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

Policy, E-Government and Fair Information Practices

- Version: 2.0
- Date: March 17, 2022
- Prepared for: Marketing and Regulatory Programs

United States Department of Agriculture

Privacy Impact Assessment for the

Building Control System

Contact Point

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

Reviewing Officials

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 Faculty (NBAF). The USDA, Building Control System (NBAF BCS) provides building automation, security camera system and access control to the NBAF facility. The NBAF BCS is located at a new site in Manhattan, Kansas.

This PIA was conducted because the NBAF BCS 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 United States livestock industry. Capabilities for the NBAF include laboratories designed, constructed, and equipped for Biosafety. The purpose of the NBAF BCS 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.

The NBAF BCS Consists of the Building Automation System (BAS) and security 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 NBAF BCS maintains the data and is responsible for the security of the stored data. The NBAF BCS may potentially contain generate, or store PII information on individuals to include name, citizenship, country of origin, SSN, address, driver's license number or passport number, photographic image, handwriting/signature.

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 required to provide the name, citizenship, and country of origin to enter the facility. The source of information is the directly input from the visitor's sponsor to the NBAF security team through encrypted emails. Form Request used is NF-SEC-0036.2-NBAF Visitor Application.

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

Facility access and internal security purposes only.

1.4 How is the information collected?

Pertinent PII data is collected from employees and facility visitors on the NBAF Visitor Application and submitted via encrypted email to NBAF Security. This information is collected by trained security personnel and securely uploaded and maintained by NBAF Physical security visitor management system. All badge requests and approvals are reviewed by their supervisors and vetted through established security screening protocols.

1.5 How will the information be checked for accuracy?

NBAF physical security verifies valid photo IDs and/or government issued documents such as government issued passports, passport cards, driver's licenses and other officially issued documents. The data is checked for accuracy by the NBAF sponsor and security team collecting and inputting the information through visitor management system.

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

Homeland Security Presidential Directive 9 (HSPD-9).

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

To minimize privacy risks such as PII exposure is mitigated through PII training, and network isolation. BCS connected workstations and servers are isolated on an internal network with no access to the Internet or other external networks.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate 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 support the use of biometric systems that grant access to controlled 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?

For security purposes, the name of the tools are not disclosed.

We use our internal applications to capture, store, and process the collected PII data and to derive the digital elements necessary to be embedded into badge access cards and readers as well as biometric throughout the facility. Biometric terminals are located throughout NBAF and are used to access the critical areas of NBAF that will alert security for access. Unique digital signatures will be derived from the provided PII data in lieu of distributed storage of PII data across the various security control systems.

The access card/biometric system will record door open/close actions along with the name of the user and date/time of the event. Corresponding PII data may be used to positively identify authorized or unauthorized access in order to support necessary inquiries or investigations as necessary. NBAF systems only permits authorized and authenticated users. When an authorized user tries to connect to the network, they must have a USDA HSPD-12 PIV smart card and password to gain access to the systems.

To minimize privacy risks, all systems including the access card and biometric system is on isolated network with no access to the Internet or other external networks. BCS is an air-gapped network.

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.

BCS follows all required security controls deemed applicable by the latest version of NIST-800-53.

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

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. All data is retained based on APHIS and NARA standard.

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.

The current risk of storing data outside of the disposition can mitigated with

- Only authorized personnel have access
- Chain of custody form and audit logging
- Separation of duties
- Training/SOP of security personnel

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 except in the event of investigative and 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 APHIS-1: Investigative and Enforcement Records Regarding Regulatory Activities
Link: Federal Register :: 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 APHIS-1: Investigative and Enforcement Records Regarding Regulatory Activities 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.

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.

BCS operates under the following 3 SORNs:

APHIS-1: Investigative and Enforcement Records Regarding Regulatory Activities (2012, USDA/APHIS)
Federal Register:: Privacy Act of 1974, as Amended; Systems of Records
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

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?

Notice was provided to individuals by the initial source systems prior to collection or processing of the information.

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

No. If information is not provided, they will not be granted access into the facility.

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 grant facility access. If the user does not consent to use of all requested information, the facility access request will be disapproved. All PII information is collected and to be used with USDA NBAF.

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.

All data is provided by the user on the account request form which contains a consent notice.

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.

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. 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 annual training in the Aglearn platform and additional training provided by NBAF ISSM. 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?

Yes.

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?

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.
- Isolated: All systems are isolated to minimize the privacy risk.

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 National Bio and Agro-Defense Facility (NBAF) Building Control System (BCS) is application that is associated with the facility, physical security, and access control. The BCS is responsible to collect, manage, visitor data, video surveillance and facility controls.

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?

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 <u>Privacy Impact Analysis</u>: 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: 2022.04.12 22:20:08 -05'00'

Elizabeth A. Lautner
APHIS/NBAF System Owner
United States Department of Agriculture

Agency Approval Signature

JANELLE JORDAN
Digitally signed by JANELLE JORDAN
Date: 2022.04.11 12:45:55 -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: 2022.04.15 08:29:11 -04'00'

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