



U.S. Department of Agriculture



Office of Inspector General
Financial & IT Operations

Audit Report

Food Safety and Inspection Service Application Controls – Performance Based Inspection System

Report No. 24501-1-FM
November 2004



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250



DATE: November 24, 2004

REPLY TO

ATTN OF: 24501-1-FM

SUBJECT: Food Safety and Inspection Service
Application Controls – Performance Based Inspection System

TO: Barbara J. Masters
Acting Administrator
Food Safety and Inspection Service

ATTN: Ronald F. Hicks
Assistant Administrator
Office of Program Evaluation, Enforcement, and Review

This report presents the results of our audit of application controls in the Food Safety and Inspection Service's Performance Based Inspection System (PBIS). The report identifies additional policies, procedures, and system changes needed to ensure the confidentiality, integrity, and availability of data entered and stored in PBIS.

Your response to our draft report is included in its entirety as exhibit B, with excerpts incorporated into the findings and recommendations section of the report. Based on your October 29, 2004, response, we have reached management decision for Recommendations 2, 3, 5, 7, 8, 9, and 11. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer. For Recommendations 1, 4, 6, and 10, additional actions are needed to reach management decision. Please refer to the OIG Position section of the report for specific details.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation of the outstanding recommendations noted above. Please note that the regulation requires management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

The courtesies and cooperation extended to the auditors during our audit are appreciated.

/s/

ROBERT W. YOUNG
Assistant Inspector General
for Audit

Executive Summary

Food Safety and Inspection Service Application Controls – Performance Based Inspection System (Audit Report No. 24501-1-FM)

Results in Brief

This report presents the results of our application controls audit of the Food Safety and Inspection Service's (FSIS) Performance Based Inspection System (PBIS). Our objective was to evaluate whether FSIS had adequate and effective controls over the input, processing, and output of PBIS data. FSIS relies on PBIS to manage its inspection activities; a critical component of its mission to ensure that the nation's commercial supply of meat, poultry, and egg products is safe and wholesome. Overall, we found that FSIS had not implemented adequate controls to ensure the integrity of PBIS data. This ultimately may affect FSIS' ability to adequately manage its inspection activities and to ensure that the nation's commercial supply of meat, poultry, and egg products is safe and wholesome.

FSIS had not established effective physical or logical controls over access to the PBIS data. While FSIS management had established certain controls over access to PBIS data, our review disclosed several physical and logical control weaknesses that, if exploited, could result in (1) fraudulent or malicious data being entered into PBIS, (2) data being removed from PBIS, or (3) data being inappropriately changed in PBIS. FSIS relies on PBIS data to conduct establishment trend analysis, generate alerts of potential food-borne illness outbreaks, and other inspection results analyses. This lack of data integrity could ultimately result in trends in unsanitary conditions in federally inspected establishments not being identified and corrected timely.

FSIS personnel had not consistently entered data into the PBIS system. This occurred because FSIS had not established procedures or controls to ensure the data in PBIS was valid. Further, FSIS had not ensured that all field personnel, who are ultimately responsible for data entry, were appropriately trained in how to enter data into PBIS. As a result, there is reduced assurance that FSIS can conduct meaningful analyses using PBIS data to identify trends in unsanitary conditions, or thoroughly rely upon PBIS data to report the accurate operating status of processing establishments.

Changes to existing PBIS data can be made without authorization and validation and are not tracked or logged in the event that the original data needs to be recovered. FSIS management relies on field inspectors for all data input and assurance of data integrity. As a result, FSIS management could not be assured that PBIS data is reliable or supportable.

FSIS was not using complete or up-to-date PBIS data to prepare management reports and conduct trend analysis. FSIS had not established written policies or controls to ensure that field inspectors synchronized, or replicated, their

local systems with the master database on a daily basis. Further, FSIS headquarters personnel prepared management reports from backup PBIS data that was a week old. Due to the distributed nature of the PBIS database, field inspectors were required to use the slow and sometimes inconvenient method of dial-up connections to synchronize their data to the master database. FSIS officials informed us that preparing management reports from the central server database would cause too much activity on the master server. As a result, FSIS' trend analyses may not accurately reflect true conditions in an establishment and may fail to timely identify a problem establishment.

The confidentiality, integrity, and availability of any application depends not only on the controls built into the application itself, but also on the underlying hardware, operating system, and network on which the application resides. Without effective physical and logical controls over network resources and the correction of operating system vulnerabilities, controls written into an application may be circumvented. We found several vulnerabilities in the operating systems used to operate the PBIS system and the firewalls that protect those systems. FSIS management was not vigilant in identifying or correcting network vulnerabilities, and was still in the process of configuring its firewall rules. As a result, the integrity of PBIS data is at risk since these weaknesses may allow the controls built into the PBIS application to be circumvented.

Due to the lack of controls noted during our audit, FSIS cannot be assured that PBIS data is complete, accurate, and reliable. As a result, FSIS management may not have the information it needs to effectively manage its inspection activities. Without effective controls over data integrity, the PBIS system may be an unreliable repository that gives FSIS management a false sense that inspection activities are adequately carried out and sanitation of plant operations is accurately reported.

Recommendations in Brief

We recommend that FSIS:

- Establish access control policies in accordance with Federal guidelines to provide reasonable assurance that access is restricted to only authorized users and that legitimate users have access to only that information needed to perform their job functions.
- Establish a policy and implement controls to provide reasonable assurance that only authorized and allowable data is entered into PBIS and that data used for management reporting is current and reliable.
- Establish a policy and implement controls to (1) limit changes to PBIS data, (2) require adequate justification be maintained when changes are necessary, and (3) require that all changes to PBIS data be logged.

- FSIS should establish and implement procedures to ensure that all security settings are configured in accordance with departmental guidance, and vigilantly identify and correct network vulnerabilities.

Agency Response

FSIS generally agreed with the findings and recommendations in the report. However, FSIS responded that the report infers that inadequate controls over data entry in PBIS could ultimately lead to the occurrence of an outbreak of foodborne illness. FSIS stated that this inaccurately suggests that the Agency's sole mechanism for enforcing its regulatory authority is accomplished based on information provided by PBIS. FSIS stated that PBIS is just one of a number of data sources that the Agency uses to prompt regulatory action.

OIG Position

While the information contained in PBIS is not the only data source FSIS has for prompting regulatory action, it is critical to planning, implementing, and documenting inspection activities. We contend that FSIS should continue to improve the timeliness and accuracy of PBIS data. This will enhance FSIS' ability to schedule inspections based on the most comprehensive and updated information.

We were able to reach management decision on Recommendations 2, 3, 5, 7, 8, 9, and 11. Our position on what is needed to reach management decision on Recommendations 1, 4, 6, and 10 is outlined in the findings and recommendations sections of the report.

Abbreviations Used in This Report

DM	Departmental Manual
FSIS	Food Safety and Inspection Service
HACCP	Hazard Analysis and Critical Control Point
ID	Identification
IT	Information Technology
NIST	National Institute of Standards and Technology
NR	Noncompliance Report
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PBIS	Performance Based Inspection System
SDLC	System Development Life Cycle
TCP/IP	Transmission Control Protocol/Internet Protocol
USDA	U. S. Department of Agriculture

Table of Contents

Executive Summary	i
Abbreviations Used in This Report	iv
Background and Objectives	1
Findings and Recommendations	3
Section 1. Integrity of Data Input	3
Finding 1 Weak Access Controls Jeopardize Data Integrity	3
Recommendation No. 1.....	7
Finding 2 Inconsistent Data Entry and Lack of Data Authorization and Validation Impacts PBIS Reliability	7
Recommendation No. 2.....	10
Recommendation No. 3.....	11
Finding 3 Changes to PBIS Data Not Adequately Controlled	11
Recommendation No. 4.....	13
Section 2. Data Completeness and Timeliness Critical for Effective Management	14
Finding 4 PBIS Data Not Complete or Timely	14
Recommendation No. 5.....	15
Recommendation No. 6.....	16
Section 3. General Controls over System Security and Development Need Strengthening...	17
Finding 5 System Configuration and Vulnerabilities	17
Recommendation No. 7.....	18
Recommendation No. 8.....	18
Finding 6 Lack of Security Planning and Segregation of Duties Jeopardizes the Continued Operation of PBIS	19
Recommendation No. 9.....	21
Recommendation No. 10.....	22
Recommendation No. 11.....	22
Scope and Methodology	23
Exhibit A – PBIS Application Controls Matrix	24
Exhibit B – Agency Response	26

Background and Objectives

Background

Application controls are the structure, policies, and procedures that apply to separate, individual application systems. An application system is typically a collection or group of individual computer programs that relate to a common function. In the Federal Government, some applications may be complex, comprehensive systems, involving numerous computer programs and organizational units, such as those associated with benefit payment systems. Application controls can encompass both the routines contained within the computer program code, and the policies and procedures associated with user activities, such as manual measures performed by the user to determine that data was processed accurately by the computer.

Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer. They are commonly categorized into three phases of a processing cycle:

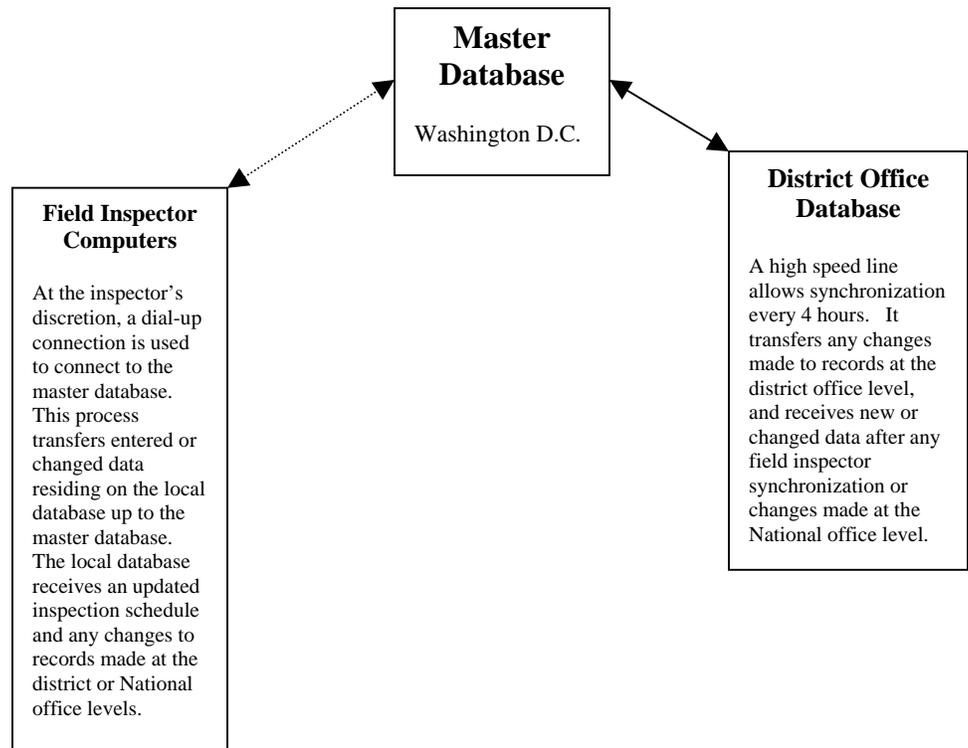
- **Input**—data are authorized, converted to an automated form, and entered into the application in an accurate, complete, and timely manner.
- **Processing**—data are properly processed by the computer and files are updated correctly.
- **Output**—files and reports generated by the application actually occur and accurately reflect the results of processing, and reports are controlled and distributed to the authorized users.

In addition, general security controls and automated controls built into the operating system that support the application should also be considered. Weak controls that allow physical or logical access to the computers that store application data could be used to circumvent the controls established within the application itself.

The Food Safety and Inspection Service (FSIS) is the public health agency in the U.S. Department of Agriculture (USDA) responsible for ensuring that the nation's commercial supply of meat, poultry, and egg products is safe, wholesome, and correctly labeled and packaged. The Performance Based Inspection System (PBIS) is a software application designed by FSIS to manage its Hazard Analysis and Critical Control Point (HACCP) assignment schedules, inspection procedures, and data reporting. PBIS is designed to use data entered by field inspectors and other district and State personnel, to

create inspection schedules and maintain records of findings for reporting purposes. Further, data entered into PBIS is used by other critical management support systems such as FSIS' early warning system, which alerts FSIS officials of potential food-borne illness outbreaks.

When it was first implemented in 1989, PBIS improved the uniformity and reporting of inspection activities. As the demands on meat and poultry inspection have grown, so have the demands on PBIS. Since its first implementation, PBIS has shifted from a paper-based system of data collection to the paperless system it is today. Using dial-up connections, inspectors receive their procedure schedules. Inspectors are also responsible for inputting their inspection results, also known as "entering feedback," and transmitting this information to headquarters on a regular basis. This process synchronizes, or replicates, the inspection findings from the local computer used by field inspectors to the PBIS national database, which resides in Washington, D.C. The following diagram explains how data flows within this distributed database:



In addition, field inspectors have the ability to enter noncompliance report (NR) records and analyze current and historical inspection results for all plans covered by their assignment.

Objectives

Our objective was to determine whether FSIS had established adequate controls to ensure that data entered into PBIS are properly authorized and completely and accurately processed.

Findings and Recommendations

Section 1. Integrity of Data Input

Input controls are perhaps the most critical of all application controls. It is this phase of the process that ensures only authorized, accurate, and complete data is entered into the application. Granting access to only authorized personnel, giving personnel only the level of access necessary to perform their job functions, and authorizing data before it is entered are all critical to ensuring the integrity of the data. We found that FSIS did not have effective controls in place to ensure that access to the PBIS system was controlled and that only authorized data and changes to that data were entered. While FSIS had implemented some access controls, those controls were not entirely effective to ensure the integrity of the PBIS data. This ultimately may affect FSIS' ability to adequately manage its inspection activities and to ensure that the nation's commercial supply of meat, poultry, and egg products is safe and wholesome.

Finding 1

Weak Access Controls Jeopardize Data Integrity

FSIS had not established stringent physical or logical controls over access to PBIS data. This occurred because FSIS had not conducted a thorough risk assessment to identify weaknesses in its access controls. Despite the controls that FSIS had established, our review disclosed several physical and logical control weaknesses that, if exploited, could result in (1) fraudulent or malicious data being entered into PBIS, (2) data being removed from PBIS, or (3) data being inappropriately changed in PBIS. FSIS relies on PBIS data to conduct establishment trend analyses, generate alerts of potential food-borne illness outbreaks, and other inspection result analyses. The lack of data integrity could ultimately result in trends in unsanitary conditions in federally inspected establishments not being identified and corrected timely.

The Department¹ requires agencies to use individual user identifications (ID) and passwords to control access to systems processing personnel, financial, market-related, or other sensitive data. The Department also requires agencies to remove employee user accounts and passwords when the employee is no longer employed by the agency. Further, the Department² requires that systems be physically controlled and that only authorized users have access. The Office of Management and Budget (OMB) lists individual accountability as a primary mechanism for personnel security.³ It recognizes

¹ Departmental Manual (DM) 3140-1.6, "Management ADP Security Manual," part 6 of 8, Appendix D, Section 4.a.

² DM 3140-1, "Management ADP Security Manual," Section 14, "Physical Security Standards," dated July 19, 1984.

³ OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 28, 2000.

that accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. Finally, both the National Institute of Standards and Technology (NIST)⁴ and OMB advocate implementation of the “least privilege” concept, granting users only the access required to perform their duties.

Access controls over system and application data include both physical and logical controls and should provide reasonable assurance that computer resources (data files, application programs, and computer equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Physical access controls, such as locked server room doors, ensure that only authorized personnel can physically handle and perform maintenance on network servers and other hardware. Logical access controls such as user names, passwords, and access permissions, ensure that only authorized users have access to network resources from their workstations, and that users are granted only the access that is needed to conduct their job responsibilities.

PBIS is a distributed database system. Daily inspection results are entered into the PBIS database residing on the individual field inspector’s computer. No dial-up connection to the central PBIS server is required to enter or alter the information in the inspector’s local computer. At his or her discretion, the inspector uses a dial-up connection to the central server in Washington, D.C., to synchronize, or replicate, all new or changed data entered since the last transmission to the central server.

Given the highly distributed nature of the PBIS application, access controls over PBIS data and the computers that store the data are FSIS’ first defense against unauthorized access and modification of inspection data. Without strong physical and logical access controls over PBIS data input and update capabilities, the integrity of the application data may be compromised. Further, with the lack of logging and an audit trail (see Finding No. 3), neither FSIS management nor the Office of Inspector General (OIG) could validate whether appropriate changes were made to the PBIS data FSIS uses for trend analysis and alerts of potential food-borne illnesses.

Restricted to Authorized Users

Our visits to ten establishments in two districts disclosed that FSIS computers used for PBIS data entry were not physically protected to prevent access by unauthorized individuals. FSIS had not established written policies on how employees were to properly safeguard PBIS data. For example, at one establishment, the computer resided in an office that opened into the employee break room. While the FSIS office door had been locked after

⁴ NIST Special Publication (SP) 800-12, “An Introduction to Computer Security,” dated October 1995.

normal business hours, we observed that the door was left unsecured while the field inspector performed his duties. FSIS personnel would not have known if establishment personnel had attempted to use the computer to enter, modify, or delete inspection data during the field inspector's normal and routine absences.

While FSIS had established certain controls over PBIS data such as unique and separate user IDs and passwords for both the computer and the PBIS system, our observations disclosed that these controls were inadequate to ensure that data entry was restricted to only authorized users. Specifically, passwords were not properly safeguarded, and passwords did not meet established guidelines. At one district office, we found that the PBIS administrators had their user IDs and passwords taped to the side of their computer monitor. This note included their user ID and password for both the computer and the PBIS application.

Additionally, password parameters in PBIS did not always meet departmental or Office of the Chief Information Officer (OCIO) requirements. FSIS had not established written password parameter requirements. For example:

- Password age was set at 180 days from creation to expiration. Departmental regulations⁵ state that the maximum life for passwords on interactive systems, like PBIS, is no more than 90 days.
- Passwords were set at five characters. Current guidance issued by the OCIO requires the use of at least eight characters.
- While the user ID appropriately locked after three unsuccessful attempts, the lock out duration was only 60 seconds. OCIO guidance states that the account should be locked "forever," that is, until unlocked by a system administrator.
- FSIS had not maintained online access logs, detailing the user ID and time of access for each connection to PBIS as required by departmental regulations.⁶

Further, we observed inspectors in five different establishments who would log into the computer and the PBIS application in the morning and remain logged in all day. Users had not manually logged out of PBIS during absences from the computer and PBIS did not have a feature to automatically log the user off for inactivity. As a result, any security protection provided by the establishment of user IDs and passwords was bypassed. We further

⁵ DM 3140-1, Appendix D, paragraph 6b, dated July 19, 1984.

⁶ DM 3140-1, Appendix D, paragraph 5, dated July 19, 1984.

observed that password-protected screen savers on the systems that store PBIS data did not activate or allowed excessive time to lapse before locking access to the computer.

FSIS management further informed us that one additional control they established was that the dial-up connections, used to transfer inspection data to the main server, automatically timed-out after a short period of inactivity. While our tests confirmed that dial-up time-out settings were not consistently set and in some cases not set at all, this control is not effective in ensuring data integrity. Given the distributed nature of the PBIS data, access to the dial-up connection and central server would not be necessary to enter fraudulent or malicious information into the data stream. Simply entering or altering information on the field inspector's computer would be sufficient for the information to be entered or modified, ultimately jeopardizing the integrity of the master PBIS database.

Restricted to Authorized Purposes

PBIS had not properly restricted authorized users as to what data they could enter. Specifically, we found that PBIS users were segregated into six user levels; consolidated, district, circuit supervisor, relief inspector, in-plant inspector, and compliance personnel. According to FSIS management, each user level had a different functionality in each input screen of PBIS. For example, the "in-plant inspector" level was locked out of the "Applicant" tab so those users could not change an establishment's name or grant date. Further, each computer used to access PBIS was limited in what establishment data could be accessed, limiting employees' ability to access inspection data pertaining to establishments not under their control.

While we agree that these were good first steps in controlling inappropriate access, these controls were not adequate by themselves. Our review of the user levels for individuals in district offices disclosed that all employees in the district office, from secretaries to managers, had the same user level associated with their user ID and had the same access authorizations in PBIS. For instance, in one district office we visited, only two individuals had the job responsibility of resetting passwords for all district personnel; however, all employees in that office had the ability to reset any district office employee's password. In addition, one district office employee who required read-only access had the ability to enter, delete, and alter information in PBIS.

Recommendation No. 1

Establish policies and implement stronger controls, in accordance with departmental and Federal guidelines, in PBIS and the systems on which PBIS data reside to ensure that access is restricted to only authorized users and that legitimate users have access to only that information needed to perform their job functions.

Agency Response. FSIS has fully deployed Windows XP on all Federal inspectors' computers. Access requirements on computers with Windows XP meet departmental guidelines for password aging, length, etc. Several of the computers in the field that the OIG examined contained the Windows 95 operating system, which was not as secure as XP. Additionally, FSIS implemented mandatory online security awareness training for all users of computers. This training provides specific guidance on system security vulnerabilities, including methods for safeguarding passwords. Employees were required to complete the security awareness training by October 25, 2004.

Additionally, FSIS will develop a written policy on PBIS access control to limit and restrict access to PBIS data to only authorized users. The access control policy will ensure that guidance is provided on safeguarding passwords and that passwords meet departmental requirements. FSIS will issue this policy by January 2005.

OIG Position. We concur with FSIS' actions to upgrade user systems, establish formal access control policies, and provide users security awareness training; however, we reported access controls throughout the PBIS system, not just with user workstations. For instance, the PBIS application contained only a few user categories (i.e., profiles) that did not sufficiently limit users' abilities to access and update data consistent with their job responsibilities. In order to reach management decision FSIS needs to provide us timeframes for reviewing access controls throughout the PBIS infrastructure and ensure that adequate controls are put in place to limit access to PBIS data in accordance with NIST and departmental policy and the least privilege principle.

Finding 2

Inconsistent Data Entry and Lack of Data Authorization and Validation Impacts PBIS Reliability

FSIS personnel had not consistently entered data into the PBIS system. This occurred because FSIS had not established formal policies or procedures on how data should be entered, or ensured that all field personnel, who are

ultimately responsible for data entry, were appropriately trained in how to enter data into PBIS. Further, FSIS relied heavily on field inspectors to ensure the validity of the data entered into PBIS, which is used by FSIS management to manage their HACCP program. As a result, FSIS may not be able to conduct meaningful analysis to identify trends in unsanitary conditions or respond to PBIS data to report on the accurate operating status of processing establishments.

The Department⁷ requires agencies to build application controls to prevent unauthorized access to data files; design and write applications to compare input controls with data, ensure the correct selection of files and validation of data, and protect the records associated with automated decision-making applications. In addition, NIST⁸ requires that data be validated during collection and entry prior to use by the system.

Inconsistency in Data Entry

We observed that data entered into PBIS varied widely among the numerous field inspectors we visited. FSIS had not established formal policies on how data needs to be entered into PBIS. Further, numerous FSIS personnel informed us (and a lack of training documentation confirmed) that field inspectors and field supervisors had not been adequately trained on using PBIS. As a result, trend analyses and sanitation alerts based on PBIS data may be unreliable.

When FSIS field inspectors identify an unsanitary condition or other issue of noncompliance, the field inspector is required to enter the noncompliance in PBIS, creating a NR. Once finalized, the NR data is locked in PBIS to prevent changes. The NR should then be printed out and provided to the establishment management for their signature and a description of what corrective action they are taking to correct the problem and prevent recurrence. According to FSIS procedures, once the corrective actions have been completed, the NR should then be flagged as closed in PBIS.

However, during our visits to 10 processing establishments, we observed that FSIS inspectors exercised their judgment on when to lock and close NR records.⁹ While most inspectors we visited locked NR records appropriately, one field inspector had never locked an NR record until we brought this to the attention of the field supervisor and district office personnel. Since the inspector had never closed an NR, the establishment management had signed

⁷ DM 3140-1, "Management ADP Security Manual," Section 17, "Application System Development," dated July 19, 1984.

⁸ National Bureau of Standards (predecessor agency to NIST) Federal Information Processing Standards Publication 73, "Guidelines for Security of Computer Applications," dated June 30, 1980. The Federal Information Security Management Act of 2002 gives NIST the authority to establish security requirements for Federal information systems.

⁹ FSIS has programmed PBIS to flag NR records as 'final' which effectively locks the record to prevent changes. Once the establishment addresses the unsanitary conditions that were noted in the NR, the NR record is flagged as 'closed.'

draft, not final, NR reports. The inspector informed us that he was never informed that he had to finalize, or lock, the NR. According to FSIS procedures, FSIS could not use draft NR reports as a justification for suspending inspection activities for unsanitary conditions.

We observed that FSIS inspectors' processes were even less consistent when it came to closing an NR record. We found instances where field inspectors closed NR records:

- When the NR was presented to or signed by establishment management even if no action was taken to correct the deficiency;
- only after the immediate cause of adulteration or contamination was eliminated, even if long-term preventative corrective action agreed to by the establishment had not yet been implemented; or
- after all immediate and long-term corrective actions had been taken.

FSIS' procedures recognize that the timeliness of corrective actions to noncompliance issues is an indication of whether continued adulteration or contamination may recur. Due to the inconsistent data entry, FSIS management would not have been able to use the NR record closed date recorded in PBIS to accurately evaluate whether processing establishments had made corrections to sanitation problems in a timely manner.

We also evaluated FSIS' controls over suspending inspection activities. Inspectors used the PBIS "suspend" code to indicate that the mandatory inspections were being temporarily suspended due to custom slaughter or if a processing line was down for repair or upgrade, resulting in no inspections being scheduled by PBIS. However, other inspectors used the "suspend" code to indicate that FSIS inspectors were being withdrawn from the establishment due to the conditions in the plant and establishment's continued ineffective corrective actions. Therefore, FSIS management may not be able to rely on PBIS data to accurately report those establishments that had inspection activities suspended due to sanitation violations.

We attribute the inconsistent data entry, in part, to FSIS not having provided effective training to field inspectors. We found that only 1 of the 12 field inspectors and field supervisors we interviewed had received training. One inspector indicated that the extent of the training received included only how to turn on the computer, start the program, and enter the user ID and password. Another field inspector received an automated tutorial that she was never required to complete. The remaining 10 field inspectors and field supervisors indicated that they were simply provided with the application, a user's manual, and a computer.

The lack of consistent coding of NR records and suspended establishments reduces the effectiveness of FSIS' analysis of PBIS data.

Lack of Authorization or Second Party Review

FSIS had not implemented adequate controls to ensure that only authorized and complete data was entered and maintained in the PBIS system. FSIS officials relied on field inspectors to ensure that only authorized data was entered into the system, and therefore have not implemented controls over the authorization of data or second-party review process. This condition is more critical considering the weak access control issues we identified in Finding No. 1. As a result, FSIS management cannot ensure that only complete and accurate data is being used to manage its inspection activities.

Historically, FSIS maintained paper documents as evidence of its inspection activities. These paper documents were ultimately entered into the system and served as a supporting basis for the data that was entered. If necessary, FSIS could use the documents to verify that the data entered into the system was accurate and complete by performing reconciliations or verifications between system data and paper documents. In paperless applications, like the current version of PBIS, controls such as those noted throughout this report need to be established to ensure the integrity of the data entered into the system.

FSIS officials informed us that field supervisors ensure that the inspection activities are conducted properly and that inspection results are entered into PBIS by conducting site visits to inspectors in their circuit. However, the frequencies of field supervisor visits to inspectors varied widely by supervisor and circuit, ranging from one visit a month to one visit a quarter. Because PBIS is a paperless system, it is impractical for supervisors to verify the accuracy of inspection reports during their visits.

Field inspectors are solely responsible for gathering and entering the results of their inspections without supervisory or independent review or approval. Further, FSIS is not conducting reconciliations of the data with expected results. Once the information is entered, PBIS accepts and processes all inspection results entered, using the data for trend analyses and indications of potential outbreaks of food-borne illnesses.

Recommendation No. 2

Establish a policy on how data is to be entered into PBIS, and implement controls to ensure that all PBIS users are provided adequate training on how to enter and control data in the PBIS database.

Recommendation No. 3

Establish a policy and implement controls to provide reasonable assurance that only authorized and allowable data is entered into PBIS.

Agency Response. To bolster the users' understanding of entering data into PBIS, FSIS will issue a policy that provides instructions on when certain inspection information should be entered into the system. Also, FSIS plans to integrate the PBIS user's guide as an online reference guide to further assist the users. In its release of PBIS version 5.1, the online help capability will assist inspection personnel in understanding how information should be entered into the system. In addition, FSIS' Center for Learning will coordinate with the Office of Field Operations and the Chief Information Officer to provide PBIS 5.1 training.

FSIS expects to release PBIS version 5.1 by January 2005. FSIS will issue its policy document by March 2005.

OIG Position. We concur with FSIS' management decision on these recommendations.

Finding 3

Changes to PBIS Data Not Adequately Controlled

Changes to existing PBIS data can be made without authorization and validation. FSIS management relies on field inspectors for all data input and assurance of data integrity. FSIS had not implemented automated controls to ensure that changes made to PBIS data were tracked and logged. As a result, FSIS management could not be assured that PBIS data is reliable or supportable.

NIST¹⁰ requires that data be validated during collection and entry. NIST further recognizes that the process of correcting errors in data is prone to contribute further errors and should be validated throughout the process. In a prior audit,¹¹ we reported that FSIS had not implemented a formal process for its database administrators to follow when making changes to the various databases maintained by its headquarters staff. We also found that numerous individuals had database administrative authority. In its response, FSIS

¹⁰ National Bureau of Standards (predecessor agency to NIST) Federal Information Processing Standards Publication 73, "Guidelines for Security of Computer Applications," dated June 30, 1980.

¹¹ Audit Report No. 24099-1-FM, "Security Over the Information Technology Resources at the Food Safety and Inspection Service," dated August 11, 2003.

stated that it had created a Change Control Board to oversee system changes, and would review the access levels of those individuals with administrative access to its databases.

At the 10 establishments visited, we observed that anyone with access to the field inspector's local computer could change inspection data, regardless of who entered the data. For example, the field supervisor could change the results of inspections for establishments in his or her circuit, even if the field inspector entered the results. Additionally, FSIS did not program PBIS to maintain a justification for why the change was made. Further, the updated data overwrites the original on the local computer, and is replicated to the master database in Washington, D.C., the next time synchronization¹² takes place.

Discussions with field supervisors disclosed that changes had been routinely made to the data originally entered by the field inspectors. This occurred despite the fact, as mentioned in Finding No. 2, that paper evidence of inspections is not maintained to validate the accuracy of changes. Further, the field supervisors did not have documentary evidence that the changes were necessary. One field supervisor informed us that he had accidentally over written the results of his subordinates' inspection activities on more than one occasion. We were unable to verify whether data was missing due to accidental deletion because (1) the lack of original source documents and (2) the lack of built-in controls to prevent or detect accidental modification or deletion of data.

For NR records that had been locked (see Finding No. 2), PBIS required an unlock code to make changes. Field inspectors and field supervisors are required to contact the district office to obtain an unlock code. However, we found that the district office personnel who issued the unlock codes did not ask for a justification or documentation of the changes. In addition, logs of the unlock codes were not maintained.

Finally, there were ineffective controls established to confirm or validate changes to NR records before being uploaded to the master database. The PBIS administrative assistants at the two district offices we visited informed us that they confirmed that changes were made to unlocked NR records, but they did not substantiate whether or not the change was appropriate or accurate. Additionally, the PBIS central server will accept and process the data regardless of whether the district office had confirmed the change.

¹² Synchronization is the process where data stored on the local field inspector's computer is uploaded, or copied, to the master server.

Recommendation No. 4

Establish a policy and implement controls to (1) limit changes to PBIS data, (2) require adequate justification be maintained when changes are necessary, and (3) require that all changes to PBIS data be logged.

Agency Response. Information in PBIS can be generally categorized as incidents and profiles. Incidents describe events occurring at a discrete point in time, for example, inspections, noncompliance reports, etc. All these occur daily throughout FSIS. On the other hand, profile data is more static in nature and is not based on time or an event. Examples include Establishment Profiles, Circuit structure, District Staffing information, etc. While the information can (and does) change periodically, it's not usually changing daily. FSIS has established an information technology (IT) work group that is exploring the need for locking certain types of data in the system based on the classification of the information as either an incident or profile type.

Currently, PBIS maintains a transaction history log that tracks changes made in the system, and the users who made them. Enclosure 1 contains a transaction history report for the period October 17-22, 2004.

OIG Position. We agree that data in PBIS is subject to periodic and necessary change. However, we observed several instances where data in PBIS was changed without justification, without second party review, or without being adequately tracked in the event that a change was made inappropriately. If FSIS maintained paper documentation to support and verify changes made in the database, these controls may not be needed; however, the paperless environment in which PBIS data is entered requires more stringent controls to ensure the appropriateness of changes. To reach management decision, FSIS needs to provide us its plan and timeframes for reviewing how PBIS changes will be limited, justified, and thoroughly logged.

Section 2. Data Completeness and Timeliness Critical for Effective Management

Finding 4 PBIS Data Not Complete or Timely

FSIS was not using complete, or the available up-to-date PBIS data to conduct trend analyses. This occurred because field inspectors were not required to synchronize their local systems with the master database on a daily basis. Further, FSIS Headquarters personnel prepared management reports from backup PBIS data that was a week old. Field inspectors did not synchronize due to the slow and sometime inconvenient process of using dial-up access to the central server. FSIS officials informed us that preparing management reports from the central server database would cause too much activity on the master server. As a result, FSIS' analytical procedures may not accurately reflect true conditions in an establishment and may fail to timely identify a problem establishment.

NIST¹³ requires that data be validated during collection and entry prior to use by the system to ensure data is accurate, complete, consistent, unambiguous, and reasonable. Validation checks play a significant role in ensuring that data is complete.

After completing an inspection, field inspectors enter the results into the database residing on their local computers. The data resides on that local computer until the field inspector manually selects the PBIS feature to synchronize (replicate) any new and updated data from the local computer to the central PBIS server in Washington, D.C. This central PBIS server is used to alert FSIS officials at both the national and district level of potentially serious sanitation trends, and is used by FSIS officials to conduct trend analyses on inspection results. Without complete and up-to-date inspection results, these projections and trend analyses are based on incomplete results and may not accurately reflect the conditions in an establishment and may fail to identify a problem establishment. The timeliness and completeness of PBIS data is critical to the effective management of FSIS inspection activities.

Data Synchronization

PBIS maintains the last synchronization date for every registered computer. Our review of all 3,660 computers registered in PBIS on March 19, 2004, disclosed that 1,072 (29 percent) had not synchronized within at least 3 days

¹³ National Bureau of Standards (predecessor agency to NIST) Federal Information Processing Standards Publication 73, "Guidelines for Security of Computer Applications," dated June 30, 1980.

from the date of our analysis. Of those, 623 (17 percent) had not synchronized for 7 days or more. Therefore, FSIS was using incomplete data to identify sanitation trends and manage its inspection activities.

FSIS Headquarters personnel monitor PBIS reports that show computers that have not synchronized in 45 days. Our review of one such report, dated February 27, 2004, disclosed that there were 63 computers, of which only 7 (11 percent) synchronized when the user was informed that they needed to synchronize. FSIS is supposed to remove systems from PBIS if they do not synchronize timely. However, we found that three computers were not eliminated from PBIS even though they appeared on this listing, and two computers appeared on two subsequent reports. Additionally, FSIS has no formal policy dictating how often the field inspectors should be synchronizing with the central server. Further, while reports are available in PBIS for district office managers to monitor synchronization, there is no formal requirement to run this report or instructions on what followup actions need to be taken.

Database Record Serial Numbers Not Tracked During Data Synchronization

In addition to the lack of controls requiring field inspectors to synchronize their local data with the PBIS master database, PBIS lacked adequate controls to ensure that complete synchronization occurs. Each database record in PBIS is assigned a unique serial number. FSIS officials informed us that the main purpose of this number was intended to ensure that duplicate data is not entered into the master database and that the data is complete. However, PBIS did not have an automated process to verify that all database record serial numbers are accounted for during processing.

For instance, a field inspector could delete a record in their local database prior to synchronizing with the master database. Instead of maintaining a record that the database record once existed, PBIS simply removes the database record from the database. When field inspectors synchronized their local database with the master PBIS database, PBIS did not provide a warning message or produce an error report signaling the missing number in the sequence. As a result, FSIS has limited assurance that all data transmitted was appropriately synchronized from the local computer into the central server.

Recommendation No. 5

Implement a policy and establish controls to ensure that field inspectors synchronize inspection results daily and that all database records are accounted for during synchronization.

Recommendation No. 6

Implement a policy and establish controls to ensure that management reports and data analyses are generated from the most up-to-date data available.

Agency Response. FSIS is able to utilize data effectively from PBIS when the database is synchronized less frequently than daily. Guidance has been provided in the PBIS users' guide for inspection program personnel to conduct daily synchronization. FSIS will determine whether the guidance provided in the PBIS users' guide should be updated. FSIS will issue a policy and update the PBIS user's guide, if necessary, establishing the time requirements for synchronization.

FSIS will issue a policy on time requirements for PBIS synchronization by March 2005.

OIG Position. We concur with FSIS' management decision on Recommendation No. 5.

Recommendation No. 6 also addressed FSIS' process of producing management reports using the PBIS backup server, which is typically 2 weeks behind the live data. This time lag, in addition to the synchronization issues addressed in Recommendation No. 5, raise questions about the timeliness and reliability of the data on management reports. In order to reach management decision, FSIS needs to provide us with its plan and timeframes for reviewing the timeliness and reliability of PBIS management reports in performing its mission and taking any necessary actions resulting from its review.

Section 3. General Controls over System Security and Development Need Strengthening

The confidentiality, integrity, and availability of any application depends not only on the controls built into the application itself, but also on the underlying hardware, operating system, and network on which the application resides. Without effective physical and logical controls over network resources and correcting operating system vulnerabilities, controls written into an application may be circumvented.

Finding 5 System Configuration and Vulnerabilities

We found several vulnerabilities in the operating systems used to operate the PBIS system and the firewalls that protect those systems. FSIS management was not vigilant in identifying or correcting network vulnerabilities, and was still in the process of configuring its firewall rules. As a result, the integrity of PBIS data is at risk since these weaknesses may allow the controls built into the PBIS application to be circumvented.

OMB Circular A-130 requires agencies to assess the vulnerability of information system assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce the threat or amount of potential loss. Further, the Department OCIO has established a policy¹⁴ that requires agencies regularly scan their systems for known vulnerabilities using a Department-purchased vulnerability scanning tool. Finally, NIST has published guidelines on the effective implementation of firewalls in Federal agency network environments.¹⁵

Transmission Control Protocol/Internet Protocol (TCP/IP) Vulnerabilities

We used a commercially available software tool that identifies vulnerabilities in network components that use the TCP/IP protocol (the protocol used on the public Internet). We found that FSIS had been using the same vulnerability assessment tool to periodically scan its network and correct vulnerabilities identified. We also found few vulnerabilities on FSIS' network routers and switches, which indicates adequate configuration management over those devices.

Our assessment, however, discovered a number of vulnerabilities on the server that FSIS uses as a backup server and the two state servers we

¹⁴ "Cyber Security Manual," DM 3500-2, Chapter 6, Part 1, dated April 4, 2003.

¹⁵ NIST SP 800-41, "Guidelines on Firewalls and Firewall Policy," dated January 2002.

scanned. FSIS had not conducted scans of these systems as vigorously as they did on the main PBIS database server. One of the most vulnerable weaknesses on the systems we scanned was the ability to easily identify user IDs on those systems. This vulnerability provides a malicious user the information needed to conduct a brute force password attack and gain entry into those systems and potentially the entire network.

Firewall Rules

FSIS had not maintained its firewall in accordance with departmental¹⁶ and NIST guidelines.¹⁷ FSIS was still in the process of configuring its firewall rules when we performed our review. We found that FSIS had incorrectly entered firewall rules giving thousands of IP addresses the ability to pass through the firewall. Our analysis of FSIS' firewall rules also revealed that several rules were either no longer needed, were redundant, or were not configured in the best interest of network security. For example, we found rules that allowed certain access using unsecured TCP/IP protocols to all systems behind the firewall rather than limiting that access to only certain systems.

Recommendation No. 7

FSIS should establish and implement procedures to ensure that all operating systems are configured in accordance with departmental guidance and vigilantly identify and fix TCP/IP vulnerabilities on all of its systems and network devices.

Agency Response. FSIS will establish and implement procedures to ensure that all operating systems are configured in accordance with departmental guidance and identify and fix TCP/IP vulnerabilities on all of its systems and network devices. FSIS will establish procedures by April 2005.

OIG Position. We concur with FSIS' management decision on this recommendation.

Recommendation No. 8

FSIS should establish and implement procedures to ensure that its firewall configuration is configured and maintained in accordance with NIST guidance.

¹⁶ USDA OCIO Cyber Security Policy CS-012, "Gateway and Firewall Technical Security Standards," dated January 18, 2002.

¹⁷ NIST SP 800-41, "Guidelines on Firewalls and Firewall Policy," dated January 2002, page 47/74.

Agency Response. FSIS will establish and implement procedures to ensure that its firewall configuration is configured and maintained in accordance with NIST guidance. FSIS will establish firewall procedures by April 2005.

OIG Position. We concur with FSIS' management decision on this recommendation.

Finding 6**Lack of Security Planning and Segregation of Duties Jeopardizes the Continued Operation of PBIS**

FSIS had not documented the PBIS system and had not established adequate segregation of duties regarding system development. Despite departmental requirements to document major applications during the system development cycle, FSIS officials informed us that they did not document their system due to other priorities. FSIS officials informed us that it was more important to get the application operational than it was to document its processes. As a result, FSIS cannot ensure that the PBIS system will continue to operate in the event of a disaster, major service disruption, or staff turnover. Further, without controls over system development, FSIS could not ensure the integrity of the PBIS data used to manage its inspection activities, conduct trend analysis, and alert FSIS management and consumers of potential sanitation violations.

The foundation for security over IT resources is found in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." This Circular establishes a minimum set of controls for agencies' automated information security programs, including certifying to the security of any systems that maintain sensitive data, establishing contingency plans and recovery procedures in the event of a disaster, and establishing a comprehensive security plan. Further, DM 3140-1 requires that documentation be prepared and maintained throughout the entire system development lifecycle. Finally, Federal Information Processing Standards Publication 73 provides guidance for separation of system development, testing, and daily operation functions.

Lack of System Security Planning

FSIS has not prepared security plans, risk assessments, or disaster recovery plans for the PBIS system as required by departmental regulations, OMB A-130, and NIST. In a prior audit,¹⁸ we reported that FSIS had not prepared

¹⁸ Audit Report No. 24099-1-FM, "Security Over the Information Technology Resources at the Food Safety and Inspection Service," dated August 11, 2003.

security plans for its major applications and general support systems or ensured that its major applications were certified and accredited. The certification and accreditation process helps ensure that adequate security planning and operational guidelines and procedures are in place and operating effectively. In response to that audit, FSIS informed us that it would have all its major applications certified and accredited by June 2003; however, FSIS had only just begun this process during our fieldwork in early calendar year 2004.

OMB Circular A-130 states that all major applications and general support systems containing sensitive information require protection to assure its integrity, availability, or confidentiality; and therefore, require security plans. Security plans should define who has responsibility for system security, who has authority to access the system, appropriate limits on interconnectivity with other systems, and security training for individuals authorized to use the system. Without security plans in place, FSIS is ill prepared to establish effective and comprehensive security over its systems and networks.

Risk assessments, as defined by NIST, are a systematic approach to assessing the vulnerability of information system assets; identifying threats, quantifying the potential losses from threat realization; and developing countermeasures to eliminate or reduce the threat or amount of potential loss. Until these risk assessments are completed, FSIS cannot be reasonably assured that all the risks attributable to PBIS have been considered and that appropriate steps have been taken to mitigate these risks. In our opinion, many of the risks associated with the PBIS system mentioned in this report would have been identified had a formal risk assessment been conducted.

We also found that FSIS is not fully prepared to respond in the event of a disaster or major disruption, and cannot be assured that vital PBIS data needed to support the management of its inspection program will be available without excessive disruption. One of the most critical weaknesses we found was that FSIS stores its master database server and two other servers that contained backup PBIS data in the same room. Further, FSIS does not backup the master server on tape or other portable media and have the media sent offsite in the event of a disaster or major disruption. FSIS officials were not concerned with these issues because every district office synchronizes with the master database every 4 hours. FSIS officials informed us that the worst-case scenario would be that they would have to recreate the master database from the district office data. If this occurred, FSIS could lose up to 4 hours of data from every district, thereby causing its analysis of PBIS data to be incomplete and inaccurate.

During our fieldwork, FSIS had begun to certify and accredit its major applications. FSIS had prepared a statement of work to begin this process,

which would include conducting a risk assessment, preparing security plans, and establishing a disaster recovery plan.

Inadequate Segregation of Duties Over System Development and Maintenance

In Finding No. 1, we reported that FSIS had not programmed PBIS to effectively limit access by employees to only the data and access capabilities needed to perform their job duties. In addition, FSIS had not established segregation of duties controls over system development and maintenance. FSIS had one person in charge of developing, programming, testing the PBIS system, and moving tested code into the production environment. Each of these functions should be separated to ensure that only authorized changes are made to applications, that the application is fully tested, and that only approved and tested code enter the production environment. In addition the one FSIS employee also had complete control to add, delete, and modify any production information in the PBIS master database.

Recommendation No. 9

FSIS should document the application, data flow, and data elements of the PBIS system to provide the foundation of operational and security planning, and ensure the continual operation of the system in the event of a disruption of service or turnover in staff.

Agency Response. FSIS agrees that system documentation to assure the continuity of operation of the PBIS is important. FSIS will follow the Department's standard System Development Life Cycle (SDLC) process for documenting its information systems. A standard SDLC, in accordance with Department requirements, will be adopted for all new major system development and modifications. FSIS will utilize a contractor to document the SDLC currently being used. The SDLC will be used on all new major system development and modifications. The SDLC will include a security study, feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation, and post implementation review. A contract to document the SDLC for all new major systems and modifications will be awarded by November 2004.

In the meantime, documentation of PBIS version 5.1 will be completed by September 2005 to address a similar issue identified in the certification and accreditation process and scheduled in FSIS' mitigation plan.

OIG Position. We concur with FSIS' management decision on this recommendation.

Recommendation No. 10

FSIS should establish controls to ensure that the current certification and accreditation process is performed on a 3-year basis and that security planning documents remain up-to-date as required by OMB.

Agency Response. FSIS included, in its annual budget request, funding to provide for performing the certification and accreditation process on a 3-year basis as required by OMB.

OIG Position. We concur with FSIS' plans to request funding to conduct certification and accreditation as required by OMB A-130. However, in order to reach management decision, FSIS needs to provide us its timeframes for establishing a formal policy and implementing controls for ensuring that the certification and accreditation process is actually performed as required by OMB throughout all of its systems' life cycles.

Recommendation No. 11

Establish a policy and implement controls to ensure the proper segregation of duties over the PBIS system development, testing, and production environments.

Agency Response. FSIS is currently reorganizing the IT structure to segregate duties and responsibilities. The reorganized structure will ensure the separation of functions such as system development, testing, implementation, and configuration management. The reorganization is expected to be completed by January 2005.

OIG Position. We concur with FSIS' management decision on this recommendation.

Scope and Methodology

Our audit was part of a nationwide audit of selected USDA agencies. We reviewed application controls over the PBIS established by FSIS to ensure the confidentiality, integrity, and availability of information in that system. The review was conducted at FSIS Headquarters in Washington, D.C., two district offices, and ten processing establishments. District and processing establishments were judgmentally selected based on the size of the processing establishment, as reported by FSIS, and the type of processing conducted.

Fieldwork was performed from January through May 2004.

To accomplish our audit objectives, we performed the following audit steps and procedures:

- We reviewed policies, procedures, and system documentation when available relating to the PBIS system.
- We interviewed FSIS officials responsible for the development, management, and data input of the PBIS system.
- We performed tests of data authorization, completeness, and accuracy at selected district and processing facilities.
- We analyzed system source code and data records to verify the integrity of PBIS data.

This audit was performed in accordance with Government Auditing Standards. The results of recently issued reports of FSIS' inspection activities and security of IT resources were considered in preparing this report.

Exhibit A – PBIS Application Controls Matrix

Control Objective (Based on U.S. General Accountability Office Federal Information System Control Audit Manual)	PBIS Control Technique(s)¹⁹	OIG Evaluation
All data are authorized before entering the application system.	<ul style="list-style-type: none"> • Data entered by field inspectors. • Locked noncompliance report records require an unlock code by district office officials. 	<ul style="list-style-type: none"> • PBIS is paperless and no input documents exist for subsequent validation or reconciliation. • Unlock codes are provided by the district office without justification. • Changes made to PBIS are flagged as ‘confirmed’ by district office without basis to confirm the validity of the change. • PBIS is programmed to accept, process, and report all changed records even if not flagged as ‘confirmed’ by the district office.
Restrict data entry terminals to authorized users for authorized purposes.	<ul style="list-style-type: none"> • User IDs and passwords are required on field, district, and headquarters computers. • User IDs and passwords are required to gain access into PBIS application and data maintained on field inspector’s computers. • Password-protected screensavers locked access to computers. • PBIS maintains records of all computers allowed to synchronize with the master database. • User IDs and passwords are needed to dial-up to central PBIS server. • Dial-up access to central server timed out after 10 minutes of inactivity. • Users are limited access to PBIS data based on one of six roles. 	<ul style="list-style-type: none"> • Field inspector’s computers were not always physically protected from unauthorized access. • Not all password-protected screensavers were configured. Some we tested were disabled, others allowed too much time to pass before locking the computer. • Password length, age, and lockout duration were not set in accordance with Department and NIST guidelines. • PBIS maintains a log of computers that have synchronized their data with the master server. • PBIS user roles are broad in nature and are not granular enough to control access based on job responsibilities. For instance, a district office secretary had the same privilege in PBIS as a district manager.
Master files and exception reporting help ensure all data processed are authorized.	<ul style="list-style-type: none"> • PBIS was programmed to synchronize with only registered computer systems. 	<ul style="list-style-type: none"> • FSIS was not timely removing systems that had not synchronized within 45 days.

¹⁹ PBIS control techniques as reported to us by FSIS officials. No system documentation existed outlining the controls established.

Exhibit A – PBIS Application Controls Matrix

<p>All authorized transactions (data) are entered into and processed by the computer.</p>	<ul style="list-style-type: none"> No controls established. 	<ul style="list-style-type: none"> Our testing disclosed that no controls existed. FSIS relied on field inspectors to ensure that all inspections performed and all noncompliance records were timely entered into the system.
<p>Reconciliations are performed to verify data completeness.</p>	<ul style="list-style-type: none"> FSIS Headquarters personnel produced a report showing field computers that had not synchronized with the master database within 45 days. FSIS Headquarters personnel judgmentally removed field computer's ability to synchronize (usually after appearing on the 45 day list). 	<ul style="list-style-type: none"> FSIS was not timely removing systems that had not synchronized within 45 days. FSIS could not provide evidence that other reconciliation reports were performed.
<p>Data entry design features contribute to data accuracy.</p>	<ul style="list-style-type: none"> PBIS screens were user-friendly. 	<ul style="list-style-type: none"> FSIS had not ensured that all employees receive adequate training. One inspector we visited needed assistance from a field supervisor and district office to enter a noncompliance report.
<p>Data validation and editing are performed to identify erroneous data.</p>	<ul style="list-style-type: none"> PBIS data fields programmed to accept certain values. 	<ul style="list-style-type: none"> PBIS system accepted records that had been changed regardless of whether the "validated" field was checked. PBIS users were not adequately trained in what constitutes a final and closed noncompliance report.
<p>Erroneous data are captured, reported, investigated, and corrected.</p>	<ul style="list-style-type: none"> No controls established. 	<ul style="list-style-type: none"> FSIS had no programmed or manual controls in place to identify erroneous data.
<p>Review of output reports helps maintain data accuracy and validity.</p>	<ul style="list-style-type: none"> FSIS Headquarters personnel produced a report showing field computers that had not synchronized with the master database within 45 days. 	<ul style="list-style-type: none"> FSIS' process for identifying computers that do not synchronize within 45 days impedes the timeliness of the data.

Exhibit B – Agency Response

Exhibit B – Page 1 of 6



United States
Department of
Agriculture

Food Safety
and Inspection
Service

Washington, D.C.
20250

OCT 29 2004

TO: Robert W. Young
Assistant Inspector General
for Audit
Office of Inspector General

FROM: Barbara J. Masters *Wm Smith Jr*
Acting Administrator

SUBJECT: Office of Inspector General (OIG) Official Draft Audit Report – Food Safety and Inspection Service (FSIS) Application Controls – Performance Based Inspection System, Report Number 24501-01-FM

We appreciate the opportunity to review and provide comments on the subject report. FSIS generally agrees with the report's recommendations. We have several observations that we would like to make.

First, we are concerned with a serious mischaracterization made in the report regarding the Agency's operations. The report infers that inadequate controls over data entry in PBIS could ultimately lead to the occurrence of an outbreak of foodborne illness. This inaccurately suggests that the Agency's sole mechanism for enforcing its regulatory authority is accomplished based on information provided by PBIS.

FSIS inspection program personnel are aware, based on their daily inspection activities, of establishments' regulatory compliance status. The subject report suggests that noncompliance trends in PBIS, if not quickly identified and corrected, increase the likelihood of adulterated or contaminated food entering the nation's food supply. This also suggests that FSIS inspection personnel have not taken appropriate action to control any potential unsafe foods. Instructions to FSIS personnel for taking appropriate regulatory control and enforcement actions are provided in the regulations and other policy documents. PBIS data is only one of a number of data sources that the Agency uses to prompt regulatory action.

Second, FSIS has completed its formal *Security Certification and Accreditation* for all major applications, including PBIS. As a result, FSIS currently is developing a mitigation plan to address all issues identified in the certification and accreditation, including requirements for addressing system vulnerabilities. Many of the issues addressed in this report were also identified as part of the certification and accreditation process. FSIS has identified corrective actions, is working to fix system vulnerabilities, and will address any duplicative problems identified. FSIS believes that management decisions can be achieved based on our responses.

FSIS FORM 2630-9 (6/86)

EQUAL OPPORTUNITY IN EMPLOYMENT AND SERVICES

Section 1. Integrity of Data Input

1. Recommendation No. 1

Establish policies and implement stronger controls, in accordance with Departmental and Federal guidelines, in PBIS and the systems on which PBIS data reside to ensure that access is restricted to only authorized users and that legitimate users have access to only that information needed to perform their job functions.

FSIS Response

FSIS has fully deployed Windows XP on all federal inspectors' computers. Access requirements on computers with Windows XP meet departmental guidelines for password aging, length, etc. Several of the computers in the field that the OIG examined contained the Windows 95 operating system, which was not as secure as XP. Additionally, FSIS implemented mandatory online security awareness training for all users of computers. This training provides specific guidance on system security vulnerabilities, including methods for safeguarding passwords. Employees are required to complete the security awareness training by October 25, 2004.

Additionally, FSIS will develop a written policy on PBIS access control to limit and restrict access to PBIS data to only authorized users. The access control policy will ensure that guidance is provided on safeguarding passwords and that passwords meet departmental requirements. FSIS will issue this policy by January 2005.

2. Recommendation No. 2

Establish a policy on how data is to be entered into PBIS, and implement controls to ensure that all PBIS users are provided adequate training on how to enter and control data in the PBIS database.

FSIS Response

To bolster the users' understanding of entering data into PBIS, FSIS will issue a policy that provides instructions on when certain inspection information should be entered into the system. Also, FSIS plans to integrate the PBIS user's guide as an online reference guide to further assist the users. In its release of PBIS version 5.1, the online help capability will assist inspection personnel in understanding how information should be entered into the system. In addition, FSIS' Center for Learning will coordinate with the Office of Field Operations and the Chief Information Officer to provide PBIS 5.1 training.

FSIS expects to release PBIS version 5.1 by January 2005. FSIS will issue its policy document by March 2005.

3. **Recommendation No. 3**

Establish a policy and implement controls to provide reasonable assurance that only authorized and allowable data is entered into PBIS.

FSIS Response

To bolster the users' understanding of entering data into PBIS, FSIS will issue a policy that provides instructions on when certain inspection information should be entered into the system. Also, FSIS plans to integrate the PBIS user's guide as an online reference guide to further assist the users. In its release of PBIS version 5.1, the online help capability will assist inspection personnel in understanding how information should be entered into the system. In addition, FSIS' Center for Learning will coordinate with the Office of Field Operations and the Chief Information Officer to provide PBIS 5.1 training.

FSIS expects to release PBIS version 5.1 by January 2005. FSIS will issue its policy document by March 2005.

4. **Recommendation No. 4**

Establish a policy and implement controls to (1) limit changes to PBIS data, (2) require adequate justification be maintained when changes are necessary, and (3) require that all changes to PBIS data be logged.

FSIS Response

Information in PBIS can be generally categorized as incidents and profiles. Incidents describe events occurring at a discrete point in time, for example, inspections, noncompliance reports, etc. All these occur daily throughout FSIS. On the other hand, profile data is more static in nature and is not based on time or an event. Examples include Establishment Profiles, Circuit structure, District Staffing information, etc. While the information can (and does) change periodically, it's not usually changing daily. FSIS has established an IT work group that is exploring the need for locking certain types of data in the system based on the classification of the information as either an incident or profile type.

Currently, PBIS maintains a transaction history log that tracks changes made in the system, and the users who made them. Enclosure 1 contains a transaction history report for the period October 17-22, 2004.

Section 2. Data Completeness and Timeliness Critical for Effective Management

5. **Recommendation No. 5**

Implement a policy and establish controls to ensure that field inspectors synchronize inspection results daily and that all database records are accounted for during synchronization.

FSIS Response

FSIS is able to utilize data effectively from PBIS when the database is synchronized less frequently than daily. Guidance has been provided in the PBIS users' guide for inspection program personnel to conduct daily synchronization. FSIS will determine whether the guidance provided in the PBIS users' guide should be updated. FSIS will issue a policy and update the PBIS user's guide, if necessary, establishing the time requirements for synchronization.

FSIS will issue a policy on time requirements for PBIS synchronization by March 2005.

6. **Recommendation No. 6**

Implement a policy and establish controls to ensure that management reports and data analyses are generated from the most up-to-date data available.

FSIS Response

FSIS is able to utilize data effectively from PBIS when the database is synchronized less frequently than daily. Guidance has been provided in the PBIS users' guide for inspection program personnel to conduct daily synchronization. FSIS will determine whether the guidance provided in the PBIS users' guide should be updated. FSIS will issue a policy and update the PBIS user's guide, if necessary, establishing the time requirements for synchronization.

FSIS will issue a policy on time requirements for PBIS synchronization by March 2005.

Section 3. General Controls Over System Security and Development Need Strengthening

7. **Recommendation No. 7**

FSIS should establish and implement procedures to ensure that all operating systems are configured in accordance with departmental guidance and vigilantly identify and fix TCP/IP vulnerabilities on all of its systems and network devices.

FSIS Response

FSIS will establish and implement procedures to ensure that all operating systems are configured in accordance with departmental guidance and identify and fix TCP/IP vulnerabilities on all of its systems and network devices. FSIS will establish procedures by April 2005.

8. **Recommendation No. 8**

FSIS should establish and implement procedures to ensure that its firewall configuration is configured and maintained in accordance with NIST guidance.

FSIS Response

FSIS will establish and implement procedures to ensure that its firewall configuration is configured and maintained in accordance with NIST guidance. FSIS will establish firewall procedures by April 2005.

9. **Recommendation No. 9**

FSIS should document the application, data flow, and data elements of the PBIS system to provide the foundation of operational and security planning and ensure the continual operation of the system in the event of a disruption of service or turnover in staff.

FSIS Response

FSIS agrees that system documentation to assure the continuity of operation of the PBIS is important. FSIS will follow the Department's standard System Development Life Cycle (SDLC) process for documenting its information systems. A standard SDLC, in accordance with Department requirements, will be adopted for all new major system development and modifications. FSIS will utilize a contractor to document the System Development Life Cycle (SDLC) currently being used. The SDLC will be used on all new major system development and modifications. The SDLC will include: a security study, feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post implementation review. A contract to document the SDLC for all new major systems and modifications will be awarded by November 2004.

In the meantime, documentation of PBIS version 5.1 will be completed by September 2005 to address a similar issue identified in the certification and accreditation process and scheduled in FSIS' mitigation plan.

10. **Recommendation No. 10**

FSIS should establish controls to ensure that the current certification and accreditation process is performed on a 3-year basis and that security planning documents remain up-to-date are required by OMB.

FSIS Response

FSIS included, in its annual budget request, funding to provide for performing the certification and accreditation process on a 3-year basis as required by OMB.

11. **Recommendation No. 11**

Establish a policy and implement controls to ensure the proper segregation of duties over the PBIS system development, testing and production environments.

FSIS Response

FSIS is currently reorganizing the IT structure to segregate duties and responsibilities. The reorganized structure will ensure the separation of functions

Exhibit B – Agency Response

Exhibit B – Page 6 of 6

such as system development, testing, implementation, and configuration management. The reorganization is expected to be completed by January 2005.

If you have any questions, please contact Ronald F. Hicks, Assistant Administrator, Office of Program Evaluation, Enforcement and Review.

Enclosure.