

Privacy Impact Assessment

Performance Based Inspection System (PBIS)

- Version: 2.4
- Date: *September 18, 2012*
- Prepared for: FSIS OFO





Privacy Impact Assessment – PBIS

Document Revision and History			
Revision	Date	Author	Comments
2.4	09/18/2012	Kenneth Hopson	Annual Update

Abstract

This document serves as the Privacy Impact Assessment for the Performance-Based Inspection System (PBIS). The purpose of the system is to manage the inspection activities for meat, poultry, and processed egg products. This assessment is being conducted in accordance with the Privacy Threshold Analysis conducted in February 2012.

Work is underway to replace PBIS with the existing Public Health Information System (PHIS). Once replaced, PBIS will be completely decommissioned. The exact dates of the system transition and decommission have not yet been determined.

Overview

The United States Department of Agriculture (USDA) Food Safety and Inspection Service (FSIS) Performance-Based Inspection System (PBIS) is a software application that manages the meat and poultry inspection activities of the field workforce of the Food Safety and Inspection Service. The system covers the scheduling and recording of Hazard Analysis Critical Control Point (HACCP) inspection procedures. Using data entered by field inspectors and other district and state personnel, PBIS creates inspection schedules and maintains records of findings for reporting purposes.

When working with the PBIS database for their respective assignments, most of the work is performed offline, that is, when inspectors are not connected to the Consolidated Server. Working offline gives inspectors the ability to print schedules and enter feedback at the native speed of the local computer (as opposed to the limited speed of a dial-up connection), and offers the convenience of using the notebook computer at locations that lack dial-up connectivity.

Inspection personnel can see only their own assignment information. Likewise, inspection personnel in State Meat and Poultry Inspection programs can see only the data from their own assignments.

Because inspectors are entering inspection results while offline, they are required to synchronize their PBIS data on a regular basis. Synchronization takes a minimal amount of time—a few minutes at most—especially when performed on a daily basis, as intended. Every time an inspector performs the synchronization procedure, the latest PBIS data on that computer gets updated to the central server. If there are any changes on the Consolidated Server that affect that particular assignment, such as a new plant being added to the assignment, or a new schedule that was just built, these changes are replicated down to the local computer.

Type of storage: PBIS 5.0 utilizes Windows client/server technology to enable multiple users to access the PBIS national database. The PBIS national database resides on the Consolidated Server in the FSIS Enterprise Data Center (EDC), which is housed in the National Information Technology Center (NITC) located in Kansas City, MO. The server hardware is Intel-based and is upgraded as necessary (in speed and capacity) to accommodate the user base of approximately 2,000 inspector personnel that use PBIS.

Processing: The front-end application is written in Visual Basic Version 6.0 and controls the logic and workflow through the user screens, while the back-end database tables are written in Sybase Version ASA 6.04.3783.

Transmission: The remote users of the PBIS database currently dial up into the UUNET, which is a frame relay connection controlled by MCI. The PBIS system does not interconnect with any systems outside the control of the FSIS agency.

Processing Flow

PBIS software components are hosted in two environments. The centralized server components of PBIS are hosted in the FSIS EDC, which is housed in NITC located in Kansas City, MO. PBIS is therefore protected by the physical and environmental controls of the NITC facility.

Users of PBIS at the NITC location include office staffs (at Headquarters in Washington, D.C., FSIS District Offices throughout the country, and 27 State Inspection offices located in the capital cities of states with State Meat and Poultry Inspection programs). The majority of the PBIS users come from the Office of Field Operation (OFO) and the Office of International Affairs (OIA), which are part of FSIS.

The localized components of PBIS reside on individual computers used by the inspection workforce in the field. Computers hosting the PBIS application are protected by the security controls used by FSIS to protect all hardware/software. PBIS users are typically made up of a remote workforce that works in environments that have limited network connectivity access. Therefore, the bulk of their work is performed in a local database environment and then synchronized to the database hosted by the NITC facility mentioned above.

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?

In addition to extensive information regarding specific inspection activities, PBIS collects first and last names of FSIS employees, contractors, establishment owners or designated persons, and State users. PBIS also contains contact information of plant personnel who do not have access to PBIS. They are key establishment personnel (authorities) who operate the Plant. Information collected from these individuals includes their name, contact telephone number and title (which usually correlate to their area of authority).

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

The PBIS module contains profiles of operating plants, which includes types of work performed at the plant, as well as contact information for people who manage and operate the plant. This information was obtained from the establishments. In addition, the RIS (Resource Information System) module within PBIS is used to identify users of the system, as well as their roles and responsibilities.

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

PBIS collects this information as part of its business function of carrying out the required public health regulatory functions associated with inspection, including assigning adequate staffing and scheduling of inspections.

1.4 How is the information collected?

Names of employees and contractors are collected by office staff when requesting new accounts be created in the USDA FSIS domain. District/State offices send requests to RISHelp@fsis.usda.gov to add the employee into the system.

Establishment names and contact information are collected as part of the application for inspection service process, or, by personal knowledge of the inspectors in the establishments as individuals change.

1.5 How will the information be checked for accuracy?

The field computers are checked for database synchronization. Those workstations that have not synchronized within the last 21 days are flagged for either deletion or troubleshooting and are updated through the FSIS Service Desk.

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

US Code (USC) TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate.

The Federal Meat Inspection Act (21 USC 601), the Poultry Products Inspection Act (21 USC 451), and the Egg Products Inspection Act (21 USC 1031) also provide statutory authority for the activities performed in and by PBIS.

The November 18, 2008 amendment to the Executive Order 9397 mandates Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use.

44 U.S.C. 3101 states that each USDA mission area, agency, and staff office shall create and maintain proper and adequate documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the Department of Agriculture (Department) to protect the legal and financial rights of the Government and of persons directly affected by the Department's activities.

Also see: 5 U.S.C. Chapter 552, 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071, 44 U.S.C. 3101 et seq., 44 U.S.C. 3506, Title 7 CFR 2.37, 36 CFR Chapter 12, Subchapter B, 36 CFR Part 1234, eGovernment Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36), OMB Circular A-130, NARA - Disposition of Federal Records: A Records Management Handbook, NARA General Records Schedules.

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

As long as employee data identified in sections 1.1 and 1.2 is collected and retained, there is the risk that it may be disclosed to unauthorized individuals. PBIS contains three major user classes for controlling data:

- Transactional Inspection users (inspectors, front line supervisors (FLS), State/Federal Inspection office staffs using PBIS, eADRS, eSample and RIS to make changes to data)
- Transactional Sampling users (Federal Inspection Office and HQ Staffs using the STEPS component)
- Analytic/Reporting users of PBISReader and ADRSReader components

To mitigate any potential risks to privacy data unauthorized disclosure, PBIS provides multiple data protection mechanisms. FSIS system users must first pass a Government National Agency Check with Inquiries (NACI) background check prior to having system access.

In addition, the servers are maintained in access-controlled facilities and logical access to FSIS data is restricted to authorized personnel.

When anyone is granted access to the FSIS environment, they are issued a USDA email account and an FSIS user account (managed in Active Directory). To access PBIS, the user must first login to the FSIS network environment by using their Active Directory account to login to their FSIS issued equipment. Furthermore, to ensure that only those users who need data are given access; associations are made between users and field laptops to specific processing plants.

Furthermore, auditing is enabled by FSIS on PBIS operating systems to provide accountability for all personnel by tracking and monitoring system activity.

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.

PBIS manages the meat, poultry, and processed egg inspection activities of the field workforce of FSIS. The information in the system covers the scheduling and recording of HACCP inspection procedures. Using data entered by field inspectors and other district and state personnel, PBIS creates inspection schedules and maintains records of findings for reporting purposes.

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

PBIS contains a built-in process that produces various feedback reports such as: number of tasks performed, number of tasks not performed, results, and percent compliant. Ad Hoc reports can be developed through the read-only PBIS applications that have been created for this purpose by downloading the information into text files. Microsoft Access and/or Excel are used when the data is downloaded.

Additionally, data is migrated to a data warehouse, for analysis by Office of Data Integration and Food Protection and others, using tools such as ad-hoc web-based reports, Excel, and SAS to analyze the data.

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

The PBIS system does not use commercial or publicly available data.

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.

This is addressed more fully in Section 1.7 above. In addition, PBIS systems are continuously monitored by Security Operation Center (SOC) and by the Infrastructure Operations Division (IOD) Engineering Branch to ensure that information is handled in accordance with the above described uses in section 2.1.

In addition, annual Computer Security Awareness Training (CSAT) is conducted by the Office of the Chief Information Officer (OCIO). Users that do not take and pass this required annual training will have their access to the FSIS environment (network and applications) revoked.

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?

Hard copy records about inactive individuals, which often do not contain PII, are kept in a secure location indefinitely. System records are marked as inactive when an individual no longer needs to use the system or leaves the organization, and will be archived out of system according to NARA.

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

Yes

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

New establishment ownership may inadvertently lead to incorrect handling of past data collected, which can include PII information about individuals with inactive accounts.

However, this risk is mitigated by providing a history of changes, including establishment ownership changes in the data warehouse for reporting purposes. This history of changes allows for after-the-fact investigations if any PII data is ever mishandled.

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?

Data is shared with others in FSIS for performing analysis. In addition, the RIS application within PBIS feeds an employee roster during an overnight download directly to AssuranceNet, to allow AssuranceNet to perform In-Plant Performance System (IPPS) reviews.

Also, in preparation for the PBIS transition to PHIS, most FSIS inspection activities have already been incorporated into PHIS. There are a few exceptions due to ongoing

NJC negotiations regarding export inspectors and egg inspectors. Also, states are still using the PBIS system.

4.2 How is the information transmitted or disclosed?

The RIS employee roster information referenced in section 4.1 is transmitted on the FSIS network during an overnight download directly into an AssuranceNet listing.

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.

See Section 1.7 above. To minimize any risks, all FSIS systems are continuously monitored by the FSIS SOC and by IOD Engineering Branch to ensure that FSIS data is handled in accordance with the FSIS security policies.

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 that was provided by the state meat and poultry inspection program (MPI) is shared only with the state MPI program that provided it. Each state inspection program can see only their own data, just as each inspector can see only their own assignment data. Technically, data is shared externally, but it is shared only with the original source of the data.

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.

N/A – As information is shared only with the organization that provided it.

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

As noted in 5.1, the information that is provided to state MPI programs is data provided by them. Please see also the control points in Section 1.7 and 8.1.

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

As external sharing is not performed, other than with those organizations that provided the data originally, please see sections 5.1, 1.7, and 8.1.

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?

Notice is provided to FSIS employees. Because this system is being decommissioned, no changes to establishment actions regarding notification are being made at this time.

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

Yes, but having access to PBIS may be required for an employee to perform their job responsibilities. Employees and contractors that fail to agree to the agreement mentioned in section 6.1 are denied access to PBIS.

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

No.

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.

See Section 6.1. In addition, all users of the system must provide a first and last name in order to gain access to the system. As a result, there is no lack of awareness regarding the collection of this information and thus, no risk.

The same awareness exists in establishment personnel who, as part of performing their job functions, provide their names and, if needed, contact telephone numbers to inspection program personnel. There is no lack of awareness of the collection of this information and thus, no risk.

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?

No additional PII outside of a first and last name is required in order to gain access to PBIS, and no information other than first and last name and in some cases, contact telephone numbers are required of the limited number of establishment personnel whose names might be stored in the system.

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

Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 690-3882, Fax (202) 690-3023, Email: fsis.foia@usda.gov.

The FOIA requestor must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.

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

Before providing information, FSIS employees are presented with a Privacy Act Notice and an explanation of the Notice on both the Form 7234-1 and Form 8822-4. The individual's acknowledgement of the Privacy Act Notice and the proffer of information signify the individual's consent to the use of the information. The purpose, use, and authority for collection of information are described in the Privacy Act Notice.

Individuals are formally notified of the procedures for correcting their information. However, individuals seeking to contest their PII being collected may submit a request in writing to the Headquarters or component's FOIA officer, whose contact information can be found at <http://www.da.usda.gov/foia.htm> under "contacts".

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

N/A – Formal 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.

Corrections to PII data are securely maintained in the same manner as the original data. Therefore, there is no privacy risk associated with redress procedures available to individuals.

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?

PBIS Application Administrators provide access controls based on Standard Operating Procedure (SOP) documentation to authorized individuals so they may access the system based on pre-determined roles. PBIS also allows Assistant Office Administrators to further refine access control parameters based on a PBIS user's geographic location. PBIS administrators employ a "least privileges" policy to ensure users only have permission to carry out duties based on their specific role.

Listed below are seven PBIS application modules:

1. PBIS (Performance-Based Inspection System), used by inspectors/Front Line Supervisors (FLS) to enter inspection findings into a remote DB
2. eADRS (Electronic Animal Disposition Reporting System), used by inspectors/FLS to enter slaughter and disease totals into a remote DB
3. eSample, used by inspectors/FLS to enter in-plant residue test results into a remote DB
4. RIS (Resource Information System), used by office staff to profile work assignments and control access to the PBIS, eADRS, eSample and RIS software modules, uses a central DB
5. STEPS (System Tracking *E. coli* O157:H7 Positive Suppliers), used by office staff to document the sources of ground beef products found to have *E. coli*, uses a central database
6. PBISReader, used by any authenticated Agency user for web-based reporting of data in PBIS, eADRS, RIS and eSample. (no changes allowed – read only access)
7. ADRSReader, used by any authenticated Agency User for web-based reporting of data in eADRS (no changes allowed – read only access).

The access controls for PBIS can be broken into three major user classes:

- Transactional Inspection users (inspectors, FLS, State/Federal Inspection office staffs using PBIS, eADRS, eSample and RIS to make changes to data)
- Transactional Sampling users (Federal Inspection Office and HQ Staffs using the STEPS component)
- Analytic/Reporting users of PBISReader and ADRSReader components

8.2 Will Department contractors have access to the system?

Yes, USDA contractors are authorized to access PBIS, if needed and as it relates to their job function. Contractors authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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

All users are required to undergo Computer Security Awareness Training prior to accessing PBIS, as well as complete annual refresher training in order to retain access.

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

Yes, the ATO was granted on 18-July-2011.

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

The PBIS application team performs periodic reviews of the system to prevent misuse of data. In addition, the FSIS SOC and the IOD Engineering Branch provide continuous monitoring for all systems within FSIS to ensure that FSIS data is handled in accordance with the FSIS security policies. Applying security patches and hot-fixes, the previously mentioned continuous monitoring, checking the national vulnerability database, and following and implementing sound federal, state, local, department, and agency policies and procedures are safeguards implemented to mitigate the risks to any information technology.

The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts

identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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?

Risks to privacy are mitigated by granting access only to authorized persons and by those controls noted in Sections 1.7 and 8.1. Furthermore, employees of the Department of Agriculture have undergone a thorough background investigation. Access to facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. Access to computerized PBIS files are password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage, and helping to ensure the accuracy and integrity of the updates.

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?

PBIS is a Major Application.

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”?

N/A - Third party websites are not being used.

10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

10.4 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

10.7 Who will have access to PII that becomes available through the agency’s use of 3rd party websites and/or applications?

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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)?

N/A - Third party websites are not being used.

10.10 Does the system use web measurement and customization technology?

N/A.

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?

N/A.

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.

N/A - Third party websites are not being used.

Responsible Officials

Julie Henderson—System Owner, PBIS
Office of Field Operations
Food Safety and Inspection Service
United States Department of Agriculture

Alicemary Leach – Director, ECIMS
Office of Public Affairs and Consumer Education
Food Safety and Inspection Service
United States Department of Agriculture

Elamin Osman – Chief Information Security Officer
Office of the Chief Information Officer
Office of the Administrator
United States Department of Agriculture

Janet Stevens - Chief Information Officer
Office of the Chief Information Officer
Office of the Administrator
Food Safety and Inspection Service
United States Department of Agriculture



PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: *Julie Henderson* 9/27/12
Julie Henderson
System Owner Date

Agreed: *Elamin Osman* 9-28-12
Elamin Osman
Chief Information Security Officer (CISO) Date

Agreed: *Janet Stevens* 9/28/12
Janet Stevens
Chief Information Officer (CIO) Date

Agreed: *Alicemary Leach* 9/27/12
Alicemary Leach
Privacy Officer Date