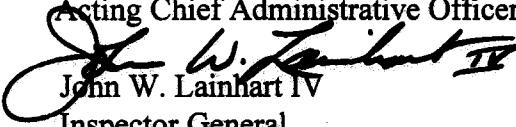


Office of Inspector General
U.S. House of Representatives
Washington, DC 20515-9990

MEMORANDUM

TO: Jeff Trandahl
Acting Chief Administrative Officer

FROM: 
John W. Lainhart IV
Inspector General

DATE: December 17, 1996

SUBJECT: Audit Report - Stronger Controls Needed Over The Data Processing Environment At The U.S. Geological Survey, Reston General Purpose Computer Center (Report No. 96-CAO-09)

This is our final report on the general controls audit of the U.S. Geological Survey (USGS), Reston General Purpose Computer Center (GPCC) located in Reston, Virginia. This audit was coordinated with the Department of the Interior (DOI), Office of Inspector General (OIG). The primary purpose of this audit was to evaluate the effectiveness of the general controls environment surrounding the Federal Financial System and the processing of U.S. House of Representatives (House) financial data at the GPCC. The body of this report summarizes the findings at a high level. Because the audit identified weaknesses that could substantially increase the risk of unauthorized access and modifications to, and disclosure of, House and other agency information, the detailed findings and recommendations are provided in a confidential appendix (see Appendix A).

At the outset of the audit, we identified two weaknesses that, if left uncorrected, would have been "show stoppers" with respect to implementing FFS at the House. The first weakness involved a vulnerability with the planned backup connection which was to be routed from the House mainframe to the USGS mainframe through the USGS and DOI networks. The second weakness dealt with a vulnerability with the planned disaster recovery connection, which called for dial-up modem access by the House to USGS's backup facility, Comdisco, through the USGS and DOI networks. These weaknesses were immediately brought to the attention of the Chief Administrative Officer for corrective actions, and were resolved prior to the House's implementation of FFS.

In this report, we identified 42 significant GPCC information systems integrity weaknesses and made 72 recommendations for corrective actions. While the majority of these weaknesses and recommendations are directed to USGS, we identified two weaknesses related to FFS administration and maintenance, and information protection and made two recommendations for

corrective action by the House. The remaining 40 weaknesses should also be of interest to the House from the standpoint of House financial data processing integrity and security.

In response to our July 15, 1996 draft report, USGS management and your office fully concurred with our findings and recommendations. The formal management responses provided by USGS and your office are incorporated in this final report and included in their entirety as confidential appendices (see Appendices B and C). The corrective actions taken and planned by USGS and your office are appropriate and, when fully implemented, should adequately respond to the recommendations. Further, the milestone dates provided for implementing corrective actions appear reasonable.

The DOI/OIG issued a very similar version of this report under separate cover to the Secretary of DOI (Report No. 97-I-98, entitled *General Control Environment Of The Federal Financial System At The Reston General Purpose Computer Center, U.S. Geological Survey*) on November 15, 1996. A copy of this report is attached.

We appreciate your office's positive attitude and cooperation throughout this audit. If you have any questions or require additional information regarding this report, please call me or Craig Silverthorne at (202) 226-1250.

Attachment

cc: Speaker of the House
Majority Leader of the House
Minority Leader of the House
Chairman, Committee on House Oversight
Ranking Minority Member, Committee on House Oversight
Members, Committee on House Oversight

I. INTRODUCTION

Background

On August 3, 1995 the Committee on House Oversight passed a Resolution mandating that the Chief Administrative Officer (CAO), in consultation with the Inspector General, implement a new financial management system. Accordingly, in September 1995, the CAO entered into a cross-servicing agreement with the U.S. Geological Survey (USGS) to implement, as a short term solution, the USGS's Federal Financial System (FFS) for the U.S. House of Representatives (House) and process the House's financial data. FFS resides on a mainframe computer at the USGS Reston General Purpose Computer Center (GPCC) located in Reston, Virginia and the application is supported by the USGS, Washington Administrative Service Center (WASC). Other services to be provided to the House by the GPCC are contingency planning, backup, and disaster recovery (including hot-site restoration of FFS operations within two business days), performance monitoring, and security administration. To ensure the integrity and security of the House's financial information, the House needed to assess the adequacy of GPCC's data processing environment. (This audit report is the result of that assessment.)

The WASC was established in 1987 as an organization within USGS to direct the Department of Interior's (DOI) efforts to standardize administrative systems. FFS was purchased in 1987 and subsequently implemented in the DOI bureaus. The FFS license that USGS has with American Management Systems, Inc. (AMS) allows the USGS to provide cross-servicing to external Federal government agencies.

The GPCC, which is government-owned and government-operated, provides a broad spectrum of data processing support for numerous sensitive major application systems, including FFS. To support FFS, the Center operates a large-scale Amdahl 5890-600E mainframe computer running IBM's Multiple Virtual Storage (MVS) Extended Systems Architecture (ESA) operating system, version 4.2 to manage its processing workload. The access control security software installed on the mainframe is Computer Associates' Access Control Facility 2 (ACF2), which not only controls user access to the FFS dedicated Customer Information Control System¹ (CICS) applications, but also access to the Time Sharing Option² (TSO) facility. In addition to this standard system-level security, FFS contains data base level security that controls the actual system action that a user may invoke. Other system software--such as other data base

¹CICS is an IBM software product that serves as the teleprocessing monitor for the MVS operating system on the GPCC mainframe computer. CICS enables transactions entered at remote terminals to be processed concurrently and is designed to control the execution of application programs in an interactive/online environment.

²TSO is an IBM software product that serves as the session manager on the GPCC mainframe computer whereby terminal users can submit jobs online. It is a method of using a computing system that allows a number of users to execute programs concurrently and to interact with the programs during execution.

management software, telecommunications software, and specialized vendor software products--also resides on the mainframe computer. Network and local communications support for both asynchronous and synchronous protocols³ are provided, as well as local area network (LAN) connectivity via Ethernet⁴ and Transmission Control Protocol/Internet Protocol⁵.

Objective, Scope, and Methodology

This review was initiated and led by the House Office of Inspector General (OIG) and coordinated with the DOI/OIG. It was conducted by Price Waterhouse LLP, under contract to the House OIG. The primary objective of this review was to evaluate the effectiveness of the general controls environment surrounding FFS and House financial data processing at the GPCC. The review focused on evaluating the adequacy of management and internal controls over the following general control areas:

- Data center management and operations;
- Mainframe system physical and logical security;
- Telecommunications security;
- LAN security; and
- Contingency planning, backup, and disaster recovery.

The scope of this audit included a review of the integrity, confidentiality, and availability of information resources for processing House financial data. Evaluation of general controls focuses on a number of control issues, including user authentication, protection of information and information systems from unauthorized access, modification, or destruction, and the backup and recoverability of information, systems, and telecommunications links in the event of a disruption in operations.

³Asynchronous protocol refers to a set of conventions used to start and stop transmissions that occur without a regular or predictable time relationship to a specific event. Whereas, synchronous protocol refers to a set of conventions used for transmissions that occur regularly or predictably with respect to a specific event.

⁴Ethernet is a networking scheme that allows microcomputers to be connected to a network. It physically consists of cabling, which connects all the machines on a network.

⁵Transmission Control Protocol/Internet Protocol is the system that networks use to communicate with each other by allowing traffic to be routed from one network to another. The Internet Protocol (IP) is a set of conventions used to pass packets (i.e., a cluster of data) from one network to another.

We conducted our review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Our review was performed during the period of March 27 through May 17, 1996, and consisted of the following specific tasks:

- Gathered documentation and conducted interviews;
- Identified business objectives and control techniques consistent with sound security standards based on current industry standards and government guidelines;
- Gained an understanding of the computing and internal controls environment surrounding security, including integrity, confidentiality, and availability of the GPCC's processing environment;
- Assessed the risks surrounding key management and internal control areas and developed a test matrix containing appropriate detailed test and verification procedures;
- Executed the steps outlined in the test matrix and updated the risk assessment based on the results of testing; and
- Utilized third party audit and security software tools to perform a number of the automated testing techniques.

In addition, we applied computer and information systems audit guidelines used by Federal government and private industry computer installations in evaluating the effectiveness of GPCC management and operations.

Internal Controls

We evaluated internal controls related to the integrity, confidentiality, and availability of the GPCC mainframe and other information system environments, which could adversely affect the House FFS data and FFS processing. The audit disclosed significant internal control weaknesses involving the GPCC's MVS operating system, security access controls, security program and functions, network controls, and business continuity planning. Collectively, these information systems integrity weaknesses constitute a material internal control weakness under the Federal Managers' Financial Integrity Act (FMFIA) of 1982 materiality criteria established by the Office of Management and Budget (OMB). We, therefore, recommend that USGS report this material internal control weakness to the Department in its next annual FMFIA submission as required under FMFIA and OMB Circular A-123. An overview of significant internal control weaknesses identified are described in the "Results In Brief" section of this report.

Prior Audit Coverage

With the exception of this audit, audits of USGS and its data centers are not in the purview of the House OIG. Therefore, there are no prior audits related to the overall FFS application processing and the general controls environment at the GPCC performed by the House OIG. However, two audit reports, described below, constitute DOI/OIG's prior audit coverage during the past ten years related to FFS processing and selected aspects of the general controls environment at the GPCC.

- *Implementation of the Federal Financial System, U.S. Geological Survey* (Report No. 92-I-1418, dated September 1992): This report disclosed that FFS had not been effectively implemented and the system did not meet requirements contained in the Joint Financial Management Improvements Program "Core Financial System Requirements" because USGS did not follow basic Office of Management and Budget (OMB) and departmental guidelines for establishing and maintaining an integrated financial management system. In addition, the report identified inadequate physical security at the Reston Automated Data Processing (ADP) Facility. The report contained 19 recommendations to correct the deficiencies noted during the audit. USGS generally agreed with the recommendations and initiated actions to correct the deficiencies identified.
- *Review of Follow up on Audit Recommendations, U.S. Geological Survey* (Report No. I-WS-GSV-11-86, dated January 1987): This review evaluated the status of audit recommendations contained in two prior audit reports (Report No. E-EM-GSV-11-83, issued on March 30, 1984 and Report No. E-WS-GSV-13-85A, issued on May 13, 1985). The review found only 17 of the prior 28 recommendations had been implemented. The resulting audit report disclosed: (1) USGS did not meet the minimum Federal and departmental requirements for ADP security at four computer centers related to risk analyses, continuity of operations, and security evaluations; and (2) administrative safeguards over user identifications and personnel screening at the Reston Center needed to be improved. The report made 17 recommendations for correcting the problems disclosed in the audit. USGS agreed with all of the recommendations and initiated actions to correct the deficiencies identified.

II. RESULTS IN BRIEF

The GPCC has not implemented adequate controls in five major areas involving (1) data center management and operations, (2) mainframe system physical and logical security, (3) telecommunications security, (4) LAN protection, and (5) contingency planning, backup, and disaster recovery. Collectively, these deficiencies were material and substantially increase the risk of unauthorized access and modifications to, and disclosure of, House and other agency information supported by GPCC's mainframe computer. Further, some of the deficiencies increase the potential for errors and omissions during system initialization (start up) and processing. Other deficiencies related to physical access to the data center increase the risk of unauthorized access and theft or destruction of hardware, software, and information. However, USGS and House management worked collaboratively with the audit team to correct key deficiencies related to FFS processing as they were brought to their attention.

The prevailing reasons for many of these deficiencies were attributed to the lack of certain formal data center standards, policies, and procedures; improper practices and processes; lack of segregation of duties; noncompliance with key vendor guidelines for MVS integrity; and lack of a formal, comprehensive data security program.

Overall, we identified a total of 72 recommendations for improving the general controls environment at the GPCC. The detailed discussion and specific recommendations for each general controls area are contained in Appendix A of this report. To facilitate the implementation of our recommendations, we have annotated in Appendix A the recommendations that require more immediate management attention. The Appendices to this report are "Confidential" and may not be disclosed or released to anyone other than auditee management except by approval of the House OIG or DOI/OIG.

Federal Government And Private Industry Data Security And Internal Control Guidelines And Practices Are Well-Established

The OMB and the National Institute of Standards and Technology have issued numerous directives, policies, and guidelines calling for Federal agencies to establish and implement computer security and controls to improve privacy of sensitive information in Executive Branch agencies' computer systems. Additionally, Congress has enacted various laws, such as the Privacy Act of 1974 and Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring the Executive Branch to assure an adequate level of computer security and controls.

For the public and private sectors, generally accepted security practices include the establishment and implementation of comprehensive information system security programs and adequate controls with respect to the sensitivity of information processed on computers. Such programs and controls normally encompass proper reporting structure, segregation of duties, establishment of computer and data security standards, policies, and procedures, risk analyses, personnel security requirements, application controls, independent reviews, and other control-related mechanisms to ensure effective management and protection of sensitive information.

Stronger Controls Needed Over GPCC's Information Systems Environment

The following is a summary of each of the five major general control subareas, highlighting key deficiencies identified during the course of the audit.

Data Center Management and Operations

We found numerous deficiencies in the areas of data center management and operations that posed significant risks to system integrity, confidentiality, and availability. For example, these weaknesses included:

- Inconsistent and inadequate security background checks and clearances for GPCC and contractor employees in accordance with job responsibilities and sensitivity of information access.
- Poor or nonexistent controls over access to the DOI and USGS general support systems, such as the Internet, DOINET, and LANs.
- Inadequate and inconsistent program change control procedures.
- Inadequate problem resolution procedures for recording, approving, and tracking reported problems through resolution.
- Failure to mark/label sensitive computer-generated printouts, such as FFS reports, and screen users for proper identification and authorization when distributing computer printouts.

In this area, we made 18 specific recommendations to address the above issues as well as other related issues--described in Appendix A of this report--and improve data center management and operations.

Mainframe System Physical And Logical Security

We found numerous instances where GPCC did not comply with vendor guidelines and generally accepted industry practices in administering and implementing operating system and access security software controls on its mainframe computer. Key deficiencies identified included:

- Improper controls over critical MVS operating system components, such as the system initialization (start up) parameters and options and the authorized program facility.
- Unrestricted access to, and use of, powerful system programs, such as CICS transaction utility programs, with data altering capabilities from the production CICS environment.
- Inadequate controls over system programmer access to terminals capable of emulating the master console.
- Inadequate change control procedures over modifications made to the CICS environment.
- Unrestricted access to, and control over, critical network performance and monitoring resources.
- Improper installation and controls over ACF2.
- Unmonitored and unmanned access to the data center facility during certain hours.
- Unprotected commercial software products--i.e., certain vendor products have not been interfaced with ACF2.
- Improper controls over the mainframe production environment associated with system programmers who install and maintain system software on the Center's mainframe computer, application programmers who are responsible for maintaining FFS, and separated/terminated employees.

In this area, we made a total of 32 recommendations to address the above issues as well as other related issues--described in Appendix A of this report--and improve the integrity and security of mainframe physical and logical controls.

Telecommunications Security

We found unrestricted user access through the Internet which poses integrity and security exposures to internal systems (e.g., the mainframe computer and certain LANs). In this area, we made two recommendations to address this issue--described in Appendix A of this report--and minimize the exposures associated with GPCC's telecommunications environment.

LAN Protection

We found numerous instances where DOI and USGS did not exercise proper controls in administering and managing its LANs, which are connected to the mainframe computer processing FFS data. Some of the key deficiencies included:

- Inconsistent management and administration practices between three LAN servers.
- Improper controls over user passwords on, and general access to, a particular LAN environment.
- Inadequate controls over powerful access privileges (e.g., supervisor privileges) to the LAN.
- Lack of procedures for monitoring LAN access and usage.
- Incomplete and untested contingency, backup, and disaster recovery plan to ensure the timely recovery and resumption of operations.
- Inadequate physical security controls to safeguard file servers, workstations, and network components.
- Inconsistent requirements for installing and using virus detection software on file servers and workstations.

In this area, we made 17 recommendations to address the above issues as well as other related issues--described in Appendix A of this report--and improve controls over DOI's and USGS's LAN environment.

Contingency Planning, Backup, and Disaster Recovery

The GPCC's contingency planning, backup, and disaster recovery for the FFS mainframe processing environment was inadequate and did not allow for complete business resumption. Key deficiencies identified included:

- Lack of contingency, backup, and disaster recovery plan for addressing telecommunications systems.
- Lack of a comprehensive contingency, backup, and disaster recovery plan for WASC's business and user operations.

In this area, we made three recommendations to address the above issues as well as other related issues--described in Appendix A of this report--and improve procedures and controls.

Conclusion

The internal control deficiencies described in this report could have had a significant impact on the House's decision to implement FFS. However, USGS and House management worked collaboratively with the audit team as key deficiencies related to FFS processing were brought to their attention. They took immediate corrective actions to resolve serious deficiencies, which could have had a direct adverse effect on the integrity and security of the House's financial data and FFS processing. USGS management also initiated efforts to correct the other remaining deficiencies, which do not adversely impact FFS processing but nevertheless are important to the overall integrity and security of data center operations. In addition, as suggested by USGS management, we have annotated the specific recommendations that are of greater importance to help management prioritize their use of resources in implementing our recommendations. Consequently, we believe that the actions taken and the continuing commitment demonstrated by USGS management to resolve the deficiencies identified has greatly reduced the risk to GPCC's processing environment.

Management Response

On August 20, 1996, the Office of the Director of USGS generally concurred with all 42 findings and 71 recommendations directed to USGS (see Appendix B). USGS has already implemented a number of recommendations either in their entirety or has initiated corrective actions to implement them. Examples of actions taken include: (1) implementing existing capability to monitor remote access activities and review reports; (2) removing duplicate APF libraries; (3) performing additional mainframe disaster recovery testing and preliminary

telecommunications testing between USGS and the backup location; and (4) updating existing disaster recovery documents, including documentation distribution requirements.

As indicated in their response to this report, numerous other corrective actions are planned to improve security and internal controls over the FFS processing environment at the GPCC. Examples of key actions planned include: (1) developing requirements for ongoing support and maintenance of FFS; (2) reviewing the existing application/operating system change control procedures and where necessary enhance and consolidate procedures across all application and/or operating system platforms; (3) developing and implementing policies and procedures addressing LAN operations and administration; (4) implementing tighter ACF2 controls over USGS and external user access to the FFS application, House data, sensitive programs, and GPCC mainframe computer; (5) logging and reviewing activities associated with sensitive transactions and powerful access privileges; (6) implementing controls to improve physical security over GPCC access; (7) evaluating the feasibility of interfacing all MVS-related software with ACF2; (8) developing an ACF2 procedures manual addressing ACF2 security administrator responsibilities, local security coordinators responsibilities, security problem/violations, escalation procedures, and logon identification (ID) recertification procedures; (9) segregating the WASC security administration functions from the software installation/data conversion functions; (10) establishing special purpose logon IDs for routine maintenance; (11) establishing formal policies and procedures for the LAN environment, logical and physical security, and user access controls and monitoring procedures; and (12) developing a comprehensive business recovery plan for the business functions of WASC.

In addition, the response included alternative corrective actions for 5 recommendations, including subparts--i.e., Recommendations 3.A., 3.B., 3.C., 14, and 20. Examples of these proposed actions included: (1) implementing much stronger authentication techniques and eliminating "reusable" passwords; (2) developing a comprehensive network security program, which will include security control techniques over IP access; (3) assessing the possibility of implementing the ACF2 user modification option to resolve the NetView security access exposure; and (4) reviewing and implementing an ACF2 User Mod, Firecall ID⁶ feature for emergency use.

On July 29, 1996, the Office of the CAO fully concurred with two findings (i.e., Weaknesses 4 and 7) and two recommendations directed to the CAO (see Appendix C). (Weakness 4 and its associated recommendation were also directed to USGS, and thus both organizations were responsible for implementing this one recommendation.) Beginning July 23, weekly conferences between CAO and USGS officials were initiated to review and plan activities involving the operating system, telecommunications, CICS, and application areas. The meetings have already

⁶A firecall ID is a logon ID with special or powerful security access privileges, established to handle emergency situations. This logon ID provides individuals, such as systems programmers, with controlled access to system data and files. That is, its use is logged and monitored on a regular basis.

resulted in establishing preliminary problem escalation procedures and will enable them to further develop formal procedures, and processes to control and manage systems operations and establish effective problem avoidance/escalation procedures. Lastly, the CAO stated that House Information Resources will be ensure that all FFS printed output is labeled as sensitive.

Office of Inspector General Comments

The actions taken by USGS management and/or the CAO for several recommendations (i.e., Recommendations 3.E., 7.A., 10.A., 10.B., 13.A., 15.A., 15.B., 18, 23, 25, 41, and 42) are responsive and satisfy the intent of our recommendations. We, therefore, consider these recommendations closed. In addition, both USGS management's and CAO's actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations. Further, the milestone dates provided appear reasonable.