and USDA employees will make up the bulk of the PII data captured, stored, and processed in the facility security system. Visitors to the facility from other USDA locations as well as partner institutions and other government agencies may be require to provide PII in order to enter the facility.

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

Visitor management system may contain PII that are collected, used, and processed for facility access and internal security purposes only.

1.4 How is the information collected?

Pertinent PII data may be collected from facility visitors for the purpose of access control. Visitor information is collected by trained security personnel and maintained by NBAF physical security and IT administrators. Visitor management software tracks and manages visitors entering and leaving the facility and provide visitor sign-in process and can notify the security that the visitor has arrived or departed.

1.5 How will the information be checked for accuracy?

NBAF physical security verifies the visitor with valid photo IDs and/or government issued documents such as government issued passports, passport cards, driver's licenses and other officially issued documents. The visitor information is collected and inputted in visitor management system for security use.

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

HSPD 12 (Policies for a common Identification Standard for Federal Employees and Contractors)
44 U.S.C. 3507 - Public information collection activities; submission to Director; approval and delegation

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

Mitigations to minimize privacy risks with all NLS connected workstations and servers are:

- Access is limited to NBAF, USDA employees, access is approved by supervisor and to be reviewed periodically
- 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 used to positively identify personnel and visitors entering and operating within the NBAF facility. The provided data may also be used to grant access to access areas within the facility. All PII data will be contained within the facility.

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

NBAF NLS uses Trusted Visitor application to capture, store, and process incoming and outgoing visitors and their whereabout throughout the facility. Visitor management software stores information who visited the NBAF facility.

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

The system in NLS is designed for internal use only.

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. 4

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 transition

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?

Data inputs include electronic files or hardcopy (non-electronic) documents to create, update, or modify master files. Electronic files encompass word processing files, pdf, pictures, spreadsheets, video files, or any type of digital media files. Information will be destroyed 3 years after system is closed, but longer retention is authorized if required for business use.

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

USDA Veterinary Service (VS) has a target date of 6/1/21 to begin the scheduling process for NLS. Once VS consolidates all system information requests in the mission area then MRP400 can be filed to ensure this is captured in National Archives and Records Administration (NARA).

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

To mitigate the risks, NBAF has developed chain of custody policies and SOP to control and document security and handling of NLS information transfer and disposition processes. The objective of chain of custody/SOP is to ensure that risk can mitigated. The chain of custody procedure mitigates the risk of non-authorized personnel having access and provide a timeline. Chain of custody information includes the material transferred, shipper and addressee, time/date/signature of each person relinquishing custody, and each person taking custody throughout the transfer/transport, storage, and use.

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 transmitted within USDA APHIS and ARS for security use only.

4.2 How is the information transmitted or disclosed?

The data is protected with encryption during transmission and at rest.

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?

External sharing is **only** restricted to federal law enforcement.

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.
See: Investigative and Enforcement Records Regarding Regulatory System of Records Notice https://www.ocio.usda.gov/sites/default/files/docs/2012/APHIS-1.txt

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.

External sharing is only restricted to federal law enforcement agencies. Mitigation such as encryption and certificate are used in email during external transmission. NBAF provides 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.

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.

NLS operates under the following 3 SORNs:

APHIS-1: Investigative and Enforcement Records Regarding Regulatory Activities (2012, USDA/APHIS)
https://www.ocio.usda.gov/sites/default/files/docs/2012/APHIS-1.txt

USDA/OCIO-2: System name: eAuthentication Services (March 7, 2017, 82 FR 8503).
https://www.federalregister.gov/documents/2017/01/26/2017-01767/privacy-act-of-1974-revised-system-of-records#page-8504 and

GSA/GOVT-7: System name: Personal Identity Verification Identity (Oct 23, 2015, 80 FR 64416).
https://www.federalregister.gov/documents/2015/10/23/2015-26940/privacy-act-of1974-notice-of-an-updated-system-of-records

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

Yes, all personnel will opt in to providing the necessary information in order to be granted access to the facility.

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?

Not applicable.

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 processing of their information during initial visitor registration process. System users have appropriate training and Rules of Behavior to access 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.

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

Individuals seeking to contest and/or amend records 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, §1.116 Request for correction or amendment to record.

Further procedures for correcting inaccurate information is found at USDA APHIS | Requesting Access to Privacy Act Records

USDA – Animal and Plant Health Inspection Service
Privacy Act Office
4700 River Road, Unit 50
Riverdale, MD 20737
Facsimile: 301-734-5941
Email: APHISPrivacy@usda.gov

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

Notice is through the applicable published Systems of Record Notice.

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

The requester can file a formal Privacy Act request for corrections to their record.

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 risk identified with this action.

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?

NBAF employees will be required to submit the necessary information to request and receive access within the facility commensurate with their roles and responsibilities. Facility access is dictated by NBAF management and the NBAF Security Office.

NBAF visitors will be granted an agreed upon level of access while adhering to all applicable policies and procedures relating to being escorted or observed at all times or as necessary.

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. Contractors who work external to NBAF will not have access to the data contained in the system as it will not be connected to external networks.

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

Users of the system(s) containing PII will be required to complete mandatory USDA annual training - Protecting Personally Identifiable (PII) Information course. Users who fail to complete the required training annually will have their access to the system suspended until they are in compliance with departmental and NBAF policies.

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

The Certification and Accreditation is in the progress with the projected completion in Spring 2021. This Privacy Impact Assessment will be used in support of the initial Authority to Operate (ATO) package.

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. System is air-gapped isolated to a protected network segment.

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?

Security control help to mitigations privacy risks:
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(s). Users must be authenticated and have role-based access to data which is limited to a need to know basis to the user’s business unit (generally state level access).

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.

Any privacy concerns are mitigated by: USDA multi-factor authentication, valid SSL certificate, SQL encryption, and VPN technology. Application is also reinforced with policy to limit on PII exposure and audit enabled for best practice.

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 and system owner have reviewed the OMB memorandums listed above.

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

PRESTON GRIFFIN

Digitally signed by PRESTON GRIFFIN
Date: 2021.04.30 15:34:55 -04'00'

Preston Griffin
MRP ISSPM
Marketing and Regulatory Programs
United States Department of Agriculture

JANELLE JORDAN

Digitally signed by JANELLE JORDAN
Date: 2021.04.08 21:12:06 -04'00'

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

KENNETH BURTON

Digitally signed by KENNETH BURTON
Date: 2021.04.09 16:27:53 -05'00'

Kenneth Burton
System Owner
APHIS/NBAF
United States Department of Agriculture