STATE COMPUTER SECURITY

OFFICE OF INSPECTOR GENERAL

OFFICE OF ANALYSIS AND INSPECTIONS

DECEMBER 1988

OFFICE OF INSPECTOR GENERAL

The mission of the Office of Inspector General (OIG) is to promote the efficiency, effectiveness and integrity of programs in the United States Department of Health and Human Services (HHS). It does this by developing methods to detect and prevent fraud, waste and abuse. Created by statute in 1976, the Inspector General keeps both the Secretary and the Congress fully and currently informed about programs or management problems and recommends corrective action. The OIG performs its mission by conducting audits, investigations and inspections with approximately 1,200 staff strategically located around the country.

OFFICE OF ANALYSIS AND INSPECTIONS

This report is produced by the Office of Analysis and Inspections (OAI), one of the three major offices within the OIG. The other two are the Office of Audit and the Office of Investigations. OAI conducts inspections which are typically short-term studies designed to determine program effectiveness, efficiency and vulnerability to fraud and abuse.

THIS REPORT

The report is entitled, "State Computer Security." It was conducted as follow-up to a study of computer related fraud which found that one-third of the frauds involving Government funds were committed on State and local computer systems. This study sought to identify State efforts to plan and implement computer security on systems administering federally-funded programs.

This study was prepared by the Regional Inspector General, Office of Analysis and Inspections, New York Region. Participating on the project were the following:

New York
Jack Molnar (Project Leader)

Chicago
John Traczyk

Dallas
Ralph Tunnell

Headquarters
Alan Stubbs

San Francisco/Seattle
Leonard Czajka
Apryl Williams

STATE COMPUTER SECURITY

Richard P. Kusserow
INSPECTOR GENERAL

OAI-02-88-00630

DECEMBER 1988

EXECUTIVE SUMMARY

BACKGROUND

The purpose of this inspection was to identify State efforts to plan and implement computer security on systems administering federally funded programs, and to assess the effect Federal requirements are having on the States efforts. It was initiated out of an awareness that one-third of computer-related frauds involving Federal funds, as identified by the President's Council on Integrity and Efficiency, were committed on State computer systems.

There were two phases of activity in this inspection. Initially, Federal guidance to States on computer security was reviewed and meetings were conducted with appropriate Federal staffs to identify relevant requirements and monitoring practices. It was then determined that the study should focus on the Aid to Families With Dependent Children, Medicaid and Food Stamp programs.

The second phase included visits to 12 States to discuss computer security with automatic data processing (ADP) and program staff. This was not an audit of the State systems, but rather a survey of State officials who were responsible for the systems. The States were selected to assure a variety of security environments. The selection criteria included program size, use of shared data centers and use of enhanced funding. At each State, discussions were held at both the State and local sites.

FINDINGS

Federal Security Guidance Has Limited Impact On States

State computer security efforts varied significantly among the States visited. The lack of common Federal guidance and monitoring, and mixed levels of interest in security appear to be the primary cause for such variation. Audits by the Inspector General for the U.S. Department of Agriculture (USDA) and State legislative pressure appear to be the major factors influencing the development of State security programs. States without such influence had less organized security programs.

Examples of the limited impact of Federal security guidance are that 3 of the 12 States visited reported that they were unaware of any Federal computer security standards, and only 4 States were able to note findings or recommendations resulting from Federal monitoring. Some said the Federal requirements were too general to be of any value. The exception was the Internal Revenue Service (IRS) guidance in the Income and Eligibility Verification System (IEVS) regulations. Seven States took strong exception to these requirements because they are too burdensome, as well as inappropriate to the IEVS use of IRS data.

When asked what they believed would be an appropriate Federal role, State agencies were virtually unanimous in their desire for assistance in this area. They want comprehensive regulations, common to all programs with supporting guidance. They are split about the level of monitoring; half opted for field visits, the others preferred the submission of vulnerability assessments. The Assistant Secretary for Management and Budget (ASMB) issued proposed regulations that include a common standard for State computer security on federally funded systems and monitoring through the submission of vulnerability assessments.

States Have Good Access Controls

Access controls in the form of passwords and identification numbers, terminal identifiers and audit trails of persons who had used the system are the strengths of the State security programs. Virtually all States used access controls to limit employees' ability to create or modify files, and to keep a log of transactions and system use. However, despite the apparently well designed and implemented access control efforts noted among the States, a potential vulnerability to the protection of personal data was noted in a number of States.

First, many States issue generic passwords for query function. While this practice does not directly permit unauthorized persons to view or print out client records, it does create opportunity for access which is not easily monitored. Secondly, many States are introducing, or increasing the use of, personal computers which have access to the client data bases. Such access, which is usually created for staff offices as opposed to program, creates the opportunity for downloading large quantities of data.

States Need to Strengthen Security in Specific Areas

Weakness in State computer security is documented by the absence of some commonly accepted practices:

- Three-quarters of the States visited do not have a specific computer security plan fully implemented.
- Only three States have plans for, and monitored, computer security at remote sites.
- Only two States do vulnerability assessments or risk analyses to evaluate their security.
- Only four States do personnel security background checks.
- Contingency plans generally exist on paper, but only three plans have been tested.

RECOMMENDATIONS

During the course of this inspection, the Office of Inspector General twice recommended changes to ASMB's Notice of Proposed Rule Making (NPRM), "Automatic Data Processing Equipment and Services; Conditions for Federal Financial Participation." The recommendations included:

- Modifying the NPRM to specifically require that the States have a single security plan.
- Adding a requirement for review of data security in addition to physical security reviews.
- Establishing a clearly defined relationship between generic security requirements and program-specific requirements.

The recommendations listed above were incorporated into the NPRM. We recommend that the Department issue the common computer security standards in final form with a risk analysis requirement. Additionally, monitoring or review procedures for these regulations should be established.

TABLE OF CONTENTS

INTRODUCTION

PURPOSE

The purpose of this inspection was to identify State efforts to plan and implement computer security on systems administering federally funded programs, and to assess the effect Federal requirements are having on the States' efforts.

BACKGROUND

While the security of Federal computer systems has long been monitored by both Congress and the Executive Branch, it is only recently that attention has begun to focus on State computer systems used in the administration of federally funded programs. Beyond the fact that significant Federal funds are used to develop and administer these systems and are expended through these systems, a number of recent events have raised questions as to the quality of State computer security.

In 1985, the President's Council on Integrity and Efficiency (PCIE) requested the Inspector General (IG) for the Department of Health and Human Services (HHS) conduct a study of computer-related fraud in government agencies. That inspection included interviews with 46 perpetrators to learn about their individual crimes and the system vulnerabilities that existed which allowed these crimes to occur. All of the perpetrators held positions with some degree of involvement in the agency's computer system. A number of the State and local agency perpetrators characterized their agency's existing computer security and internal controls as weak and, therefore, vulnerable to the type of crime they committed. The study also found that 43 percent of these State and local employees had previous criminal records when hired by their agency.

Congress has also expressed concern that computer security systems have inadequate controls which leave them vulnerable to improper use and inadequate protection of privacy. Several legislative initiatives have been introduced which address the problems involving the security of computer systems in federally funded programs. The Office of Technology Assessment, the research arm of Congress, issued a report which warned that the opportunities for unauthorized access to and use of government computer data have increased, and also identified the computer matching performed by State agencies as an area where protection of data may be insufficient.

The U.S. Department of Agriculture's (USDA) IG found computer system vulnerabilities at State and local agencies administering Food and Nutrition Service (FNS) programs. Its 1984 audit of 13 non-Federal computer systems administering Food Stamp programs found weaknesses in all of them, leading the IG to consider these systems highly vulnerable. It also reported that FNS had not issued any security guidelines for non-Federal systems and needed to improve its monitoring of these systems.

Another concern is the relative lack of Federal guidance for State computer security as opposed to Federal systems. Federal standards for Federal systems, which run thousands of pages and include NSDD-145, Office of Management and Budget (OMB) Circulares A-130 and Federal Information Processing Standards (FIPS) publications, require each agency to have its own computer security program. These Federal computer security programs are monitored by individual agencies and OMB through the A-123 process, by Inspectors General internal reviews, as well as by the General Accounting Office.

By comparison, Federal standards for State systems are a patch-work of uncoordinated regulations. Each Federal agency, in overseeing the State administration of its programs, issues guidelines; only some of them include standards on computer security. The agency may also issue differing standards depending upon whether or not the State receives enhanced (i.e., 75 or 90 percent) Federal funding for its ADP system. Those Federal standards which do exist vary in degree and types of security required, and may sometimes duplicate or conflict with each other or with State requirements. This may present compliance difficulties for those States which process more than one Federal program at the same computer center.

Among the various programs, Medicaid (title XIX of the Social Security Act) has had regulations in place for almost 15 years providing for enhanced Federal Financial Participation (FFP) for the Medicaid Management Information System (MMIS) for States requesting it. However, an amendment that required the development of security standards for MMIS, not enacted until 1980, allows States to conduct internal reviews using standards developed by the Department. A yearly review by the Health Care Financing Administration (HCFA) of the States' systems was required until 1985 when the Consolidated Omnibus Reconciliation Act (COBRA) revised the frequency of reviews to once every 3 years. The standards issued to the States are general in nature and the specific development of State security criteria is left to the States.

With regard to the Aid to Families with Dependant Children Program (AFDC), a general statement requiring safeguards for information existed for many years, but no discussion of State computer security existed until Public Law 96-265 was enacted, with the regulations effective in 1981. Public Law 96-265 allowed States to request enhanced funding for the development of a computerized information system which met certain standards, including security against unauthorized access to or use of data. The law also required the Department to monitor the system's compliance with the standards.

Within USDA, the FNS, which monitors the Food Stamp program, issued an *ADP Security Guide* which provides States with general automatic data processing (ADP) security guidelines for developing their own security programs. These standards, which were developed as a result of the 1984 audit noted above, apply to States with or without enhanced funding.

A reassessment of computer system security programs of States is now occurring due to the passage of Public Law 98-369, the Deficit Reduction Act of 1985 (DEFRA), which created the Income and Eligibility Verification System (IEVS). This law requires AFDC, Medicaid,

Food Stamps and other programs to receive income information from the Internal Revenue Service (IRS) and Social Security Administration (SSA), and to use it in determining applicants' eligibility for program benefits. All programs were required to start using IEVS by September 30, 1986. Both the IRS and SSA have personal data safeguarding guidelines which all agencies obtaining information from them must follow. The IRS *Tax Information Security Guidelines* goes into specific detail on areas of computer security and record safekeeping. It also requires a periodic report to the Federal funding agency on the status of safeguarding procedures. The SSA issued security instructions in its Program Operations Manual which apply to States that obtain information from the Benefit and Earnings Data Exchange (BENDEX) or Supplementary Data Exchange (SDX) systems. However, SSA is currently in the process of changing these requirements by adopting the IRS requirements.

To add to the concern at the Federal level, States' assessments of their own security programs offer little reassurance. The National Association for State Information Systems (NASIS) stated in its 1984-1985 report that States' "...data security appears to be far from an accomplished fact and that progress in establishing physical security at States' data centers does not appear to have been made." Of the States reporting as part of the NASIS survey, half volunteered that their data centers do not have a security plan.

METHODOLOGY

There were two phases of activity in this inspection. Initially, Federal guidance to States on computer security was reviewed and meetings were conducted with appropriate Federal staffs to identify relevant requirements and monitoring practices. Based upon these activities, it was determined that the study should focus on the AFDC, Medicaid and Food Stamp programs.

The second phase was to visit 12 States to discuss computer security with ADP and program staff. The States were selected to assure a variety of security environments. The selection criteria included program size, use of shared data centers and use of enhanced funding. At each State, discussions were held at both the State and local sites. The States visited were:

California	Florida	Georgia
Illinois	Maryland	Michigan
New Jersey	New York	Pennsylvania
Texas	Vermont	Washington

FINDINGS

State Computer Systems and Operating Environments Vary

Unlike many Federal agencies or the Medicare carriers and intermediaries, not all State human service agencies own and operate their own computer systems. Six of the 12 States visited operated through a centralized ADP agency. These agencies, which may be peer agencies to the human service agencies or components within a larger administrative services agency, house and operate the State computer systems. Among the States we visited, the centralized ADP agencies served from 32 to 61 other agencies besides the human service agency. While this situation is not a problem in and of itself, it has implications for the implementation of program specific regulations and guidelines that relate to computer systems such as computer security.

First, these centralized ADP agencies have their own operating rules and regulations as well as administrative systems that address computer security. Often these rules and systems are the result of State law or policy. Second, because as many as 10 different federally funded programs are served by some of the centralized ADP agencies, the ADP agencies are potentially obligated to be in compliance with all of the various Federal agency requirements. The lack of Federal recognition of this working environment has created a problem for some States. Specifically, the IRS security requirements under IEVS require the program officials to personally supervise the processing of the IRS tapes. However, they do not have access to the central data center. Under normal operating procedures, program officials would simply send a tape to the data center for processing. In practice, States appear to be ignoring the IRS requirement because it is not practical.

On the other hand, two of the centralized ADP agencies reported that they were unaware of any Federal computer security requirements that might apply. This occurs for two reasons: first, because of uneven and sometimes weak Federal monitoring of program-specific computer security requirements; second, because Federal requirements are, by design, communicated to program staff in the agency administering the human service program. Therefore, the program agency becomes an intermediary with the central ADP agency and must also attempt to encourage or assure its compliance.

Federal Security Guidance Has Limited Impact On States

While all States were aware of the need for computer security and had security programs in place, computer security efforts varied significantly between the States visited. This is due to the lack of common Federal guidance and monitoring, and mixed levels of interest among the States in computer security.

For example, the Family Support Administration (FSA) has security standards that must be addressed in plans for, and met in the certification of, Family Assistance Management Information Systems (FAMIS) which receive enhanced funding. However, since 32 States are in the

planning or development stage and 10 States are not seeking such a system, most States are currently not covered by these requirements. Security requirements for non-enhanced systems are virtually non-existent in that they only speak to protecting personal data. The FSA performs some *ad hoc* reviews of security by funding ADP audits conducted by outside consultants where vulnerabilities are suspected.

The HCFA has MMIS security standards, and these are regularly reviewed. However, since most MMISs are contracted to private agencies, the reviews rarely include the State systems. Also the guidance to regional offices, which conduct these reviews, focuses primarily on claims processing and minimally on eligibility systems. Additionally, in the most recent reviews for 8 of 12 States in this study, computer security standards were documented as "deemed met," meaning they were not actually reviewed because they had been met in an earlier review.

The USDA/FNS issued a comprehensive computer security guide to State agencies in February 1986 as a follow-up to the USDA/IG's review of computer security in 13 States. This guide, however, does not have the force of law and has largely been implemented and monitored by correspondence.

The SSA had a requirement until September 1986 for each State receiving BENDEX data to have a security officer and a written, comprehensive security plan which was to be submitted to SSA. However, it appears that SSA has not implemented these security requirements, according to the States visited in this inspection.

The IRS' "Tax Information Security Guidelines" now apply to State agencies because of the IEVS requirement. Based upon Internal Revenue Code requirements to safeguard tax data, they require a self-assessment of data security that includes a review of computer security. States report that the IRS requirements are inappropriate and burdensome for the purposes of IEVS. A few States reported that they will use a liberal interpretation of the IRS guidelines until "caught."

Audits by the USDA/IG and State legislative pressure appear to be the major factors influencing the development of State security programs. States without such influence had less organized security programs. For example, only 4 of the 12 States have a personnel security component to the computer security programs. (Personnel security is a mandated component of Federal computer security programs.) In each of these four instances, personnel security was initiated as part of the corrective action plan resulting from the USDA/IG audits.

Only two States did formal risk analyses on their systems; in both instances they were mandated by the State legislatures. Two State legislatures mandated the format of the State computer security plan. As one central ADP administrator pointed out: "they (the State Legislature) control our budget and our agencies' budgets. We do what they tell us to do." The most common computer security problem noted by State ADP officials was the lack of a

management commitment to security. While this is not a problem unique to States or even the public sector, legislative concern, in at least 2 of 12 States, appears to have assured a management commitment.

An example of the limited effect of Federal guidance is the fact that 3 of the 12 States visited reported that they were unaware of any applicable Federal computer security standards. All States reported that they were unaware of the BENDEX requirements; this is understandable since it appears SSA never formally implemented them. A BENDEX computer security requirement calls for States to have a Security Action Plan (SAP) and to submit an annual evaluation of the SAP to SSA as a condition of receiving BENDEX and SDX data. Copies of the SAP and evaluations for each of the States visited were requested of SSA. The SSA has failed to respond.

Although eight States reported computer security monitoring by HCFA, and four each by FNS and FSA, only four recalled findings or recommendations resulting from this Federal monitoring. The most commonly reported finding was the already noted lack of personnel security found by the USDA/IG. Other problems noted were the lack of testing of contingency plans or the lack of risk analysis. Although States were most aware (8/12) of HCFA visits, only one noted any recommendations resulting from HCFA monitoring, a concern regarding the use of IEVS data. A likely reason for the lack of findings resulting from the HCFA monitoring is that HCFA did not always review computer security during its System Performance Review (SPR) monitoring visits. For eight of the visited States, HCFA deemed security satisfactory and did not review it since it had passed review in the past. It should be noted here that while only eight States reported HCFA monitoring visits, HCFA produced monitoring reports for all States.

When asked about problems with Federal security guidance, only five States offered any comments. One important comment was with regard to IRS' guidance in the IEVS regulations. Seven States took strong exception to these requirements as being too burdensome, as well as inappropriate to the IEVS use of IRS data. One State official said, "If we had to handle and use IRS data as IRS guidelines suggest, the use of IRS data would be unworkable." Another offered, "The IRS requirements to destroy tape by cutting the tape every so many inches, or to run IRS tapes, shut down the system, verify JCL and then restart the system cold are antiquated and costly." There have been, and continue to be, efforts by HHS/ASMB to balance IRS needs to assure that tax data is protected with States' needs to implement IEVS in an efficient manner.

When asked what they believed would be an appropriate Federal role, State agencies were virtually unanimous in their desire for assistance in this area. The State agencies want a comprehensive set of minimum standards, common to all programs, and to have supporting guidance. In fact, it should be noted that a number of States are actively looking for a computer security standard and requested such guidance from the inspection team. States are, however, split about how they would like to see the monitoring done. While half opted for monitoring site visits, the others preferred the submission of a risk or vulnerability assessment. (Some noted that the latter could be done by a State audit agency.) The ASMB has issued a

proposed regulation that includes a common standard for State computer security on federally funded systems. It includes monitoring through the submission of vulnerability assessments. It should be noted, however, that only two of the States visited did vulnerability assessments and both were reluctant to share them with us voluntarily.

States Have Good Access Controls

Access controls in the form of passwords and ID numbers, terminal identifiers, and audit trails of persons who had used the system are the strengths of State security programs. Virtually all States used access controls to limit to their job responsibilities, employees ability to create or modify files, and to keep a log of transactions and system use. States report that their use of controls and audit trails have developed out of a long history of establishing eligibility and authorizing benefits through a decentralized operation. Thus, with the advent of automation it was logical to build such controls into their computer systems. Seven of the States use commercial access control software such as "RACF," "ACF II," or Top Secret, while the others developed their own.

More specifically, the access controls virtually always consisted of both employee specific passwords and an ID. The latter was often the employee's Social Security number. Ten of the States had procedures for periodically changing passwords. This ranged from every 3 months to a year. The IDs were used to limit the employees to specific terminals, specific cases and/or specific types of transactions.

Despite the apparently well-designed and implemented access control efforts noted among the States, a potential vulnerability to the protection of personal data was noted in a number of States. This vulnerability took two forms:

- Many States issue generic passwords for the query function. This is typically done for persons in clerical or receptionist positions so they can determine if a client has a record. While this practice does not directly permit unauthorized persons access to view, print, create or modify client records, it does create an opportunity for access that is not easily monitored. Generic passwords are easily shared and thereby render personal data vulnerable to disclosure.

- Many States are introducing, or increasing the use of, personal computers which have access to the client data bases. Such access, usually created for staff offices as opposed to program personnel, creates the opportunity for the mass manipulation of, or downloading of, large quantities of data.

States Need To Strengthen Security In Specific Areas

Weaknesses in State computer security can be documented by the absence of some commonly accepted practices. If one were to use OMB Circular A-130 (*Management of Federal Informa-*

tion Resources, the computer security requirement applicable to Federal agencies) as a standard for evaluating State computer security programs, a number of specific deficiencies could be noted among the States visited.

- Three-quarters of the States did not have a specific computer security plan in place. The OMB Circular A-130 requires a specific computer security plan and the designation of an individual to be responsible for the implementation of the plan. Only four States had such procedures in place. The others, when queried about computer security plans, reported that they relied on a variety of administrative guidelines, had a plan that addressed data security or access controls only or had no plan but were developing one.

The Office of Inspector General in commenting on ASMB's proposed computer security guidelines for federally funded systems during the in-house review period, recommended that one of the requirements be for States to have one, comprehensive computer security plan.

- Only three States had plans and monitoring procedures for computer security at remote sites (State district or county welfare offices). While Federal computer security guidance stresses that security must be system-wide (i.e., including remote sites), States in general appear to leave remote site security to the discretion of local managers or ADP staff. The access control system, in most instances, is statewide by design, and therefore, is in place at remote sites. These nine States are providing local managers with little more than the access control manual. Two of these States report that they do look at security during monitoring visits but neither had standards against which to evaluate the security at the local offices.

- Only two States did vulnerability assessments or risk analyses to evaluate their security. It should be noted that not only is a periodic risk analysis required on Federal computer systems, but the proposed ASMB computer security requirements for States will require a risk assessment. As noted earlier, the two States that did risk assessments did so at the direction of their State legislatures. A possible implementation problem for the ASMB regulation is that both States were reluctant to share those reports with us on a voluntary basis. However, most State computer systems had been reviewed by outside agencies such as "Big 8 CPA" firms or State auditors.

- Eight States did not do personnel security background checks. Background checks are a standard requirement for Federal employment and personnel security is a mandated component of Federal computer security. The discussions with States revealed that the idea of background checks for persons who had access to computers was never really considered. In fact, the four that do perform background checks do so in response to the USDA/IG audits.

- Contingency plans generally exist on paper in the form of a proposal to move into and share another agency's facility. Only three plans have been tested.

RECOMMENDATIONS

The most significant finding of this inspection is the lack of common, Federal standards for States to meet with regard to security on their federally funded computer systems. The HHS/ASMB issued on September 21, 1987 a Notice of Proposed Rulemaking - "Automatic Data Processing Equipment and Services; Conditions for Federal Financial Participation." The NPRM, among other things, will establish such standards. During the process of developing the standards, OIG made recommendations to strengthen them based upon the experience gained in conducting this inspection.

The recommendations included:

- Modifying the NPRM to specifically require that the States have a single security plan.

- Adding a requirement for review of data security in addition to physical security reviews.

- Establishing a clearly defined relationship between generic security requirements and program-specific requirements.

The recommendations listed above were incorporated into the NPRM. It should also be noted that USDA is in the process of developing a companion security regulation for its grantees.

We recommend that the HHS common computer security standards be issued in final, with the requirement for risk analyses.

Review and follow-up procedures will need to be established in order to properly monitor implementation of the standards. The OIG will monitor implementation of the standards to determine their effectiveness in addressing the areas of concern highlighted by this report.

AGENCY COMMENTS

Substantive comments on the draft report were received from ASMB and FSA within HHS and from the Food and Nutrition Service (FNS) and the Inspector General at USDA.

The HHS/ASMB reported that lead responsibility for State ADP systems had been transferred from ASMB to FSA, and that FSA was now in the process of finalizing the computer security regulations for States receiving Federal funds. FSA reports that the final regulations will soon go through final Departmental clearance.

The USDA/FNS reported that on August 8, 1988 they issued an NPRM establishing minimum computer security requirements for State and local agencies administering Food Stamp Programs. Our analysis of these regulations indicates that they are virtually identical to the HHS regulations. The USDA/IG suggested that responsibility for assuring and monitoring compliance with the regulations be assigned. The USDA regulations note that FNS will be responsible for assuring compliance; FSA will assume that responsibility within HHS. They will be using either the required security reviews or the corrective action plans as the primary means for monitoring compliance.