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

Policy, E-Government and Fair Information Practices

- Version: 1.7
- Date: December 28, 2020
- Prepared for: USDA OCIO-Policy and Directives - Privacy Office

United States Department of Agriculture

Privacy Impact Assessment for the

Building Control System

28 December 2020

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 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 boundary of the data stored is the responsibility of the application including the SORNs and privacy impacts. 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 (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.).

Photograph (For ID Badging)

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?

Physical security footage and internal badging 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 is collected from employees and facility visitors for the purpose of access control and badge access system. Employee information is collected by trained security personnel and maintained by NBAF Physical security and IT administrators. 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 employees collecting and inputting the information. The internal security application has data validation capability at time of input

that will enforce standards compliant inputs of data types and formats ensuring a high degree of accuracy.

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 all BCS connected workstations and servers are isolated on an internal network with no access to the Internet or other external networks.

NBAF staff uses APHIS Schedule or NARA Records Schedule based off the current MRP400 to insure what should be deleted is done per regulatory guidance.

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 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 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

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?

A	B	C	D	E	F
System Name	**Building Control System**				
INFORMATION TYPE	**CONTROLLING OFFICE**	**ITEM #**	**DISPOSITION**	**AUTHORITY**	**GRS #**
Full Motion Video Surveillance	Security	090	**Temporary.** Destroy when 30 days	DAA-GRS-2017-0006-0012	5.6 Security Records
Site and PIV Card Access	Security	020	**Temporary.** Destroy 3 years after r	DAA-GRS-2017-0006-0002	5.6 Security Records
Energy Consumption	Facilities	010	**Temporary.** Destroy 5 years after p	DAA-GRS-2013-0005-0006	3.1 General Technology Management Records
Building Automation	Facilities	010	**Temporary.** Destroy 5 years after p	DAA-GRS-2013-0005-0006	3.1 General Technology Management Records
Facility Operation	Facilities	010	**Temporary.** Destroy 5 years after p	DAA-GRS-2013-0005-0006	3.1 General Technology Management Records
Industrial Control System	Information Technolog	010	**Temporary.** Destroy 5 years after p	DAA-GRS-2013-0005-0006	3.1 General Technology Management Records
Facility System Proprietary Data	Information Technolog	010	**Temporary.** Destroy 5 years after p	DAA-GRS-2013-0005-0006	3.1 General Technology Management Records
Security System Proprietary Data	Information Technolog	010	**Temporary.** Destroy 5 years after p	DAA-GRS-2013-0005-0006	3.1 General Technology Management Records
System Architecture Records	Information Technolog	020	**Temporary.** Destroy 7 years after (	DAA-GRS-2017-0009-0002	6.2 Information Technology Records
System Access/Security Records (Low Securit	Information Technolog	030	**Temporary.** Destroy when busines	DAA-GRS-2013-0006-0003	3.2 Information Systems Security Records
System Access/Security Records (High Securi	Information Technolog	031	**Temporary.** Destroy 6 years after p	DAA-GRS-2013-0006-0004	3.2 Information Systems Security Records

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. **Electronic files are retained on the host device until one year after system closeout**. Disposition of paper are governed by local authority following disposition guidelines. Longer retention may require if it is authorized for legal or audit purposes. Informational content of the Master file may consist of footage, ICS data, scanned document, PDFs, digital images, or some other form of electronic information. They may include the information content of an entire system or that of a group of related files. Related records within a single master file are not always the same format. In case of an investigation, BCS Data (Proprietary services): Includes address, owner contact, resource and property management information Disposition: 30 years from when the investigation status is closed.

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

A MRP400 is in the progress of being 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 BCS 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 not transmitted or disclosed to organizations external to the USDA

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.
See 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.

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.

BCS 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?

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?

Personnel who wish to view the data used to grant their facility access should contact the NBAF Security office directly.

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

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

Submit your request by mail, facsimile, or e-mail.
USDA – Animal and Plant Health Inspection Service
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 annual training. 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 date of 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?

Mitigations:

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 users 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 National Bio and Agro-Defense Facility (NBAF) Building Control System (BCS) Animal and Plant Health Inspection Service (APHIS) complete control of the facility in terms of physical security and access control. The BCS is responsible for environmental controls as well as monitoring and control of laboratory environment and equipment necessary to operate the facility in a safe, controlled manner NBAF BCS is a strategically planned communications infrastructure operated and maintained to provide secure connectivity for information systems operated within NBAF.

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 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: 2021.01.07 10:58:33 -05'00'

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

JANELLE JORDAN

Digitally signed by JANELLE JORDAN
Date: 2020.12.28 12:25:07 -05'00'

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: 2020.12.30 13:50:57 -06'00'

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