U.S. Department of Agriculture
Office of Inspector General
Midwest Region
Audit Report

CONTROLS OVER THE ACCESS, DISCLOSURE, AND USE OF SOCIAL SECURITY NUMBERS

Report No.
27601-29-Ch
FEBRUARY 2003

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: February 26, 2003

REPLY TO
ATTN OF: 27601-0029-CH

SUBJECT: Controls Over The Access, Disclosure, and Use of Social Security Numbers

TO: Roberto Salazar
Administrator
Food and Nutrition Service

ATTN: Lael Lubing
Director, Grants Management Division

This report presents the results of our audit of the Controls Over the Access, Disclosure, and Use of Social Security Numbers. The Food and Nutrition Service's responses to the official draft, dated January 16 and 21, 2003, are included in their entirety as exhibits B and C, with excerpts and the Office of Inspector General's position incorporated into the Findings and Recommendations section of the report.

Based on the information contained in the responses, we have reached management decisions on Recommendations Nos. 2, 4 and 5 in the report. Please follow your agency's internal procedures in forwarding documentation for final action to the Office of the Chief Financial Officer. We have not reached management decision on Recommendations Nos. 1 and 3. Management decisions can be reached when the Food and Nutrition Service provides the additional information outlined in the OIG Position sections of the report.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective action taken or planned and the timeframes for implementation of those recommendations for which management decision has not yet been reached. Please note that the regulation requires that management decisions be reached on all findings and recommendations within a maximum of 6 months from the date of report issuance, and final action to be taken within 1 year of each management decision.

/s/

RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

CONTROLS OVER THE ACCESS, DISCLOSURE AND USE OF SOCIAL SECURITY NUMBERS

AUDIT REPORT NO. 27601-29-Ch

RESULTS IN BRIEF

This report presents the results of our audit of the Controls Over Access, Disclosure, and Use of Social Security Numbers (SSN's). We performed this audit in conjunction with the President's Council on Integrity and Efficiency (PCIE). The Social Security Administration's (SSA) Office of Inspector General was the lead agency coordinating the audit. The audit was based on a Government Accounting Office study to determine how and to what extent Federal, State, and local Government agencies use individuals' SSN's and how they safeguard records and documents containing SSN's. The objective of our audit was to assess the controls over the disclosure and use of SSN's by third parties in the Food Stamp Program (FSP), one of the largest USDA programs using SSN's.

Our audit disclosed that Food and Nutrition Services' (FNS) controls over the disclosure of SSN's to third parties, contractors' access and use of SSN's, requirements placed on entities receiving SSN's, and direct access to SSN's by other organizations were in place and functioning. However, we found several instances at the State and county level where controls over computer access and physical access of SSN's needed strengthening. Specifically, the States needed to limit access to SSN's and prevent the possibility of identity theft from unauthorized disclosure of FSP SSN's located in computer files or on written documents. We noted that two of four county offices visited had control weaknesses that allowed access to SSN's through the computer system. We also noted that case files in two county offices were kept in unlocked drawers, file cabinets, and boxes.

KEY RECOMMENDATIONS

We recommended that guidance be issued to the Food and Nutrition Service Regional Office and State offices concerning access to confidential information in FSP databases, and that confidential information be secured according to internal procedures.

AGENCY RESPONSE

FNS' responses to the official draft report, dated January 16 and 21, 2003, generally agreed with the audit findings and recommendations.

OIG POSITION

Based on the FNS' responses, management decisions can be reached on Recommendations Nos. 2, 4, and 5. Management decisions can be reached on the Recommendations Nos. 1 and 3 once FNS has provided us with the information specified in the OIG Position sections of the report. We have incorporated applicable portions of FNS' responses, along with our position, in the Findings and Recommendations section of the report. FNS' responses to the official draft report are included in their entirety as exhibits B and C of the audit report.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The Food Stamp Program (FSP) is administered by the Food and Nutrition Service (FNS) through 7 Regional Offices, and in cooperation with 53 State welfare agencies. Through the State agencies, the FSP provides benefits to low-income people to buy eligible food in authorized retail food stores. In Fiscal Year (FY) 2001, the FSP provided benefits to 7.5 million households and 17.3 million individuals each day. Individuals must complete an application and meet certain income and resource criteria to receive benefits. It is through the application process that States obtain, verify, and maintain personal information for each applicant, including the social security numbers (SSN) for each household member participating in the FSP.

Due to concerns over the widespread collection and sharing of personal information, and occurrences of identity theft, Congress asked the Government Accounting Office (GAO) to study how and to what extent Federal, State, and local government agencies use individuals' SSN's and how they safeguard records and documents containing SSN's. The expanded use of the SSN as a national identifier provides a tempting motive for many unscrupulous individuals to acquire a SSN and use it for illegal purposes. While no one can fully prevent SSN misuse, Federal agencies have some responsibility to limit the risk of unauthorized disclosure of SSN information. In response, the Chairman of the House Ways and Means Subcommittee on Social Security asked the Social Security Administration and the President's Council on Integrity and Efficiency (PCIE) to look across Government at the way Federal agencies disseminate and control the use of SSN information to third parties.

As a result of this request, the U.S. Department of Agriculture's (USDA) Office of Inspector General (OIG) initiated an audit of controls over the access, disclosure, and use of SSN's in the FSP, one of the largest USDA programs to use SSN's. The Privacy Act[1] and other statutes regulate FNS' use of SSN's, while State agencies are responsible for administering the FSP in accordance with the Food Stamp Act[2], Federal regulations[3], and their FNS approved Plans of Operation[4].

[1] The Privacy Act of 1974, 5 U.S.C. §552A as amended
[2] The Food Stamp Act of 1977, 7 U.S.C. 2020
[3] 7 CFR Parts 271 through 283
[4] The Food Stamp Act of 1977, 7 U.S.C. 2020(d)

Specifically, with regard to collecting SSN information, Section 7 of the Privacy Act requires any agency which requests an individual to disclose his/her SSN to inform them whether the disclosure is mandatory or voluntary, by what statutory authority or other authority the request is made, and how the agency will use the number. With regard to disclosures of SSN's contained in Federal record systems (i.e., records maintained on individuals), the Privacy Act controls the use and disclosure of such personal information, but without specifically addressing SSN's. For each record system maintained by an agency, a Privacy Act notice must be published. The notice must contain the routine uses and disclosures of that system's information, which will include the SSN if relevant.

The Food Stamp Act of 1977, which governs the States, mirrors the Privacy Act. The Food Stamp Act requires disclosure of SSN's of all household members as a condition of eligibility for participation in the FSP, and the State agencies are authorized to use those SSN's in the administration of the FSP. Regulations require that each application form notify households how their information and SSN will be used[5]. The Food Stamp Act requires that States, through their Plans of Operation, provide safeguards that limit the use or disclosure of information obtained from the applicant households and enforcement of the provisions of this act[6].

Additionally, the Food and Agricultural Resources Act of 1990 (P.L.101-624), Section 1735, requires a SSN for the officers of food and retail stores that redeem food stamps, and provides that the SSN's maintained will be confidential and may not be disclosed.

OBJECTIVES

Our objective was to assess the controls over the access, disclosure, and use of SSN information by third parties. Specifically, we determined whether the FSP as a whole: (1) Makes legal and informed disclosures of SSN's to third parties; (2) has appropriate controls over contractors' access and use of SSN's; (3) has appropriate controls over other entities' access and use of SSN's; and (4) has adequate controls over access to individuals' SSN's maintained in its databases.

SCOPE

We performed audit work at the FNS National Office in Alexandria, Virginia, and the FNS Midwest Regional Office in Chicago, Illinois. We judgmentally selected State offices for testing including one where the FSP is State administered (Illinois) and

[5] 7 CFR, Subtitle B, Chapter II, Part 273.2(b)(4)
[6] The Food Stamp Act of 1977, 7 U.S.C. 2020(e)(8)

one where the FSP is county administered (Wisconsin). Within each State, we judgmentally selected 2 county or local offices, hereinafter referred to as county offices, based on location and size. (See exhibit A.)

We followed the audit guide set forth by the Social Security Administration (SSA) Office of Inspector General. This guide focused on the 4 sections in the GAO program questionnaire completed by the FSP offices. The sections included questions numbered 39 through 63 and covered the following four areas: (1) Disclosures of individuals' SSN's to third parties; (2) controls over contractors' access and use of SSN's; (3) requirements placed on entities receiving SSN's; and (4) controls over direct access to individuals' SSN's by other organizations.

Our audit primarily covered calendar year 2001. However, calendar year 2002 data was reviewed where deemed necessary to accomplish the audit objectives. Our audit work was conducted from March 5 through May 20, 2002.

We conducted the audit in accordance with Government Auditing Standards established by the Comptroller General of the United States for performance audits.

METHODOLOGY

To accomplish our objectives we:

- Reviewed Federal laws and regulations related to the collection, use and privacy of SSN's, including the Privacy Act and Food Stamp Act.
- Reviewed the State Plans of Operation, for the selected States.
- Reviewed applicable State policies, procedures, and rules and regulations governing the proper safeguarding of confidential information.
- Reviewed controls over the disclosure of, and access to, SSN information.
- Reviewed contracts or memoranda of understanding with third party contractors and subcontractors.
- Reviewed the controls over the destruction of sensitive information.
- Observed the physical security over sensitive information at the State and county offices.

- Interviewed agency officials responsible for controlling SSN disclosure and access.

- Verified and updated key pieces of information provided on the GAO questionnaires by FSP offices.

- Obtained documentation supporting FSP offices' answers to the GAO questionnaire, questions 39 through 63.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1 SAFEGUARDING OF SOCIAL SECURITY NUMBERS

We found several instances at the county level where confidential information, such as Social Security numbers (SSN's), of Food Stamp Program (FSP) applicants and participants were not sufficiently safeguarded to protect against unauthorized use or disclosure. We noted weaknesses in the controls over both computer access and physical access, which are intended to safeguard the confidentiality and misuse of FSP participants' SSN's. As a result, the SSN's are susceptible to theft and unauthorized use.

FINDING NO. 1

COMPUTER ACCESS TO SOCIAL SECURITY NUMBERS WAS NOT ADEQUATELY SAFEGUARDED

We found that computer users in two of four county offices reviewed had inappropriate access to SSN's due to weaknesses in the controls over the granting and monitoring of computer access. As a result, SSN's were not adequately safeguarded and kept confidential, which created the potential for the use of SSN's in identity theft.

The Food Stamp Act requires State safeguards limiting the use and disclosure of FSP information. Additional regulations require States to have computer model plans,[7] which maintain appropriate levels of confidentiality of program information.

We obtained State security office lists of computer users in the two State and four county offices tested. Included on the lists were State and county office employees, outside contractors or subcontractors, and other third parties, such as outside researchers. We included users with access to the outside electronic benefits transfer system and to State systems. We interviewed employees and contractors, spoke with county security officials who approved access requests, State security officials who implemented requests, and obtained information about specific job duties to determine whether access was properly authorized and appropriately limited to users' duties on a need to know basis only.

Based on our review, we found examples of access granted to those who were not authorized under Wisconsin State policy to use State or Social

[7] 7 CFR 272.10(b)(3)(iii)

Security Administration (SSA) databases containing individuals' SSN's, and found examples where access levels exceeded those necessary to perform job duties. For instance, in one county we determined that the security officer did not adequately review the computer access request forms, which were then forwarded to the State security office for activation. In addition, the State relied solely on the computer access form, which did not provide sufficient information or was not correctly completed for the State to determine if the access requested was appropriate. The State informed us that they generally rely on the county security officers' signature as proof that a request for access is valid; therefore, unless a request is grossly inappropriate it will be activated. We also noted that the State security office does not periodically review or monitor current employees', contractors' or subcontractors' computer access on a regular basis to ensure that access and security levels were accurate and updated properly and promptly. As a result of the various exceptions of inappropriate access, there is the potential for theft and unauthorized use of SSN's.

At the same county office as above, we judgmentally selected 24 of the county office's 143 users to test computer access to FSP data in the State Client Assistance for Reemployment and Economic Support (CARES) system, and the county database within that system. We discovered that a contracted case manager who was not responsible for determining eligibility, had access to the SSA's database through CARES, which was prohibited by the State's data sharing agreement with the county. The county security officer confirmed that all 7 case managers, including the one in our sample, had access to the SSA's database through CARES. He stated that he was unaware that access to the SSA's database for outside contractors was prohibited by the data sharing agreement with the State.

The county security officer was responsible for monitoring compliance of the agreement between the State and the county. In addition, he was the individual designated by the county to request access for individuals on staff and contractors from the county office. Once the access request forms were completed and signed, they were forwarded to the State security officers for review and activation. The State security officers were aware of the requirements of the data sharing agreement, however they were unaware that the case managers were contractors until we brought it to their attention during the audit. We determined that the computer access form did not identify the contractor to the State security officers, so they could limit their access. Six of the seven case managers wrote on the form that they worked for the Kenosha County Department of Human Services (DHS). However, the State still granted access to the one case manager, who correctly identified himself as a contractor. The State had no explanation for this and stated it was an oversight. If the State is

relying on the county security officer signatures and not evaluating each request form based on the information presented, they have no way of determining if request for access is valid.

We also interviewed the selected case manager that had Statewide database inquiry. She stated her duties only required countywide access in the State's database. The State security officer stated that all seven of the case managers, including the one tested in our sample, had Statewide inquiry access. The county security officer had previously stated that all case managers performed the same duties; therefore all seven would have been able to perform their job with the inquiry access limited to the county. The State security officer stated that Statewide access is granted unless the request form specifies countywide access only. However, the access request form does not specifically mention whether access should be limited to the county so county offices generally do not limit access when preparing a request.

We also noted other instances where the users' level of computer access exceeded that required to accomplish their duties. Although this additional access did not give the users access to any more SSN's than they already had, we believe it is necessary for the State to ensure that the county offices have appropriate guidance and controls in place to ensure that access is commensurate with job requirements.

A former county employee, now a private investigator, had access to FSP SSN's in the State's CARES system. The private investigator was self-employed and contracted to perform front-end verification of eligibility and fraud investigations as required. When we asked about the appropriateness of the private investigator's access to the database, the State security officer immediately revoked the investigator's access and stated that this can occur when the State security officer cannot determine, based on the computer access request form if the user should have access or not. In some cases, the form may indicate that the user is a county employee when in fact they work for an outside contractor or subcontractor, because the request form does not adequately identify the user as an outside contractor. A user may also mistakenly report that they are working for the county when they are contracted to perform services for the county. In this case, the computer access form for the private investigator indicated she was working for DHS. The county security employee believed that the investigator required access to the FSP files because she performed duties in the administration and enforcement of the FSP. However as an outside contractor, the State security officer stated that no outside contract private investigator should be given access to CARES. The security officer also said that information required by the investigator should be obtained on a case-by-case basis from the employee who assigns the case to the investigator.

In addition to the private investigator's access, we also found that a county Government user had access to FSP SSNs on the State's data warehouse to produce statistical reports for the county Government. The State data sharing coordinator stated that they do not require a data sharing agreement with the county because it is a Government agency. The State could not explain why access to individual SSN's was granted to the user, because the State security supervisor who granted this access has retired. The State security officer stated that access should not have been granted, since the county does not require the SSN's to produce the statistical reports. Since our audit, the State has set up a separate computer user access for the county Government to receive one data file by file transfer that contains no personal identifiers, including SSN's.

Our review disclosed several instances where weaknesses in procedures and documentation of the computer access policies, created inappropriate computer access to SSN's and created the opportunity for identity theft.

RECOMMENDATION NO. 1

Issue guidance to the Food and Nutrition Service Regional Offices (FNSRO) and State offices reminding them to ensure that access to confidential information in FSP databases is appropriate to the users duties and is sufficiently limited on a "need to know basis."

Agency Response

FNS officials generally agreed with the finding. They will provide more details of planned actions at a later date.

OIG Position

To reach a management decision, FNS officials need to provide us with the guidance that will be provided to its regional offices, and the State offices, and the timeframe when this action will be completed.

RECOMMENDATION NO. 2

Follow-up with the State of Wisconsin to ensure that computer access procedures, including computer access request forms, are appropriate to the users assigned duties.

Agency Response

FNS Regional officials required the State to strengthen computer access procedures and documents. The State also is implementing a training program in this area.

OIG Position

We have accepted FNS' management decision for this recommendation. For Final Action, FNS needs to provide the Office of the Chief Financial Officer (OCFO) with documentation that it required the State to strengthen computer access procedures and documents.

FINDING NO. 2

PHYSICAL ACCESS TO SOCIAL SECURITY NUMBERS WAS NOT SAFEGUARDED

In one Wisconsin county office, we found that desk drawers, file cabinets, and boxes of papers to be shredded were not properly secured and locked. The county security officer stated they did not have a policy to lock their desk drawers or file cabinets and had not considered the possible access to data by other employees and custodial staff a breach of physical security. In an Illinois county office, a file room without locks contained FSP files in 35 boxes and 300 file cabinets. As a result, SSN's and other sensitive information were not adequately protected from unauthorized disclosure and possible use in identity theft.

The Food Stamp Act and Food Stamp Regulations[8] require safeguards which limit the use or disclosure of information obtained from applicant households to persons directly connected with the administration or enforcement of the FSP laws and regulations. In addition, regulations state that recipients of information released under 7 CFR 272.1(c)(1) must adequately protect the information against unauthorized disclosure to persons or for purposes not specified[9]. Prudent business practice would also suggest the use of locked desk drawers, file cabinets, or rooms as the proper safeguard for participant information.

[8] 7 CFR 272.1(c)(1)(i)
[9] 7 CFR 272.1(c)(2)

In Wisconsin, we observed specific examples of sensitive records being left out unlocked on desktops or open shelves after normal working hours. For example, 12 case files were left on a desk or credenza in each of two child support workstations and about 30 case files were left on open shelves in another child support workstation. Child support workers verify the paternity of every minor included in a food stamp assistance group, and the security officer indicated some of the files would contain food stamp SSN's. We specifically noted that a data processing specialist, whom we had interviewed earlier in the day and is responsible for entering participant data into the county office's master database, left documents containing SSN's and other personal identifiers out on her desk in plain sight after she had left for the day.

In the Economic Support work area, a caseworker stated that she always kept her food stamp monthly caseload report, which contains SSN's for all her cases, on an open shelf. We confirmed this during our observations after hours.

The county security officer stated they did not have a policy to lock their desk drawers or file cabinets because the majority of the workers were located beyond a locked door and the public was always escorted within those areas. He did not consider the presence of after-hours custodians and other employees or contractors, who should not have access to SSN's, to be a breach of controlled physical access.

The Wisconsin security manual states: "It is the State's responsibility to ensure that reasonable steps are taken to safeguard sensitive and confidential client information. Physical access means the ability to obtain paper reports located in an office." The manual adds: Any computer printouts of information, case record information, etc., must not be left where others can access it. This information must be secured in locked files."

Continuing in the Wisconsin security manual: "If paper or printouts are used, items with client specific data should be secured when the user leaves their work area. By secured, a locked file cabinet may be used for very sensitive information (such as Food Stamp Program eligibility data) or a locked desk drawer might be suitable depending on how accessible the office is to non-staff. Confidential or sensitive information must not be left in a place for individuals who should not have access to it." And "If using paper or printouts, items with client specific data should be secured when you leave the area. Any printout with confidential information (including screen prints) should be filed; it must be locked up. When they are discarded, they must be shredded."

The State/County Data Sharing Agreement states: "Protection Against Unauthorized Access or Disclosure – the County agrees to comply with the following measures to protect the confidentiality of any information provided under this agreement and to protect such information against unauthorized access or disclosure. The information shall be stored in a place physically secure from access by unauthorized persons in conformance with the State's security system rules and State internal security rules."

We also noted an Illinois county office where case files were stored in 300 unlocked filing cabinets and 35 boxes within a storage room without a lock. The local office administrator agreed that security over files was not adequate. At a minimum, the storage room should be locked. Illinois policy[10] is broad and calls for effective control over the maintenance of records. As a result of the lack of physical safeguarding of access to SSN's, there is the potential of theft of SSN's, unauthorized disclosure, and identity theft.

RECOMMENDATION NO. 3

Issue guidance to the FNSROs, and State offices reminding them to ensure that data such as SSNs is properly secured, according to internal procedures.

Agency Response

FNS officials generally agreed with the finding. They will provide more details of planned actions at a later date.

OIG Position

To reach a management decision, FNS officials need to provide us with the guidance that will be provided to its regional offices, and the State offices, and the timeframe when this action will be completed.

RECOMMENDATION NO. 4

Follow-up with the State of Wisconsin to ensure county offices' compliance with State security requirements over FSP SSN's, according to internal procedures.

[10] Illinois Administrative Directive No. 01.05.04.030 effective 10/01/01

Agency Response

The State is publishing a joint operation memorandum for all authorized users of public assistance program data on CARES. The memorandum is a policy statement that reiterates Wisconsin's requirements for safeguarding access to sensitive records.

OIG Position

We have accepted FNS' management decision for this recommendation. For Final Action, provide documentation to OCFO that the State has issued the memorandum.

RECOMMENDATION NO. 5

Follow-up with the State of Illinois to ensure county offices' compliance with State security requirements over FSP SSN's, according to internal procedures.

Agency Response

The Department of Human Services has issued two new Administrative Directives on the subject of employee conduct, both of which cover security issues. The Office reviewed during the audit has since moved locations and now has a locked file room.

OIG Position

We have accepted FNS' management decision for this recommendation. For Final Action, provide documentation to OCFO that the State has issued the memorandums.

EXHIBIT A – SITES VISITED

Office	Location
Food and Nutrition Service Headquarters	Alexandria, Virginia
FNS Midwest Regional Office	Chicago, Illinois
Illinois State Office	Springfield, Illinois
Sangamon County Local Office	Springfield, Illinois
Lower North (Cook County) Local Office	Chicago, Illinois
Wisconsin State Office	Madison, Wisconsin
Kenosha County Department of Human Services	Kenosha, Wisconsin
Richland County Health & Human Services	Richland Center, Wisconsin

EXHIBIT B – FNS' NATIONAL OFFICE RESPONSE TO DRAFT REPORT

USDA

United States
Department of
Agriculture

Food and
Nutrition
Service

3101 Park
Center Drive

Alexandria, VA
22302-1500

JAN 21 2003

SUBJECT: FSP – Office of Inspector General (OIG) Audit Report No. 27601-29-CH, Control Over The Access, Disclosure, And Use Of Social Security Numbers

TO: Richard D. Long
Assistant Inspector General for Audit
Office of Inspector General

This provides the Agency's comments on the official draft report on OIG Audit No. 27601-29-CH, Control Over The Access, Disclosure And Use Of Social Security Numbers. We appreciate the opportunity to provide written comments on this official draft.

In general, we agree with audit findings and recommendations. However, as the report does not dispute the adequacy of Food Stamp Program laws and regulations to safeguard information, we ask that you remove the discussion of "prudent business practice" in the last sentence in paragraph two on page nine of the draft report. Introducing this discussion confuses rather than clarifies the required actions that each State must take to safeguard information.

We are providing the details of our actions on the recommendations in separate correspondence. If you need further explanation or information, please contact Lou Pastura of my staff. He can be reached on 703-305-2414.

Roberto Salazar
Administrator

EXHIBIT C – FNS' REGIONAL OFFICE RESPONSE TO DRAFT REPORT

United States Department of Agriculture

Food and Nutrition Service

Midwest Region

77 W. Jackson Blvd.
20th Floor
Chicago, IL
60604-3511

Edward R. Krivus, Regional Director for Audit
Office of the Inspector General, USDA
Midwest Region
111 North Canal Street, Suite 1130
Chicago, IL. 60606-7295

January 16, 2003

Dear Mr. Krivus,

We reference the official audit report #27601-0029-Ch, entitled " Controls Over the Access, Disclosure and Use of Social Security Numbers." We received the State Agency (SA) response and attach a copy for your information. We address each recommendation below.

Recommendation 2: Follow-up with the State of Wisconsin to ensure that the computer access procedures, including computer access request forms, are appropriate to the users assigned duties.

FNS Position: We agree with the recommendation.

State Agency Response: The Department of Workforce Development (DWD) and Health and Family Services (DHFS) will revise the Computer Access Request form (DES-10) to obtain adequate employer and need-to know information to enable the county and state staff to properly assess the access needs and limitations for the requesting individual.

The Computer Security awareness document (DWS-11328-P), which is distributed to all CARES users, will be revised to more specifically define access limitations.

An ongoing training program for county security staff will be implemented to access their training needs and to deliver appropriate training

We have reached Management Decision on this recommendation and request your concurrence.

Estimated date of completion is September 1, 2003.

Recommendation 4: Follow-up with the State of Wisconsin to ensure county offices' compliance with State Security requirements over FSP SSN's according to internal procedures.

FNS Position: We agree with the recommendation.

State Agency Response: The DWD and DHFS is publishing a joint operations memorandum for all authorized users of public assistance program data on CARES.

The memorandum is a policy statement that reiterates Wisconsin's requirements for safeguarding access to sensitive records. A draft copy of the Operations Memo is attached.

We have reached Management Decision on this recommendation and request your concurrence.

Estimated date of completion is August 1, 2003.

Recommendation 5: Follow-up with the State of Illinois to ensure county offices' compliance with state security requirements over FSP SSN's, according to internal procedures

FNS Position: We agree with the recommendation and requested in writing that State of Illinois ensure county offices' comply with state security requirements over FSP SSN's according to internal procedures.

State Agency Response: The office reviewed by OIG, the lower North Office, has recently moved from the location visited. The new office has a locked file room.

Also the Department of Human Services has issued two new Administrative Directives on the subject of employee conduct, both of which cover security issues. Copies are attached.

We have reached Management Decision on this recommendation and request your concurrence.

Estimated date of completion is January 16, 2003.

If you have any questions, please contact me at (312) 353-8239.

Sincerely,

FRANK SUCHY
Chief
Financial Management/Fiscal State Systems

Attachment

Cc: Tim English, Acting Director, FSP

Informational copies of this report have been distributed to:

Office of the Chief Financial Officer
    Director, Planning and Accountability Division (1)
Administrator, FNS
    Through Agency Liaison Officer, FNS (8)
General Accounting Office (1)
Office of Management and Budget (1)