Audit Report

Application Control Review of the Food and Nutrition Service’s Store Tracking and Redemption System II

Report No. 27501-02-Hy
March 2008
March 31, 2008

REPLY TO
ATTN OF:  27501-02-Hy

TO:        Roberto Salazar
           Administrator
           Food and Nutrition Service

ATTN:      Lael Lubing
           Director
           Grants Management Division
           Food and Nutrition Service

FROM:      Robert W. Young /s/
           Assistant Inspector General
           for Audit

SUBJECT:   Application Control Review of the Food and Nutrition Service’s Store Tracking and Redemption System II

This report presents the results of our Application Control Review of the Food and Nutrition Service’s Store Tracking and Redemption System II. Your written response, dated March 6, 2008, is included as Exhibit A with excerpts of your response and the Office of Inspector General’s (OIG) position incorporated into the Findings and Recommendations section of the report, where applicable.

We have reached management decision for Recommendations 1, 4, 6, 8, and 9. Please follow your agency’s internal procedures in forwarding information on final action to the Office of the Chief Financial Officer.

In order to achieve management decision on Recommendations 2, 3, 5, 7, and 10, please furnish a reply within 60 days describing the information requested in the OIG position section of the report. Please note that Departmental Regulation 1720-1 requires a management decision to be reached on all recommendations within a maximum of 6 months from report issuance and completion of final action within 12 months of management decision.

We appreciate the courtesies and cooperation extended to us by members of your staff during this audit.
Executive Summary
Application Control Review of Food and Nutrition Service’s Store Tracking and Redemption System II (Audit Report No. 27501-02-Hy)

Results in Brief

The Food and Nutrition Service (FNS) uses the Store Tracking and Redemption System II (STARS II) to store information on retailers that redeem benefits as part of the Food Stamp Program (FSP). STARS II also supports the benefit redemption activity by storing redemption data used for evaluating individual store activity. In fiscal year (FY) 2006, STARS II tracked $30 billion in food stamp redemptions and the system currently manages over 160,000 authorized FSP retailers.

We assessed whether FNS properly documented and accredited the STARS II application and instituted the necessary controls to ensure that data in the system were valid, complete, and accurately processed. We also determined whether STARS II met the security requirements of the Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources and other applicable regulations.

STARS II replaced the STARS mainframe system and received final certification and accreditation in August 2005. We concluded that FNS properly documented and accredited STARS II and established adequate application controls to ensure that the system contained valid, complete, and accurately processed data. However, we noted several weaknesses that FNS should address to further strengthen the security of STARS II. During discussions throughout the audit, FNS agreed that these weaknesses need to be corrected. FNS needs to: (1) improve security over computer resources, (2) implement actions agreed to in a prior recommendation regarding processing access requests, and (3) finalize the contingency plan for the STARS II primary computer facility, the Benefit Redemption System Branch (BRSB).

Departmental Manual (DM) 3510-001, Physical Security Standards for Information Technology (IT) Restricted Space, dated August 2004, requires the Department of Agriculture (USDA) to protect information resources through such means as layered physical security and effective security procedures and administration.

- FNS did not adequately secure computer resources for STARS II at one field office and the two computer facilities we visited. For example, we identified weak controls for monitoring physical access to restricted areas at the computer backup facility. We also found an unlocked room was used to store a server and supporting communication equipment in one

1 Retailers include grocery stores, supermarkets, meal services, farmer’s market, etc.
field office. Finally, FNS did not cleanse damaged hard drives of
sensitive data before returning the drives to the manufacturer. The data on
the hard drives included personally identifiable information (e.g.,
individual store owner names, addresses, and dates of birth) that was not
encrypted. This occurred because FNS had not implemented the
necessary procedures and controls to identify security weaknesses. As a
result, Information Technology (IT) data and resources are vulnerable to
unauthorized access.

- FNS did not implement the agreed upon corrective action associated with
a recommendation in our September 2001 report on FNS’ Security Over
IT Resources (Audit Report No. 27099-18-Hy). FNS officials explained
that other funding priorities since 2000 have prevented the agency from
implementing an automated process for system access. Most recently,
homeland security directives have taken priority. As a result, FNS has not
implemented an automated process for approving system access requests.
FNS is currently working with contractors to automate access requests.

- According to FNS officials, the BRSB did not update its contingency plan
due to staffing shortages. BRSB, within the FNS’ Information
Technology Division, manages the STARS II application. As a result,
FNS’ computer facilities are more susceptible to unknown vulnerabilities,
damage, or unplanned down time in the event of a disaster or unexpected
event. Without updates, FNS has limited assurance that operations can be
recovered in a timely manner.

The Dallas Field Office did not adhere to established procedures for
obtaining supervisory approval before authorizing stores in STARS II. This
procedure provides assurance that STARS II data is accurate. In addition, the
Dallas Field Office did not follow procedures² for reviewing system data for
significant changes. The Officer-in-Charge (OIC) cited efficiencies in having
one person enter store data in STARS II and authorize the store’s approval
before the OIC performs the supervisory review of the information. The OIC
also stated that reviewing STARS II data for significant changes was
redundant. This procedure is not redundant because it provides a second party
review to ensure that only appropriate stores are authorized. As a result, FNS
has reduced assurance that stores are appropriately authorized and reinstated
to operate in the FSP.

In February 2007, we identified that FNS had not monitored its vulnerability
scans since it implemented the FNS Universal Telecommunications Network
(UTN)³ in August 2006. DM 3530-001, USDA Vulnerability Scans

² The procedures are detailed in chapters 3 and 6 of the STARS Users Manual.
³ The purpose of the FNS UTN is to incorporate the FNS wide area network into the USDA UTN. UTN is designed to include not only the USDA Office
of the Chief Information Officer backbone, but to expand to accommodate unique needs of each agency. UTN supports multiple virtual private
networks which allow each agency (including FNS) to keep its traffic completely isolated and set up unique virtual networks over the shared physical
structure.
Procedures, dated July 20, 2005, requires USDA agencies to use scanning software to scan networks, systems and servers, on a monthly basis for all existing and new networks, systems, servers, and desktops. Although FNS received notification that the scanning was performed, a firewall in the UTN prevented FNS from receiving the results of the scanning. During this time period there were no reported security incidents. However, STARS II was vulnerable to illegal and malicious activity or exploitation by internal and external sources. FNS addressed this weakness at the time we brought it to their attention. Accordingly, we are making no additional recommendations.

**Recommendations In Brief**

FNS needs to (a) develop and implement controls to ensure only authorized individuals have physical access to restricted areas at the STARS II backup facility, (b) require the field office to mitigate the physical security weakness identified, and (c) develop and implement controls to ensure sensitive data are removed from hard drives before returning them to the manufacturer. In addition, FNS should implement an automated process for processing system access requests and approval and should update the BRSB contingency plan. Finally, FNS should instruct the Dallas Field Office to follow established procedures for authorizing stores in STARS II and reviewing system data for significant changes and ensure this instruction is followed.

**Agency Response**

FNS generally agreed with the report’s 10 recommendations. We have incorporated FNS’ response into the Findings and Recommendations section of this report, along with OIG position. FNS’ response, dated March 6, 2008, is included as exhibit A.

**OIG Position**

Based on FNS’ response, we were able to reach management decisions on Recommendations 1, 4, 6, 8, and 9. Management decisions on Recommendations 2, 3, 5, 7, and 10 can be reached once FNS has provided us with the additional information outlined in the report section, OIG Position.
### Abbreviations Used in This Report

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AO</td>
<td>Authorizing Official</td>
</tr>
<tr>
<td>BRSB</td>
<td>Benefit Redemption System Branch</td>
</tr>
<tr>
<td>DM</td>
<td>Departmental Manual</td>
</tr>
<tr>
<td>EBT</td>
<td>Electronic Benefit Transfer</td>
</tr>
<tr>
<td>FNCS</td>
<td>Food, Nutrition, and Consumer Services</td>
</tr>
<tr>
<td>FNS</td>
<td>Food and Nutrition Service</td>
</tr>
<tr>
<td>FSP</td>
<td>Food Stamp Program</td>
</tr>
<tr>
<td>FY</td>
<td>Fiscal Year</td>
</tr>
<tr>
<td>HSPD-12</td>
<td>Homeland Security Presidential Directive 12</td>
</tr>
<tr>
<td>ITD</td>
<td>Information Technology Division</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OCFO</td>
<td>Office of the Chief Financial Officer</td>
</tr>
<tr>
<td>OIC</td>
<td>Officer-in-Charge</td>
</tr>
<tr>
<td>OIG</td>
<td>Office of Inspector General</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedures</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>STARS II</td>
<td>Store Tracking and Redemption System II</td>
</tr>
<tr>
<td>SWRO</td>
<td>Southwest Regional Office</td>
</tr>
<tr>
<td>UTN</td>
<td>Universal Telecommunications Network</td>
</tr>
<tr>
<td>USDA</td>
<td>U.S. Department of Agriculture</td>
</tr>
<tr>
<td>WIC</td>
<td>Special Supplemental Nutrition Program for Women, Infants, and Children</td>
</tr>
</tbody>
</table>
# Table of Contents

Executive Summary ............................................................................................................................................ i
Background and Objectives .............................................................................................................................. 1
Findings and Recommendations ....................................................................................................................... 3

## Section 1 Security Improvements Needed ................................................................................................ 3

Finding 1 ....................................................................................................................................................... 3
  Recommendation 1 ................................................................................................................................... 6
  Recommendation 2 ................................................................................................................................... 7
  Recommendation 3 ................................................................................................................................... 8
  Recommendation 4 ................................................................................................................................... 8
  Recommendation 5 ................................................................................................................................... 8
  Recommendation 6 ................................................................................................................................... 9

## Section 2 Access Request Process Needs Improvement ........................................................................... 10

Finding 2 ....................................................................................................................................................... 10
  Recommendation 7 ................................................................................................................................... 11
  Recommendation 8 ................................................................................................................................... 11

## Section 3 Contingency Planning Needs Improvement .............................................................................. 12

Finding 3 ....................................................................................................................................................... 12
  Recommendation 9 ................................................................................................................................... 12

## Section 4 Supervisory Review of STARS II Data Needs Improvement .................................................... 14

Finding 4 ....................................................................................................................................................... 14
  Recommendation 10 ................................................................................................................................. 15

Scope and Methodology ................................................................................................................................. 17
Exhibit A – Agency Response .......................................................................................................................... 19
Background and Objectives

Background

The Food and Nutrition Service (FNS) provides needy families better access to food and a more healthful diet. The Food Stamp Program (FSP) is one of the primary Federal food assistance programs FNS uses to accomplish its mission. FSP recipients receive their program benefits through electronic benefits transfer. Once a month, each participating household receives a benefit allotment determined by the family size, household income, and other related factors. Recipients can use their benefits to pay for food items at participating retailers. Recipients use cards much like a debit card. By providing a personal identification number, recipients gain access to benefits through point of sale terminals located at approved food retailers.

The Store Tracking and Redemption System II (STARS II) stores information on the authorization, monitoring, investigation, withdrawal, and disqualification of retailer organizations that redeem food stamp benefits. STARS II also supports the benefit redemption activity by storing redemption data used for evaluating individual store activity. STARS II is located within FNS’ Information Technology Division (ITD), Benefit Redemption Systems Branch (BRSB).

STARS II replaced the STARS mainframe system and received final certification and accreditation in August 2005. STARS II is a web-based system, utilizing updated client server technology and provides user friendly access. In fiscal year (FY) 2006, STARS II tracked $30 billion in food stamp redemption activity. The system currently manages over 160,000 authorized FSP retailers. STARS II users include FNS officials responsible for FSP administration, Office of Inspector General’s (OIG) Office of Investigations, Electronic Benefit Transfer (EBT) processors and State agencies administering the FSP and the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).

STARS II interfaces with other applications and systems to provide the following types of information.

- EBT processors and States depend on STARS II to provide them with updated information on currently authorized stores.

- FNS users depend on STARS II to update their store list for the Anti-fraud Locator using the EBT Retailer Transactions system; to

---

4 Generally, States award contracts to private sector companies to develop and operate their EBT systems. These companies are usually financial institutions or other organizations that already handle debit and credit card systems or electronic funds transfer activities. However, the States remain financially liable to the Federal Government for actions of their EBT processors.
manage the retailer side of the FSP at the National, Regional, and field levels; and to provide data to respond to requests for information.

- Contractors depend on STARS II to inform them of store visit information and scheduling.
- OIG users depend on STARS II for FSP investigatory needs.
- WIC program administrators rely on STARS II information to keep current on the status of authorized stores. WIC and FSP have a reciprocal agreement concerning disqualified stores.

Objectives

Our objectives were to assess whether STARS II has been properly documented and accredited; determine if application controls assure that data are valid, complete, and accurately processed; and determine if STARS II meets the security requirements of Office of Management and Budget (OMB) Circular No. A-130, *Management of Federal Information Resources* and applicable regulations.

To accomplish these objectives, we interviewed FNS officials; reviewed applicable policies, procedures, and records; and visited the STARS II primary and backup computer facilities and two FNS field offices.
Findings and Recommendations

Section 1 Security Improvements Needed

Finding 1

FNS did not adequately secure computer resources for STARS II at one field office and the two computer facilities we visited. For example, we identified weak controls for monitoring physical access to restricted areas at the computer backup facility. Also, we found that an unlocked room was used to store a server and supporting communication equipment in one field office. Finally, FNS did not cleanse damaged hard drives of sensitive data before returning the drives to the manufacturer. This occurred because FNS had not implemented the necessary procedures and controls to identify security weaknesses and ensure sensitive data is safeguarded. As a result, IT resources are vulnerable to unauthorized access.

Departmental Manual (DM) 3510-001, Physical Security Standards for IT Restricted Space, August 2004, requires the Department of Agriculture (USDA) to protect information resources through such means as layered physical security and effective security procedures and administration. National Institute of Standards and Technology (NIST) Special Publications (SP) are a collection of documents used to assess the adequacy of system controls, and ensure compliance with established policies and operational procedures.5

We reviewed physical security controls over STARS II at the primary and backup facilities and at two field offices. The primary and back-up facilities house the STARS II application and its supporting configuration. Field offices initiate updates to the status of stores participating in the FSP. We identified weaknesses in the controls FNS used to secure facilities where STARS II resources are stored and used and to ensure sensitive data are safeguarded.

Physical Security

FNS’ controls were not effective to ensure that only authorized individuals were permitted physical access to restricted areas at the STARS II computer backup facility. The automated access system has been in place for several years and FNS acknowledged that the system is cumbersome and requires some work to produce the access list, by person and room.

- FNS granted access to its restricted computer supply room to a group of individuals identified only as “ITD Work Crew.” This group entered the

---

5 OMB Circular A-130, Management of Federal Information Resources, requires agencies to apply OMB policies and NIST guidance to achieve adequate security.
restricted room nine times during a 2–day period; however, the specific individuals who entered could not be identified. FNS created group access for convenience. FNS agreed that the best solution was eliminating group access and identifying access individually, by name. NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems* (NIST SP 800-53, Revision 1) recommends that the organization develop and keep a current list of personnel with authorized access to the facility where the information system resides and issue appropriate authorization credentials.

- FNS did not correctly program access control cards allowing unauthorized individuals to enter restricted areas. For example, a contractor had access to the backup computer facility without authorization and a card keyed for OIG staff use during fieldwork inappropriately granted access to a restricted contractor work area. We also identified a contractor who left in December 2006 but whose access rights were not removed until February 2007. FNS was unaware of the contractor’s departure until after our inquiry because the departure was not communicated to FNS. FNS acknowledged that access should not have been granted in these cases and attributed these errors to incorrect system programming and mistakes in data entry. NIST SP 800-53 Revision 1, recommends that an organization issue appropriate authorization credentials and encourages the prompt removal of personnel no longer requiring access, which mirrors guidance provided in DM 3510-001, Section 3d(2).

- The automated access control system has no audit trail for cancelled badges. FNS stated the current system is not designed to retain historical information, including the start date, expiration date, deletion date, and changes to access. Upon deletion, all records of that person are deleted. DM 3510-001, Section 3c(11) explains that access to the computer room will be electronically controlled and have the capability of providing an audit trail.

- FNS uses a manually prepared access list for the STARS II backup facility and computer supply room because the automated access system cannot readily generate an access list by door number. Our review of the current list, dated February 16, 2007, identified errors. For example, five contractors and the “ITD Work Crew” were inappropriately omitted from the list. In addition, the list did not identify which of the facility’s two rooms the individuals were authorized to access. NIST SP 800-53, Revision 1, recommends that the organization develop and keep a current list of personnel with authorized access to the facility.

- FNS did not maintain records of individuals with access to the STARS II backup facility. Copies of access authorizations were not
available for 36 of 54 individuals on the access list for the STARS II backup facility. According to FNS, they did not update their access authorizations when a new authorization procedure was implemented in 2005. This procedure utilized an e-mail request system to grant access to restricted areas. NIST SP 800-53, Revision 1, recommends that the organization develop and keep a current list of personnel with authorized access to the facility where the information system resides.

- FNS did not have documentation to support its quarterly review of the access list to the STARS II backup facility and the computer supply room. FNS stated that the review was completed through a review of an electronic file, but FNS did not annotate the file with evidence of review. A quarterly review is required by DM 3510-001, Section 3d(6).

At both the primary and back-up STARS II facility, the visitor’s log did not identify the name of the visitor’s escort. Officials at both the primary and back-up facilities agreed with our concerns and stated that they would change the visitor’s log form to identify the escort. NIST SP 800-53, Revision 1, requires the organization to maintain visitor access records to the facility where the information system resides, including the name and organization of person visited.

We identified two significant physical security weaknesses in one field office. Although this field office was located in a Federal office building, with its own access control measures, the public is granted access to the office for periodic EBT training.

- Removable door hinges faced an exterior hallway which provided the opportunity to access the field office. The public used this door to access the office for periodic EBT training. DM 3510-001, Physical Security Standards for IT Restricted Space, August 2004, section 3c(16), requires that exterior doors have either interior hinges or exterior hinges with non-removable pins.

- An unlocked room was used to store a server and supporting communication equipment for STARS II access. The door to this room had a cipher lock that was disabled with tape on both the door latch and the strike plate. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, explains most users need to understand good computer security practices such as protecting the physical area and equipment, including locking doors.

---

6 Subsequent to our visit, the field office installed a combination lock on the door.
Sensitive Data

FNS sent damaged hard drives to the manufacturer without removing sensitive data because the agency did not have the necessary equipment to cleanse the drives. The data on the hard drives included individual personally identifiable information (e.g., store owner names, addresses, and dates of birth) that was not encrypted. Once we brought this to FNS’ attention, the agency ceased returning the hard drives to the manufacturer. The Privacy Act of 1974\(^7\) requires the protection of this type of information. The hard drives also included social security numbers; however, these data were encrypted. FNS received free replacement hard drives from the manufacturer for returning the damaged hard drives.

FNS’ contract with the manufacturer did not require the manufacturer to remove data from the hard drives. FNS stated that the manufacturer refurbished and re-sold the hard drives. This issue was identified and reported in the Departmental Security Review, performed by USDA’s Office of Chief Information Officer in April 2007. FNS agreed that a computer forensic expert could recover the individual data from the hard drives after the drives had left FNS’ control. FNS agreed with this issue and ordered degaussing equipment to remove all data from the hard drives. Until the degaussing equipment arrives, FNS plans to destroy the damaged hard drives, instead of returning them to the manufacturer.

FNS needs to implement the necessary procedures and controls to improve the security of computer resources for STARS II at the field office and two computer facilities that we visited. These improvements need to address weaknesses in controls FNS used to secure facilities where STARS II resources are stored and used and to ensure sensitive data are safeguarded.

Recommendation 1

Develop and implement controls to ensure only authorized individuals have access to restricted areas. These controls, at a minimum, should: (a) address how individuals are authorized access to restricted areas, (b) prohibit providing access to groups of individuals, and (c) detail procedures for timely revising and deleting authorizations.

Agency Response.

The Food, Nutrition, and Consumer Services (FNCS) Information Systems Security Guidelines and Procedures Handbook (FNCS-702) was published and distributed to all users on January 31, 2008. Section 700 of the

---

\(^7\) The Privacy Act of 1974 requires that Federal agencies not disclose any record of information about an individual by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.
Handbook, **Guidance on IT Restricted Space and Physical Access Control**, clearly defines requesting, deleting, and auditing access to restricted space.

An FNS-767, FNS IT Restricted Space Access Control Form, will be completed by March 14, 2008, and approved for each individual with access to IT restricted space. Visitors must sign in and be escorted at all times by an individual who has a completed and approved FNS-767 on file.

As of March 17, 2008, the Property Management Branch will maintain all user access requests to IT restricted space by generating weekly reports of user access and performing audits for unauthorized access; remove access for users who have been inactive for 90 days; remove all access for users who have been terminated: FNCS employees, contractors and others who are no longer at FNCS; ensure that all user access requests to IT restricted spaces meet the appropriate security standards required to receive access; block access to IT restricted space for those individuals who lack the required security authorization; and perform user recertification quarterly.

**OIG Position.**

We accept FNS’ management decision.

**Recommendation 2**

Develop and implement a system for generating an accurate list of individuals who have access to restricted physical areas. This system should provide an audit trail with historical data on how individual authorizations were revised or deleted.

**Agency Response.**

MDI software, by virtue of design, cannot provide this type of information automatically. At this time, FNS can generate the OIG requested files manually, FNS will be implementing Departmental issued Homeland Security Presidential Directive-12 (HSPD-12) compliant software. HSPD-12 card readers have been installed in preparation for the new software.

**OIG Position.**

To reach management decision, FNS needs to state whether the new access system required by HSPD-12 will provide the automated access list and audit trail lacking in the current MDI system. In addition, FNS needs to provide the expected timeframes for implementing the HSPD-12 compliant software.
Recommendation 3

Develop and implement controls to ensure that the quarterly review of the access list to restricted rooms is documented.

**Agency Response.**


Please see FNS Response for Recommendation 1.

**OIG Position.**

We agree with FNS’ proposed corrective action, however, to reach management decision, FNS needs to state whether the controls to ensure the quarterly reviews are documented is included in Section 700 of the FNCS-702 Handbook.

Recommendation 4

Revise the visitor logs to identify the visitor’s escort.

**Agency Response.**

The Visitor Log was modified in August 2007 to include visitor escort in Minneapolis and Alexandria prior to completion of the OIG audit.

**OIG Position.**

We accept FNS’ management decision.

Recommendation 5

Require the field office to mitigate the physical security weaknesses identified (e.g., properly locking the computer room and ensuring that exterior door hinges impede access to the office).

**Agency Response.**

As of February 27, 2008, the physical security requirements noted in the recommendation have been implemented in the computer rooms in Minneapolis and Alexandria that house STARS server components. There are no STARS server components or computer rooms in any FNS Field Office.
OIG Position.

While there are no STARS II server components or computer rooms in FNS field offices, the field offices provide support for managing the benefit redemption function, and STARS provides automated support for this function. The field office could be compromised because an unlocked room was used to store a server and supporting communication equipment for STARS II access. In addition, removable door hinges faced an exterior hallway which provided opportunity to access the field office. The public used this door to access the office.

To reach management decision, FNS needs to require the field office to mitigate the physical security weaknesses identified.

Recommendation 6

Develop and implement controls to ensure that sensitive data are removed from damaged hard drives before these drives are returned to the manufacturer.

Agency Response.

As of January 31, 2008, FNS had implemented procedures to ensure that all equipment is degaussed before being disposed of. FNCS-702 Handbook, Section 1542, SDLC Phases and Detailed Security Requirements for each Phase, Part 5c and 5d, covers degaussing.

FNS has procured [ ], to ensure that sensitive data are removed from damaged or excess hard drives. All equipment is degaussed before being disposed of.

OIG Position.

We accept FNS’ management decision.
Finding 2

FNS did not implement the agreed upon corrective action associated with a recommendation in our September 2001 report on FNS’ Security Over IT Resources (Audit Report No. 27099-18-Hy). FNS officials explained that other funding priorities since 2000 have prevented the agency from implementing an automated process for system access. Most recently, homeland security directives have taken priority. As a result, FNS had not implemented an automated process for approving system access requests. FNS is currently working with contractors to automate access requests.

In our prior report, we recommended that FNS establish controls to ensure the security office maintains and utilizes a master list of current users by system. In response, FNS agreed to implement an automated process for computer access requests for all FNS systems, to be implemented by December 31, 2001. The automated process will be based on the Form FNS-674, Computer System Access Request, which is currently still in use.

FNS reported that implementing the automated system has been part of its plans since 2000, but due to funding issues, it did not occur. The most recent funding priority was the completion of Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. Currently, FNS has funding for the automated process and, as of June 2007, FNS was working with contractors to test the new system. As of January 2008, the new system had not been implemented.

FNS Handbook 702, FNS Information Systems Security Standards and Procedures, June 2002, requires the use of Form FNS-674, Computer System Access Request, for all system access including STARS II. FNS Handbook 702 requires supervisory approval for system access; however, the level of approval is unclear. FNS developed a procedure to use Regional approval officials; however, this was not incorporated into practice. The approval evolved into a centralized approval process. Currently, FNS-674s are being approved centrally by a single authorizing official (AO) for the over 700 STARS II users nationwide. However, FNS recognizes that a single approving official cannot knowledgeably assess individual needs for system access. FNS plans to have 7 Regional AO’s who will approve access requests within their regional offices and field offices.

---

8 HSPD-12, effective August 2004, requires a common identification standard for Federal employees and contractors and includes the completion of background investigations for those who require long-term access to federally controlled facilities and/or information systems.
Recommendation 7

Develop and implement an automated process for system access requests and approval.

Agency Response.

The Office of Information Technology is in the process of completing work on an automated system for access requests and approvals for STARS. The system will be rolled out to the user community no later than March 3, 2009.

OIG Position.

We agree with FNS’ proposed corrective action; however, we cannot accept management decision. FNS originally agreed to implement the new system by December 31, 2001. In June 2007, FNS officials told us the agency was working with contractors to test the new system. To reach management decision, FNS needs to provide specific implementation milestones to rollout the system to the user community by March 2009.

Recommendation 8

Update FNS Handbook 702 to reflect changes in the STARS II approval process, which implements the use of regional AO’s.

Agency Response.

Standard Operating Procedures (SOP) are being created for User Access Request for all FNCS Systems. The SOP for STARS II will address the approval process implementing the use of Regional Authorizing Officials. Estimated completion dated June 1, 2008.

OIG Position.

We accept FNS’ management decision.
Finding 3

BRSB did not update the overall contingency plan for the IT center where STARS II is located. According to FNS officials, this was caused by staffing shortages. As a result, FNS’ computer facilities are more susceptible to damage or unplanned down time in the event of a disaster or unexpected event. Without an updated contingency plan, FNS has limited assurance that operations can be recovered in a timely manner.

NIST SP 800-34, *Contingency Planning Guide for IT Systems*, June 2002, requires a set of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization’s IT systems.

BRSB provides primary support for the STARS II application. In April 2007, FNS successfully completed a full recovery test of STARS II and revised the application portion of the contingency plan. BRB developed the STARS II Contingency Plan as a key element of BRB’s overall contingency plan, which includes the continuity of operations plan.

BRB’s overall contingency plan included an outdated system description that references old equipment and platforms, an outdated damage assessment team that reflects former BRB personnel, and an outdated sequence of recovery operations that references an outdated telecommunications network. FNS explained that it had been short staffed for an extended period and did not have an opportunity to review and update the plan. At the exit conference to discuss the results of our review in January 2008, FNS officials explained that the agency is still in the process of updating the BRB contingency plan.

**Recommendation 9**

Finalize the BRB’s overall contingency plan to update such things as system descriptions, assessment team members, and the sequence of recovery operations.

**Agency Response.**

The BRB contingency plan is a living document and updated continually. The next revision will be completed by May 1, 2008. The plan must conform to all USDA Office of the Chief Information Officer templates and standards in order to fulfill existing departmental requirements. These requirements include: Introduction, Concept of Operations, Notification and Activation Phase, Recovery Phase, Reconstitution Phase, Testing, Training and Exercise, and Plan Maintenance. System Descriptions and Assessment Teams are located in the Concepts of Operations Section. Operations are defined in the Recovery Phase Section.
OIG Position.

We accept FNS’ management decision.
Section 4 Supervisory Review of STARS II Data Needs Improvement

Finding 4

The Dallas Field Office did not adhere to established procedures for obtaining supervisory approval before authorizing stores in STARS II. This procedure provides assurance that STARS II data is accurate. In addition, the Dallas Field Office did not follow procedures for reviewing system data for significant changes. The Officer-in-Charge (OIC) cited efficiencies in having one person enter store data in STARS II and authorize the store’s approval before the OIC performs the supervisory review of the information. The OIC also stated that reviewing STARS II data for significant changes was redundant. This procedure is not redundant because it provides a second party review to ensure that only appropriate stores are authorized. As a result, FNS has reduced assurance that stores are appropriately authorized and reinstated to operate in the FSP. We identified 7 of 15 newly authorized and reinstated stores within the Dallas Field Office without documentation of supervisory approval, which places FNS at risk of allowing stores to operate in the FSP without approval.

To test the processes used for entering data in STARS II and verifying data accuracy, we reviewed supporting records for retailer actions entered into STARS II by two FNS field offices. The retailer actions included such things as new authorizations, withdrawals, and disqualifications. Supporting records include hard copy case files and queries of STARS II. This review was conducted to evaluate the timeliness and accuracy of actions entered into STARS II.

The OIC of the Dallas Field Office allowed Program Specialists to enter and authorize store information in STARS II. However, the STARS II User Manual, Chapter 3, requires that stores should be approved by the OIC before the stores are authorized in STARS II.9 The user manual includes an Application Workflow Diagram that illustrates that after data entry and examination of the related documentation, the final application package should be submitted to the OIC for review and approval. For our sample of 15 newly authorized and reinstated stores in the Dallas Field Office,10 we identified 7 without documentation of supervisory approval. In response to our inquiries, the OIC explained that supervisory review and approval occurred after the Program Specialists entered and authorized store information in STARS II. The OIC explained that she considered this to be a more efficient process. The Dallas Field Office is responsible for over

---

9 The procedures allow the OIC to designate a Program Specialist with the authority to approve stores in place of the OIC. The OIC of the Dallas Field Office did not designate someone with this authority.

10 We randomly selected 15 newly authorized and reinstated retailers from a universe of 297 stores and a universe of 1 meal service for the period of October 1, 2006 through April 20, 2007. The sample consisted of 9 newly authorized stores, 1 newly authorized meal service, and 5 reinstated stores. We selected the greater of 5 retailers or 5 percent of each universe. If the universe consisted of fewer than 5 retailers, we selected all the retailers for review.
5,000 stores currently authorized in STARS II, approximately 3 percent of all stores authorized in FY 2007.

Post approval of new authorizations places FNS at risk of allowing stores to operate in the FSP without approval. In March 2007, BRSB began printing and mailing the authorization letters and cards the day after stores were authorized in STARS II. As a result, authorization letters and cards could be mailed to stores before they have been approved by the OIC. In addition, STARS II sends EBT processors daily updates of store actions, including newly authorized and reinstated stores. The EBT processors use the information to identify the new stores that need food stamp redemption equipment. We found that the OIC in the Dallas Field Office reviewed and approved one new authorization 7 days after the store had been authorized in STARS II. The OIC could not explain why the review took this long. In contrast, the OICs in the New York City Field Office reviewed and approved new stores prior to the stores being authorized in STARS II. The New York City Field Office is responsible for over 8,000 currently authorized stores, or approximately 5 percent of all stores authorized in FY 2007.

The STARS II User Manual, chapter 6, section 6.5.9, requires each OIC to run the monthly Supervisory Store/Meal Service Report, for the purpose of reviewing significant data changes, specifically new store authorizations, as a second party to ensure that only the appropriate stores are authorized to accept food stamp program benefits. The OIC for the Dallas Field Office informed us that this report was not reviewed; adding that it was redundant. This review is not redundant because the monthly review of the Supervisory Store/Meal Service Report provides a second party review to ensure that only appropriate stores are authorized. This control was put in place in response to a prior OIG audit recommendation.

**Recommendation 10**

Instruct the Dallas Field Office to follow established controls for authorizing stores in STARS II and reviewing system data for significant changes and ensure the controls established in the STARS II User Manual are followed.

**Agency Response.**

On February 29, 2008, FNS forwarded a reminder of proper procedures to the Southwest Regional Office (SWRO) Acting Director of Field Operations. The agency indicated that it had reviewed the draft audit report and explained that the purpose of the audit was to assess whether FNS properly documented and accredited the STARS II application and instituted the necessary controls to ensure that data in the system were valid, complete, and accurately processed.
FNS specified that the report included information regarding the lack of adherence of the Dallas Field Office to established procedures for obtaining supervisory approval before authorizing stores in STARS II. FNS clarified that the purpose of its memorandum was to inform the SWRO of this finding and to request that the Field Office Director remind all of the OIC’s, particularly the OIC of the Dallas Field Office, that it is imperative that established controls for authorizing stores in STARS II and reviewing system data for significant changes be completed. FNS reiterated that Section 6.5.8 of the STARS II User Manual requires that each OIC run the monthly Supervisory Store/Meal Service Report (253-L) for the purpose of reviewing significant data changes, specifically new store authorizations, as a second party to ensure that only the appropriate stores are authorized to accept program benefits. FNS also reminded them that this control was put in place in response to a prior OIG audit recommendation. As specified in the STARS II User Manual, this report is mandated and is required to be run by each OIC by the 15th of each month.

**OIG Position.**

We agree with FNS’ corrective action; however, to reach management decision, FNS needs to describe how it will ensure controls established in the *STARS II User Manual* are followed.
Scope and Methodology

Our review was performed to assess whether the STARS II has been properly documented and accredited; determine if application controls assure that data are valid, complete, and accurately processed; and determine if STARS II meets the security requirements of OMB Circular No. A-130, Management of Federal Information Resources and applicable regulations. Our reviewed covered STARS II operations in FY 2007; however, system documentation and related activities from prior years were reviewed as needed.

We performed onsite fieldwork at FNS headquarters in Alexandria, Virginia; the BRSB in Minneapolis, Minnesota; and FNS field offices in New York, New York, and Dallas, Texas. To accomplish our objectives, we did the following:

- Interviewed FNS officials responsible for managing STARS II at the BRSB in Minneapolis, Minnesota (the primary computer facility) and FNS headquarters in Alexandria, Virginia (the backup computer facility).

- Reviewed agency, Departmental, and other federally mandated IT security polices and procedures.

- Interviewed FNS officials responsible for entering store authorization data at field offices in New York, New York and Dallas, Texas.

- Performed testing of the STARS II to ensure data were valid, complete, and accurate. This included reviewing documentation to support updates to store authorizations and daily transmission of this data between STARS II and EBT retailers. We also validated daily redemption data sent from EBT retailers to STARS II.

- Performed testing of STARS II to ensure compliance with security requirements for such things as physical security, access to systems, and encryption.

In FY 2006, STARS II tracked $30 billion in food stamp redemption activity. STARS II currently manages over 160,000 authorized FSP retailers. To accomplish our work, we visited the New York City and Dallas Field Offices. We selected these offices for review based on the number of authorized stores they managed for FY 2007. The New York City Field Office managed over 8,000 currently authorized stores, or approximately 5 percent of all stores authorized in FY 2007. The Dallas Field Office managed over 5,000 stores, or 3 percent of all stores authorized in FY 2007.
Audit fieldwork was performed from January to August 2007. We conducted this performance audit in accordance with *Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.
Exhibit A – Agency Response

MAR - 6 2008

“Application Control Review of the Food and Nutrition Service’s Store
Tracking and Redemption System II”

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

This responds to Official Draft Report # 27501-02-Hy. The Food and Nutrition Service
(FNS) offers the following information in response to each OIG recommendation and
requests acceptance of management’s decisions.

Recommendation 1 – Develop and implement controls to ensure only authorized
individuals have access to restricted areas. These controls, at a minimum, should:
(a) address how individuals are authorized access to restricted areas, (b) prohibit
providing access to groups of individuals, and (c) detail procedures for timely
revising and deleting authorizations.

FNS Response

The FNCS Information Systems Security Guidelines and Procedures Handbook (FNCS-
702) was published and distributed to all users on January 31, 2008. Section 700 of the
Handbook, Guidance on IT Restricted Space and Physical Access Control, clearly
defines requesting, deleting, and auditing access to IT Restricted Space.

An FNS-767 FNS IT Restricted Space Access Control Form will be completed by March
14, 2008, and approved for each individual with access to IT Restricted Space. Visitors
must sign in and be escorted at all times by an individual who has a completed and
approved FNS-767 on file.

As of March 17, 2008, the Property Management Branch will maintain all user access
requests to IT restricted space by generating weekly reports of user access and
performing audits for unauthorized access; remove access for users who have been
inactive for 90 days; remove all access for users who have been terminated: FNCS
employees, contractors and others who are no longer at FNCS; ensure that all user access
requests to IT restricted spaces meet the appropriate security standards required to receive
access; block access to IT restricted space for those individuals who lack the required
security authorization; and perform user recertification quarterly.

Recommendation 2 - Develop and implement a system for generating an accurate
list of individuals who have access to restricted physical areas. This system should
provide an audit trail with historical data on how individual authorizations
were revised or deleted.

AN EQUAL OPPORTUNITY EMPLOYER
OIG Audit
Page 2

FNS Response

MDI software, by virtue of design, cannot provide this type of information automatically. At this time, FNS can generate the OIG requested files manually. FNS will be implementing Departmental issued HSPD-12 compliant software. HSPD-12 card readers have been installed in preparation for the new software.

Recommendation 3 - Develop and implement controls to ensure that the quarterly review of the access list to restricted rooms is documented.

FNS Response

The FNCS-702 Handbook was published and distributed to all users on January 31, 2008. Section 700 of the Handbook, Guidance on IT Restricted Space and Physical Access Control, clearly defines requesting, deleting, and auditing access to IT Restricted Space.

Please see FNS Response for Recommendation 1.

Recommendation 4 - Revise the visitor logs to identify the visitor's escort.

FNS Response

The Visitor Log was modified in August 2007 to include visitor escort in Minneapolis and Alexandria prior to completion of the OIG Audit.

Recommendation 5 - Require the field office to mitigate the physical security weaknesses identified (e.g., properly locking the computer room and ensuring that exterior door hinges impede access to the office).

As of February 27, 2008, the physical security requirements noted in the recommendation have been implemented in the computer rooms in Minneapolis and Alexandria that house the STARS server components. There are no STARS server components or computer rooms in any FNS Field Office.

Recommendation 6 - Develop and implement controls to ensure that sensitive data are removed from damaged hard drives before these drives are returned to the manufacturer.

FNS Response

As of January 31, 2008, FNS has implemented procedures to ensure that all equipment is degaussed before being disposed of. FNCS-702 Handbook, Section 1542, SDLC Phases
and Detailed Security Requirements for each Phase, Part 5c and 5d, covers degaussing.

FNS has procured [ ], to ensure that sensitive data are removed from damaged or excess hard drives. All equipment is degaussed before being disposed of.

Recommendation 7 - Develop and implement an automated process for system access requests and approval.

FNS Response

The Office of Information Technology is in the process of completing work on an automated system for access requests and approvals for STARS. The system will be rolled out to the user community no later than March 3, 2009.

Recommendation 8 - Update FNS Handbook 702 to reflect changes in the STARS II approval process, which implements the use of Regional AO's.

FNS Response

Standard Operating Procedures (SOP) are being created for User Access Requests for all FNCS systems. The SOP for STARS II will address the approval process implementing the use of Regional Authorizing Officials. Estimated completion date is June 1, 2008.

Recommendation 9 - Finalize the BRSB's overall contingency plan to update such things as system descriptions, assessment team members, and the sequence of recovery operations.

FNS Response

The Benefit Redemption Systems Branch (BRSB) contingency plan is a living document and updated continually. The next revision will be completed by May 1, 2008. The plan must conform to all USDA OCIO templates and standards in order to fulfill existing departmental requirements. These requirements include: Introduction, Concept of Operations, Notification and Activation Phase, Recovery Phase, Reconstitution Phase, Testing, Training and Exercise, and Plan Maintenance. System Descriptions and Assessment Teams are located in the Concepts of Operations Section. Operations are defined in the Recovery Phase Section.

Recommendation 10 - Instruct the Dallas Field Office to follow established controls for authorizing stores in STARS II and reviewing system data for significant changes and ensure the controls established in the STARS II User Manual are followed.
OIG Audit
Page 4

On February 29, 2008, we forwarded a reminder of proper procedures to the Southwest Regional Office (SWRO) Acting Director of Field Operations. We indicated that we had reviewed the draft audit report and explained that the purpose of this audit was to assess whether FNS properly documented and accredited the STARS II application and instituted the necessary controls to ensure that data in the system were valid, complete and accurately processed.

We specified that the report included information regarding the lack of adherence of the Dallas Field Office to established procedures for obtaining supervisory approval before authorizing stores in STARS II. We clarified that the purpose of our memorandum was to inform the SWRO of this finding and to request that the Field Office Director remind all of the Officers-in-Charge (OICs), particularly the OIC of the Dallas Field Office, that it is imperative that established controls for authorizing stores in STARS II and reviewing system data for significant changes be completed. We reiterated that Section 6.5.8 of the STARS II User Manual requires that each OIC run the monthly Supervisory Store/Meal Service Report (253-L) for the purpose of reviewing significant data changes, specifically new store authorizations, as a second party to ensure that only the appropriate stores are authorized to accept program benefits. We also reminded them that this control was put in place in response to a prior OIG audit recommendation. As specified in the STARS II User Manual, this report is mandated and is required to be run by each OIC by the 15th of each month. We have attached the memorandum to this response.

[Signature]
Roberto Salazar
Administrator

Attachment
February 29, 2008

"Application Control Review of the Store Tracking and Redemption  
System (STARS) II"

To: Ron Gwinn, Acting Director of Field Operations  
Southwest Regional Office  
Food and Nutrition Service

We are in the process of reviewing and commenting on the subject draft audit report. The purpose of this audit was to assess whether FNS properly documented and accredited the STARS II application and instituted the necessary controls to ensure that data in the system were valid, complete and accurately processed.

Included in the subject report is information regarding the lack of adherence of the Dallas Field Office to established procedures for obtaining supervisory approval before authorizing stores in STARS II. The purpose of this memorandum is to inform you of this finding and to request that you remind all of the Officers-in-Charge (OICs), particularly the OIC of the Dallas Field Office, that it is imperative that established controls for authorizing stores in STARS II and reviewing system data for significant changes be completed. Section 6.5.8 of the STARS II User Manual requires that each OIC run the monthly Supervisory Store/Meal Service Report (253-L) for the purpose of reviewing significant data changes, specifically new store authorizations, as a second party to ensure that only the appropriate stores are authorized to accept program benefits. This control was put in place in response to a prior OIG audit recommendation. As specified in the STARS II User Manual, this report is mandated and is required to be run by each OIC by the 15th of each month.

Thank you in advance for ensuring that each of the OICs comply with the procedures established for obtaining supervisory approval before authorizing stores in STARS II. We appreciate your cooperation.

Andrea Gold, Chief  
Retailer Management and Issuance Branch  
Benefit Redemption Division