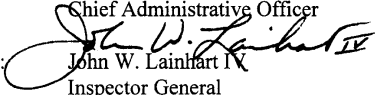


**John W. Lainhart IV**  
Inspector General

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

**MEMORANDUM**

TO: James M. Eagen III  
Chief Administrative Officer

FROM:  John W. Lainhart IV  
Inspector General

DATE: November 12, 1998

SUBJECT: Audit Report – Additional Controls Needed Over The Data Processing Environment At The U.S. Geological Survey, Reston Enterprise Data Services Center (Report No. 98-CAO-13)

This is our final report on the general controls audit of the U.S. Geological Survey (USGS), Reston Enterprise Data Services Center (EDSC) 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 (FFS) and the processing of U.S. House of Representatives (House) financial data at EDSC.

The body of the report summarizes the findings at a high level. Because the audit identified weaknesses that could 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 Exhibit 1 of this report. Exhibit 2 summarizes the implementation status of each of the 72 recommendations aimed at resolving 42 weaknesses identified in our prior audit report, entitled *Stronger Controls Needed Over The Data Processing Environment At The U.S. Geological Survey, Reston General Purpose Computer Center* (Report No. 96-CAO-09, dated December 17, 1996). Both exhibits are confidential and may not be disclosed or released to anyone other than House or DOI management except by approval of the House OIG or DOI/OIG.

In this report, we identified 19 information systems management and security control-related weaknesses. As a whole, these weaknesses increase the risk of unauthorized access and modifications to, and disclosure of, House and other agency information processed on EDSC's mainframe computer. Additionally, some of the weaknesses increase the potential for operational errors, which can adversely affect service continuity. Accordingly, we made a total of 25 recommendations for corrective actions. While the majority of these weaknesses and recommendations are directed to USGS, we identified one weakness involving off-site storage of the House's FFS back-up tapes which, in the event of a disaster, could result in a loss of a large

volume of House financial data. Accordingly, we made one recommendation to your office for corrective action. The remaining 24 new recommendations and the 13 prior recommendations, which are still not fully implemented, are directed to USGS, but should also be of interest to the House from the standpoint of House financial data processing integrity and security.

In response to our August 4, 1998 draft report, you fully concurred with the weakness identified and the associated recommendation. Your verbal response is included in Exhibit 1 of this report under Weakness 17. The corrective action taken by your office to resolve this weakness satisfies the intent of our recommendation. In addition, USGS management concurred with the remaining 18 weaknesses identified and 24 recommendations. USGS's formal management response is summarized in Exhibit 1 and is included in its entirety as a confidential appendix (see Appendix). The actions taken and planned by USGS are appropriate and, when fully implemented, should satisfy the intent of the recommendations. Further, the milestone dates provided by USGS for completing actions appear reasonable.

Since our first audit, USGS has notably improved controls over its mainframe operations, system software, and telecommunications security. While we believe the additional weaknesses identified are important to the USGS and the House, we do not consider these weaknesses to constitute a material internal control weakness under the Federal Managers' Financial Integrity Act of 1982 materiality criteria established by the Office of Management and Budget.

We appreciate the courtesy and cooperation extended to us by your staff. If you have any questions or require additional information regarding this report, please call me or Robert B. Frey III at (202) 226-1250.

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

Since September 1995, the Chief Administrative Officer (CAO) has entered into cross-servicing agreements with the U.S. Geological Survey (USGS) to implement and customize 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 Enterprise Data Services Center (EDSC), formerly known as the Reston General Purpose Computer Center, located in Reston, Virginia. The application is supported by the USGS, Washington Administrative Service Center (WASC). Other services EDSC provides to the House 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 periodically assesses the adequacy of EDSC's data processing environment. This audit report is the result of our latest assessment.

FFS was purchased by USGS in 1987 and subsequently implemented in the Department of Interior's (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.

EDSC, 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 IBM 9672 mainframe computer running IBM's Multiple Virtual Storage (MVS) Extended Systems Architecture (ESA) operating system, version 5.1. In late 1997, EDSC installed new access control security software on the mainframe, IBM's Resource Access Control Facility (RACF), replacing Computer Associates' Access Control Facility 2. The security software not only controls user access to the FFS dedicated Customer Information Control System<sup>1</sup> (CICS) applications, but also access to the Time Sharing Option<sup>2</sup> (TSO) facility and numerous vendor products. In addition to this standard system-level security, FFS contains data base level security that controls the actual system functions that a user may invoke. Other system software, such as data base management software, telecommunications software, and specialized vendor software products, also reside on the mainframe computer.

Network and local communications support for both asynchronous and synchronous protocols<sup>3</sup> are provided, as well as local area network (LAN) connectivity via Ethernet<sup>4</sup> and Transmission Control Protocol/Internet Protocol<sup>5</sup>.

---

<sup>1</sup>CICS is an IBM software product that serves as the teleprocessing monitor for the MVS operating system on EDSC's 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.

<sup>2</sup>TSO is an IBM software product that serves as the session manager on EDSC's 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.

<sup>3</sup>Asynchronous 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.

<sup>4</sup>Ethernet 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.

<sup>5</sup>Transmission 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., clusters of data) from one network to another.

**Objectives, Scope, and Methodology**

This review was initiated and led by the House Office of Inspector General (OIG) and coordinated with the DOI/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 EDSC. The review focused on evaluating the adequacy of management and internal controls over the following general control areas:

- Data center management and operations;
- Mainframe systems logical and physical security;
- Telecommunications security;
- LAN protection; 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 focused on a number of control issues, including (1) standards, policies, and procedures; (2) user authentication; (3) protection of information and information systems from unauthorized access, modification, or destruction; and (4) backup and recoverability of information, systems, and telecommunications links in the event of a disruption in operations. The assessment of business continuity planning and ongoing operations also included the review of the ability of EDSC's hardware and software to function in the Year 2000.

We conducted our review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Our review covered the period of January 1997 through May 1998. Our audit work was performed during the period of April 10 through June 5, 1998, and consisted of the following specific tasks:

- Gathered pertinent documentation, including standards, policies, and procedures;
- Conducted discussions and interviews with key USGS and House officials;
- 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 EDSC'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;
- Compared critical MVS operating system and other pertinent system software control

parameters and option settings implemented on the mainframe computer against vendor recommended guidelines and industry practices;

- Conducted a review of custom-designed and vendor-supplied Supervisor Calls (SVC)<sup>6</sup>;
- Utilized third party audit and security software tools to perform a number of the automated testing techniques to assess the status of EDSC's operating system and system software environment; and
- Performed a follow-up of the status of prior audit recommendations.

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

### **Internal Controls**

We evaluated internal controls related to the integrity, confidentiality, and availability of EDSC's mainframe and other information system environments, which could adversely affect the House FFS data and FFS processing. Although notable improvements have been made in EDSC's mainframe operations, system software controls, and telecommunications security controls since our 1996 audit, we identified significant internal control weaknesses, including weaknesses that remain uncorrected. These weaknesses involve EDSC's MVS libraries, overall security function and administration, RACF security access controls, CICS sensitive transaction controls, and business continuity planning, including Year 2000 readiness. An overview of the internal control weaknesses identified are described in the "Results of Review" section of this report and in Exhibit 1. While we believe that the weaknesses identified are important to the USGS and the House, we do not consider these weaknesses to constitute a material internal control weakness under the Federal Managers' Financial Integrity Act of 1982 materiality criteria established by the Office of Management and Budget.

### **Prior Audit Coverage**

One prior audit was performed by the House OIG, in conjunction with DOI/OIG, which relates to the overall FFS application processing and the general controls environment at EDSC. The audit results were reported in two separate OIG reports: House OIG Report No. 96-CAO-09 and DOI/OIG Report No. 97-I-98, both issued in late 1996. The reports are identified below, followed by a synopsis of their contents.

- *Stronger Controls Needed Over The Data Processing Environment At The U.S. Geological Survey, Reston General Purpose Computer Center* (House OIG Report No. 96-CAO-09, dated

---

<sup>6</sup>SVCs (also known as operating system extensions) are special machine instructions within the operating system environment which application programs use to communicate with the operating system. For example, a "calling program" uses the SVC mechanism to request the operating system to perform a desired system service routine, such as opening a data file for modification.

December 17, 1996) and *General Control Environment Of The Federal Financial System At The Reston General Reston General Purpose Computer Center, U.S. Geological Survey* (DOI/OIG Report No. 97-I-98, dated November 15, 1996). Both reports disclosed that USGS had 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. The prevailing reasons for many of these deficiencies were attributed to the lack of formal data center standards, policies, and procedures; improper practices and processes for control and administration of data security within the center; lack of segregation of duties; noncompliance with key vendor guidelines for MVS integrity; and lack of a formal, comprehensive data security program. Overall, the reports identified 42 significant information systems integrity weaknesses and made a total of 72 recommendations for improving the general controls environment at the GPCC.

Exhibit 2 provides a summary of the implementation status of each of the recommendations in the above reports.

## II. RESULTS OF REVIEW

The results of our evaluation of the general controls environment surrounding FFS and House financial data processing at the USGS showed marked improvement since our 1996 audit. For example, USGS:

- Placed all systems and programs under the control of the RACF access security software;
- Obtained base level security clearances for all employees requiring access to the data center;
- Restricted passwords so that they are only routed through the segments of the network required for verification, thereby, limiting their exposure to unauthorized detection;
- Established and implemented formal change control procedures for mainframe applications;
- Implemented controls over the mainframe operating system and the access security software; and
- Established a disaster recovery plan to minimize disruptions to operations.

USGS's progress is clearly evident from the results of our follow-up work on the 72 prior audit report recommendations aimed at resolving 42 weaknesses identified in House OIG Report No. 96-CAO-09, entitled *Stronger Controls Needed Over The Data Processing Environment At The U.S. Geological Survey, Reston General Purpose Computer Center*, dated December 17, 1996. (Of the 72 recommendations, only 2 recommendations related to FFS administration and maintenance, and information protection weaknesses were directed to the CAO for action, one of which required the CAO to work jointly with USGS to resolve the weakness.) The results of our follow-up work on the 72 prior audit recommendations showed that corrective actions were completed<sup>7</sup> for 39 recommendations. In addition, two recommendations were otherwise resolved<sup>8</sup> and seven were

---

<sup>7</sup> Action taken fully implements the recommendation or changes in USGS operations remedied this weakness or eliminated the problems affected by the weakness.

<sup>8</sup> Changes in the nature of operations eliminated the significant concerns underlying the recommendation

superseded by new recommendations. Of the remaining 24 open recommendations<sup>9</sup>, substantial progress<sup>10</sup> was made on 2, some progress<sup>11</sup> was made on 8, limited progress<sup>12</sup> was made on 6, and no actions were taken on 8. As these statistics indicate, the majority of the report recommendations have been implemented and action has been taken on most of the remaining recommendations, thereby improving general controls over the FFS mainframe processing environment. (Exhibit 2 lists the 72 prior recommendations with comments on the recommendations not completed including the corrective actions taken and/or planned, and actions needed for closure.)

Notwithstanding these notable improvements in system software controls, we identified 19 weaknesses that span the following 4 general control areas: (1) data center management and operations; (2) mainframe systems logical and physical security; (3) telecommunications security, and (4) contingency planning, backup, and disaster recovery. In addressing the fifth general control area (i.e., LAN protection), we evaluated USGS's progress in improving controls over this environment and found the risk for uncompleted actions to be extremely low on an overall basis. LAN-related issues were identified as part of three weaknesses under the data center management and operations, mainframe systems logical and physical security, and telecommunications security areas. However, from the House's standpoint, no House data is stored or transmitted through the DOI or USGS internal LANs. While USGS management can benefit by fully implementing our prior audit LAN-related recommendations, we are not reporting any additional weaknesses in this area.

The 19 weaknesses include weaknesses originally identified in our prior audit and new weaknesses that could have a significant adverse impact on data processed at EDSC, if left unaddressed. Collectively, these weaknesses increase the risk of unauthorized access and modifications to, and disclosure of, House and other agency information processed on EDSC's mainframe computer. Additionally, some of the weaknesses increase the potential for operational errors which can adversely affect service continuity. In addition to the 13 prior audit recommendations still not fully implemented<sup>13</sup>, we made 24 new recommendations for addressing the weaknesses and improving the general controls environment at EDSC. (A detailed discussion of the weaknesses and associated recommendations for each general controls area are contained in Exhibit 1 of this report.)

The primary reasons for these deficiencies include, but are not limited to, the following: lack of formal standards, policies, and procedures; inappropriate practices and processes; inadequate security review and monitoring of sensitive system and data access activities; noncompliance with vendor guidelines for MVS integrity; and lack of a comprehensive data security program.

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

The Office of Management and Budget and the National Institute of Standards and Technology

---

<sup>9</sup>Recommendations which still require action to be fully implemented.

<sup>10</sup>Action taken substantially addresses the more significant aspects of the recommendation.

<sup>11</sup>Action taken partially addresses the more significant aspects of the recommendation.

<sup>12</sup>Action taken addresses the less significant aspects of the recommendation.

<sup>13</sup>The other 11 prior audit recommendations that remain open are not included because they relate to DOI or USGS LANS which do not store House data and represent an extremely low risk as they relate to House FFS data.

(NIST) have issued numerous directives, policies, and guidelines calling for Federal agencies to establish and implement overall management and computer security controls to improve internal controls over system software, and application programs and data in Executive Branch agencies' computer systems. NIST has specifically prescribed guidelines for achieving strong disciplines and a clearly defined approach to software maintenance, including change management, to assure smooth operational continuity. 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.

More recently, the 2<sup>nd</sup> Edition of *COBIT: Control Objectives For Information and Related Technology* (published by the Information Systems Audit and Control Association, April 1998) provides guidelines and tools based on established best practices for managers in both the public and private sector to establish controls for ensuring the confidentiality, integrity, and availability of information as well as the protection of other information technology resources. Such controls normally encompass adequate change management processes, proper reporting structure, segregation of duties, establishment of computer and data security standards, policies, and procedures, risk analyses, application controls, independent reviews, Year 2000 date impact compliance, and other control-related mechanisms to ensure effective management and protection of sensitive information and other information technology resources.

Additional controls are needed to ensure the effective management and protection of sensitive information and other information technology resources within EDSC's information systems environment. The following is a summary of each of the four major general control areas, highlighting key deficiencies identified during the course of the audit, which are discussed in Exhibit 1.

### **Data Center Management And Operations**

We noted deficiencies in the areas of data center management and operations where controls should be improved to reduce unnecessary risk to system integrity, confidentiality, and availability. Key deficiencies include:

- Inadequate systems assurance reviews of proposed system software changes by either a systems programmer or a team of systems programmers for appropriateness of the changes/solutions, test plans, and their impact on the systems environment and the FFS application prior to implementation.
- Inadequate problem resolution procedures for ensuring that all incoming calls are logged into, and tracked by, the help desk system.
- Insufficient details to support FFS processing and other service charges appearing on House bills from USGS.

In this area, we made three new recommendations and referenced five prior recommendations to address the deficiencies and improve data center management and operations.



### **Mainframe Systems Logical And Physical Security**

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

- An excessive number of USGS personnel have the ability to access and modify the critical MVS authorized program facility libraries, including two individuals no longer working at the USGS.
- Implementation of new software products on EDSC's mainframe computer without prior review for proper set-up of security parameters and approval by the Security staff.
- Inadequate controls over the assignment of the RACF "Operations" and "Special" attributes for ensuring that programs initiated as started tasks cannot process in a state which bypasses security software controls.
- Inadequate controls over WASC and non-government (i.e., contractor) application programmers who have "write" and "allocate" access to the FFS production libraries and data.
- Ineffective set-up of RACF options for ensuring proper password administration and data protection on EDSC's mainframe computer.
- Use of sensitive CICS supplied transactions with data altering capabilities in the House CICS production region as well as unrestricted access to such sensitive CICS transactions by application and systems programmers.

In this area, we made 17 new recommendations and referenced 8 prior recommendations to address the deficiencies and improve the integrity and security of mainframe physical and logical controls.

### **Telecommunications Security**

We found that unrestricted user access to USGS through the Internet still poses integrity and security exposures to the agency's internal systems (e.g., the mainframe computer and certain LANs), because passwords are not encrypted in the network. In this area, we made one recommendation to address the deficiency and eliminate the exposure associated with EDSC's telecommunications environment.

## **Contingency Planning, Backup, And Disaster Recovery**

A large volume of House FFS data could be lost without the ability to recover the lost data, except through its reentry. In addition, EDSC's contingency planning, backup, and disaster recovery procedures do not provide reasonable assurance that the FFS mainframe processing environment will be able to operate after Year 2000. Key deficiencies identified include:

- Inadequate rotation of backup tapes to off-site storage to facilitate full recovery of data in the event of a prolonged disruption or disaster at the data center
- Lack of a designated EDSC Year 2000 coordinator to ensure that all vendor software and hardware on EDSC's mainframe computer are identified for remediation and testing to ensure ongoing operations of the data center infrastructure.
- Inadequate testing of disaster recovery plan; no evidence to ensure that disaster recovery testing was performed by users at the House.

In this area, we made four recommendations to address the deficiencies and ensure that USGS and House personnel are sufficiently prepared to quickly recover from unforeseen disruptions, such as a prolonged outage or disasters.

## **Conclusion**

Since the release of our prior audit report in November 1996, USGS has made significant progress in addressing weaknesses and recommendations identified in that report. However, significant weaknesses related to mainframe systems logical and physical security, and contingency planning, backup, and disaster recovery still remain which require immediate attention. To a lesser extent, we also identified weaknesses in data center management and telecommunications, which also need to be addressed. Overall, while we consider all the weaknesses as important to the USGS and the House, we do not believe that they constitute a material internal control weakness under the Federal Managers' Financial Integrity Act of 1982 materiality criteria established by the Office of Management and Budget.

## **Management Response**

On October 5, 1998, the Chief Administrative Officer (CAO) verbally responded to a draft finding (i.e., Weakness 17), and fully concurred with the issue identified and the associated recommendation (i.e., Recommendation 17). In late June 1998, his office requested WASC to provide daily off-site storage of the House's FFS application and database backup tapes. Accordingly, the CAO informed us that WASC implemented this procedure on August 27, 1998.

On October 15, 1998, the Office of the Director of USGS generally concurred with the remaining 18 weaknesses and 24 recommendations directed to them (see Appendix). According to the response, actions were completed for 2 (i.e., Recommendations 6.C and 18.A) of the 24 recommendations and included: (1) requiring that security noncompliance problems involving

EDSC users be elevated to the responsible department level security officials to enforce compliance; and (2) establishing a Year 2000 Team to oversee the Year 2000 compliance efforts for EDSC's software and hardware.

The response also indicated that numerous other corrective actions were underway or planned for addressing the remaining 22 recommendations. These include: (1) developing and implementing change management procedures for the LAN environment; (2) conducting an Overhead Rate Study/Review to document and determine an appropriate rate to use in preparing subsequent interagency agreements; (3) providing appropriate reports to support time and charges billed to the House for WASC services; (4) revising the APF library semi-annual review process to include documented justification for systems programmer access in addition to management signoff; (5) logging systems programmer access to APF libraries, and implementing procedures for distributing reports to systems programming management for review; (6) reviewing authorized changes based on change control documentation; (7) revising the security review process to include contact with vendor representatives to ensure the required software controls are available and implemented; (8) establishing a policy to ensure security administration has the responsibility to review and control all software product implementations from a security perspective; (9) reviewing a specific RACF option and removing the privilege or providing the necessary documentation to justify the requirement where appropriate; (10) establishing guidelines for requesting/authorizing application programmer access to production programs and data; (11) revising RACF access rules based on review results; (12) implementing procedures for security administration staff to periodically review and monitor access controls implemented by all Security Coordinators; (13) reviewing and implementing the password characteristics identified, and implementing the erase on scratch once proper testing has been performed; (14) establishing a policy to require the creation of RACF groups to meet specific access requirements; (15) implementing appropriate features to eliminate the potential for eavesdropping on USGS's network; (16) requiring application programmers to use hardwire connections when accessing House data; (17) revising the USGS Manual to address a comprehensive Bureau-wide Security program that includes all platforms; (18) reviewing for, and limiting, access to the use of a specific CICS transaction; (19) developing and documenting procedures for periodic reviews of data center physical access privileges; (20) developing a comprehensive security program to protect the overall internal network; (21) coordinating activities to identify and resolve all areas that would be affected by the Year 2000 problem across the information system infrastructure within EDSB; and (22) conducting and documenting a comprehensive disaster recovery test associated with the House's FFS processing requirements, and resolving problems identified.

### **Office Of Inspector General Comments**

The action taken by the CAO is responsive to the issue identified and satisfies the intent of the recommendation. We therefore consider Recommendation 17 closed.

Based on the actions completed by USGS, we consider Recommendations 6.C and 18.A closed. The actions taken and planned for the remaining 22 recommendations are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendations. Further, the milestone dates provided for completing these actions appear reasonable.