John W. Lainhart IV
Inspector General

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

MEMORANDUM

TO: Scot M. Faulkner
Chief Administrative Officer

John W. Lainhart IV

FROM: John W. Lainhart IV
Inspector General

DATE: July 18, 1995

SUBJECT: Audit Report - House Computer Systems Were Vulnerable To Unauthorized Access, Modification, And Destruction (Report No. 95-CAO-18)

This is our final report on the performance audit of data security. The objective of the audit was to assess effectiveness of data security within the House to ensure integrity, confidentiality, and availability of information resources. In this report, we identified problems associated with the operational practices of Human Resources and made recommendations for corrective actions.

In response to our June 26, 1995 draft report, your office concurred with our findings and recommendations. The formal management response provided by your office is incorporated in this final report and included in its entirety as an appendix. The corrective actions taken and planned by 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. However, we would appreciate you providing us milestone dates for several pending actions as indicated in the report once the Committee on House Oversight has made a decision on your data security proposal and the Security Administrator position is filled.

We appreciate your office's positive response and concurrence with the recommendations, and 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 Craig W. Silverthorne 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

HOUSE COMPUTER SYSTEMS WERE VULNERABLE TO UNAUTHORIZED ACCESS, MODIFICATION, AND DESTRUCTION

Report No. 95-CAO-18
July 18, 1995

RESULTS IN BRIEF

CONCLUSIONS

A high risk of unauthorized access, modification, and destruction of data residing on Member, committee, and other House offices computer systems existed within the House information systems environment. Systems supported by the House Information System (HIS[1]) organization and outside vendors were vulnerable to external access. Weaknesses were noted throughout all processing environments, including HIS operations and office-level systems (i.e., local area networks, Internet[2], standalone microcomputers, and other distributed computing systems) at Member, committee, and House office locations. A comprehensive security risk program needed to be developed and major improvements were needed to improve controls over the integrity, confidentiality, and availability of information and systems.

There were a number of reasons for this conclusion:

- No risk assessment model or data classification scheme existed to form a key component of an effective data security program. Security standards, policies, and procedures were neither consistently maintained nor enforced for HIS operations, office-level systems, or vendors to determine what information needed to be protected and what mechanisms needed to be implemented to protect sensitive data. In addition, a House-wide information security awareness program that educated users on the need for security did not exist.

- The House lacked a formal, comprehensive data security program to help manage its information systems processing environment. Further, the HIS security function--responsible for overseeing and implementing House information systems security--was not adequately staffed nor appropriately placed within the HIS organizational structure.

[1] On July 14, 1995, HIS was renamed by the Committee on House Oversight and is now House Information Resources (HIR).

[2] The Internet is a large international network that connects many computer systems, providing network services including, electronic mail (i.e., e-mail), remote terminal sessions, and multi-media services such as the world-wide web.

In addition, security background checks were not consistently performed for HIS employees and not performed at all for vendors. These deficiencies substantially increase the risk of unauthorized access and modifications to, and disclosure of, House information resources. Consequently, the House was not assured that information resources were sufficiently protected from fraud, waste, unauthorized use, and mismanagement.

- Disaster recovery planning and testing for the IBM mainframe processing environment supported by HIS were inadequate. In addition, no formal disaster recovery planning and testing existed for the telecommunications infrastructure. Furthermore, no formal disaster recovery planning and testing existed for the office-level computer processing environment, supported by both HIS and external vendors. As a result, the House could not be sufficiently prepared to handle potential business interruptions resulting from prolonged computer outages, emergencies, or disasters.

- The House did not have adequate or appropriate security software controls in place over House information resources. Serious security control deficiencies were identified involving House e-mail systems, administration and implementation of Access Control Facility 2 (ACF2) security software controls, Customer Information Control System (CICS), access to sensitive production resources, and the use of a production scheduler. In addition, controls were inadequate over UNIX[3] systems, local area networks (LANs), standalone microcomputers, fileservers, and correspondence management system (CMS) operating systems and databases. Without effective security controls over information resources and user access to such resources, the House substantially increased the risk of unauthorized access and modifications to, and disclosure of, sensitive House data. Consequently, the House was not assured that information resources were sufficiently protected from fraud, waste, unauthorized use, and mismanagement.

- Significant weaknesses existed in the data security environment surrounding remote dial-in access to office-level systems (see Report No. 95-CAO-01).

- Significant weaknesses existed in the controls over access to the House network and Member office systems via the Internet through external agencies on CapNet[4], the internal network connecting the various Legislative Branch agencies (see Report No. 95-CAO-03).

[3] UNIX is a proprietary general-purpose multi-tasking operating system originally developed by Bell Laboratories and MIT and distributed by a number of vendors, including AT&T, SUN, Digital, and Hewlett Packard.

[4] CapNet is the internal network connecting the various Legislative Branch agencies, including the House.

As the House moves to a more "open" and distributed environment, data security needs to be carefully managed, balancing the Member office needs to access a wide range of information via diverse technologies with the appropriate level of security over sensitive data, such as e-mail or Member correspondence.

RECOMMENDATIONS

We recommend that the Chief Administrative Officer develop proposals, for approval by the Committee on House Oversight, to: (1) implement a formal, comprehensive data security program; (2) establish a plan for adequately staffing a formal data security officer function, (3) establish a plan for expanding the data security function to include broader authority to address security on House information systems, all office-level systems, mainframes, and networks; (4) implement a House-wide information security awareness program; (5) implement a data security compliance structure and enforcement mechanism; (6) establish employee security clearances requirements; (7) implement a comprehensive disaster recovery plan and procedures for HIS operations (including backup arrangements for the Network Control Center) and office-level systems; (8) implement and update the business impact analysis for critical HIS systems as well as office-level systems and telecommunications links; (9) implement an e-mail system that supports the Data Encryption Standard; (10) establish data security procedures for LANs, standalone computers, and other distributed computing systems, including UNIX, Novell Netware, Windows NT, DOS, Windows, servers, and any other operating environments supporting House systems; and (11) implement appropriate physical and environmental controls surrounding microcomputers, servers, communications equipment, and other computing facilities for Member, committee, and other House offices.

We also recommend that the Chief Administrative Officer: (1) implement procedures for the ongoing maintenance of the business impact analysis and business recovery plan as well as comprehensive, routine (e.g., minimum once a year) testing of the plan. Additionally, a full data center "power-down" test should be included in the business recovery plan; (2) implement stronger ACF2 access controls over HIR; (3) schedule all production jobs, including ad hoc jobs, through the Control/M scheduling software package; and (4) enhance controls surrounding CMS systems to ensure that users can only access data through the designed application features and not by other means that circumvent the application system; and (5) develop a plan for approval by the Committee on House Oversight to perform periodic security reviews to ensure that adequate controls are in place to protect House data and other sensitive system files.

MANAGEMENT RESPONSES

On July 11, 1995, the Office of the Chief Administrative Officer (CAO) fully concurred with the findings and recommendations in this report. According to the response, numerous initiatives are either underway or planned to significantly improve security and integrity throughout the House information systems environment, including HIR. Examples of corrective actions taken and planned include: (1) restaffing of the data security function, including hiring a Security Administrator; (2) developing and implementing a formal, comprehensive data security program; (3) preparing a proposal for approval by the Committee on House Oversight to provide HIR's security function broader authority for implementing stronger security controls over House information systems, office-level systems, network facilities, and mainframes; (4) instituting an internal data security compliance structure and enforcement program; and (5) establishing employee and vendor security clearance requirements.

In addition, the CAO intends to: (1) prepare a business impact and cost analyses that consider various levels of disaster recovery; (2) explore the feasibility of implementing DES encryption for House e-mail systems; (3) establish an audit service for providing periodic security reviews, and security consultation to offices; (4) implement more stringent prevention and detection mechanisms; and (5) revise security guidelines, including appropriate physical and environmental controls over desktop and in-office systems.

Currently, milestone dates for completion of these actions range from December 31, 1995 to February 1996. Milestone dates for completing the remaining tasks are dependent upon the approval of the CAO's data security proposal and selection of a Security Administrator.

OFFICE OF INSPECTOR GENERAL COMMENTS

The 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 for selected actions appear reasonable. However, we would appreciate you providing us milestone dates for the remaining actions once a decision has been made on the CAO's data security proposal and the Security Administrator position is filled.

TABLE OF CONTENTS

I. INTRODUCTION

Background

House Information Systems' (HIS[1]) mission is to "satisfy the requirements for information, information technology, and related computer service of the Members, committees and staff of the U.S. House of Representatives." HIS is the major provider of information technology services to the House and is responsible for the technical infrastructure and other services. It helps to shape the House information technology infrastructure by matching office needs with vendor and custom developed products and services.

The House information systems environment consists of a wide range of technologies:

- IBM mainframe;
- Mainframe communications to terminals;
- Local area networks (LANs);
- Wide area networks (WANs)
- Internet access;
- Microcomputers; and
- Minicomputers;

Member (Washington, D.C. and district), committee, and other House offices generally have individual computer systems that are used to support office operations (e.g., scheduling, correspondence management, budgeting, etc.). While some of the microcomputers and minicomputers in Washington, D.C. are stand-alone machines, most of the computers are interconnected via LANs, the HIS network, and CapNet[2]. Other connections between these offices and external parties (e.g., computer vendors, constituents, etc.) are accomplished using

[1] On June 14, 1995, HIS was renamed by the Committee on House Oversight and is now House Information Resources (HIR).

[2] CapNet is the internal network connecting the various Legislative Branch agencies, including the House.

modems[3] over phone lines located in each individual office or using the Internet through connections available on CapNet.

A data security function currently exists within HIS that primarily supports users accessing IBM mainframe systems. Computer Associates' Access Control Facility 2 (ACF2) access control software system[4] provides protection of resources processed and stored on the IBM mainframe system. The data security function within HIS administers, monitors, and maintains the ACF2 software. However, not all data or applications operating on the IBM mainframe are currently under the protection of ACF2. Alternatives to ACF2 are employed to provide protection over other IBM mainframe system resources. These alternatives provide varying levels of security.

In addition to the IBM mainframe facilities, other systems exist within the House environment that are not under the direct control of HIS, therefore, these systems require other means of security and control in order to protect system resources. These office-level systems include LANs, standalone personal computers, and other departmental computer systems. These systems may reside in Member (Washington, D.C. and district), committee and House offices. Outside vendors install and maintain the security features on office-level systems. In addition, HIS or internal office personnel also perform security administration functions.

A disaster recovery plan is in place that includes coverage of the House IBM mainframe computer facility. HIS contracted with IBM's Business Recovery Services organization for "hot site"[5] support of mainframe processing in the event of a disaster that could cause prolonged interruption of services. However, no similar agreement exists for telecommunication facilities or for office-level systems.

[3] A modem (MODulator-DEModulator) is a device that adapts a terminal or computer to a telephone line. It converts the computer's digital pulses into audio frequencies (analog) for the telephone system and converts the frequencies back into pulses at the receiving side. The modem also dials the line, answers the call and controls transmission speed, which ranges from 300 to 14,400 bits per second (bps) and higher.

[4] ACF2 access control software is a licensed product from Computer Associates. Access control software systems such as ACF2 include many features and functions that, if installed properly, provide security and control features designed to prevent and detect unauthorized or inappropriate user access to computer facilities.

[5] A hot site is a computer processing facility located separate from a primary data center, ideally several hundred miles away, that is set up to assume immediate (e.g., 24 - 48 hours) computer processing and operations in the event of a disaster or prolonged computer outage.

Objectives, Scope, And Methodology

The audits conducted as part of the overall assessment of the economy, efficiency, and effectiveness of House operations included a comprehensive review of HIS operations and the House information systems environment. The overall objective of this audit was to assess the effectiveness of data security within the House to ensure integrity, confidentiality, and availability of information resources. Integrity involves ensuring that information resources are protected from inappropriate or unauthorized modification or destruction. Confidentiality involves ensuring that information resources are protected from inappropriate or unauthorized disclosure. Availability involves ensuring that information resources are protected from processing interruptions and that information is adequately backed up and can be restored in a timely manner.

The scope of this audit included a review of the integrity, confidentiality, and availability of information resources for HIS and office-level systems. This included consideration of the general controls environment, including management, data center operations, and data center protection. Evaluation of general controls focuses on a number of control issues including user authentication, protection of information and systems from unauthorized access, modification, or destruction, and backup and recoverability of information and systems in the event of a disruption in operations. Our review of general controls focused on the following specific areas:

- Mainframe data center management and operations;
- Mainframe physical and logical security protection;
- Digital Equipment Corporation (DEC) VAX operations;
- Telecommunications and network control;
- Internet and UNIX[6] security, including firewall[7] protection;
- Office-level LANs, standalone personal computers, and other distributed systems management, operations, physical security, and logical security; and
- HIS operations and office-level backup, recovery, and contingency planning.

[6] UNIX is a proprietary general-purpose multi-tasking operating system originally developed by Bell Laboratories and MIT and distributed by a number of vendors, including AT&T, SUN, Digital, and Hewlett Packard.

[7] A firewall is a combination of computer hardware and software designed to control the flow of information between an organization's internal systems and systems outside the organization.

We conducted our review in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Our review of HIS operations and House information systems was performed during February through May 1995. In conducting this review, we performed the following specific tasks:

- Gathered documentation and conducted interviews;
- Identified business objectives and control techniques consistent with sound data security standards based on current industry standards;
- Gained an understanding of the internal control environment surrounding data security, including integrity, confidentiality, and availability of information resources;
- Assessed the risks surrounding the House information system data security environment and developed a test matrix based on this assessment;
- 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.

We also applied computer and information systems audit guidelines used at Federal government and private industry computer installations in evaluating the effectiveness of HIS and office-level systems security. These guidelines and standards are described in government and private industry publications, such as:

- National Institute of Standards and Technology's (NIST) Federal Information Processing Standards (FIPS)
- NIST's Special Publication 500-153, *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*
- Information Systems Control Foundation, *Computerized Information Systems (CIS) Audit Manual*
- Institute of Internal Auditors' - *Systems Auditability and Control Report*
- Price Waterhouse LLP Systems Management Methodology (SMM) *Data Security Review, Information Systems Risk Management and Disaster Contingency Planning Modules*

Although the House is not mandated to comply with the standards used in our review, they represent sound practices that other government agencies and private industry follow.

Security and control of House information resources is a sensitive matter. Access to Member information resources, including correspondence, legislative matters, electronic mail (i.e., e-mail), scheduling, budgeting, and financial data should be handled with utmost care and confidentiality. The results of this audit and report address these sensitive issues and provide recommendations for eliminating control weaknesses, mitigating future risk, and improving the awareness of House Members, and staff to the importance of sound data security practices.

Internal Controls

This review evaluated internal controls related to data security, including integrity, confidentiality, and availability of the House information systems environments. The audit disclosed serious internal control weaknesses involving the House security program and functions, disaster recovery planning and testing, and security access controls. The internal control weaknesses, we identified in performing this audit, are described in findings A, B, and C of this report.

Prior Audit Coverage

As part of a comprehensive review of HIS operations, we are preparing a series of reports addressing weaknesses associated with the House information systems environment. The results of three are summarized below:

Internet Security Weaknesses (Report No. 95-CAO-03): This report noted serious weaknesses surrounding access to the House network and Member office systems via the Internet through external agencies on CapNet. The report identified the capability for unauthorized individuals to access Member systems and read mail in a Member's correspondence management system. For example, we were able to read a Member's mail and other data, and send an e-mail message to the Inspector General's office posing as that Member. Consequently, we exploited a "back door" into the House network, and we easily and effectively bypassed the HIS firewall installed to protect the HIS "front door" into the network. The report contained nine recommendations to correct the internal control weaknesses and prevent recurrence. HIS agreed to correct these deficiencies and is taking corrective actions.

Information Systems Security Weaknesses (Report No. 95-CAO-01): This report noted serious weaknesses surrounding remote dial-in access to House office-level systems. The report identified the capability for unauthorized individuals to access member systems and read mail in a Member's correspondence management system. The report also identified the capability to change outgoing correspondence in a Member's system to alter the position of the Member on a sensitive issue. Collectively, these weaknesses highlight the risks associated with dial-in access and the need for improved security to reduce the risk of access to sensitive House computer resources by unauthorized individuals. The report contained seven recommendations to correct the internal control weaknesses and prevent recurrence. HIS agreed to correct these deficiencies and is taking corrective actions.

Proposed New Financial Management System Will Not Meet the House's Needs And Should Be Terminated (Report No. 95-CAO-02) : This review evaluated the functional adequacy of the proposed FMS and the system development life cycle procedures that were utilized in the development of the system. This report recommended that the system be terminated and also made recommendations to improve the systems development practices with HIS as well as management oversight.

In addition, three management advisory services studies were performed for HIS addressing various aspects of the data security environment, as described below:

Computer Emergency Response Team (CERT) Coordination Center - Report on HIS Internet Connectivity Issues, March 1994: This review covered security issues related to connecting HIS and office systems to external organizations through the Internet. CERT provided several issues for HIS to evaluate and implement solutions to as they connected HIS and office-level systems to the Internet.

Trusted Information Systems (TIS), Inc. - Report on CapNet Network Security, February 1994: This review presented security issues related to connecting HIS and office systems to external organizations through the Internet. TIS provided various strategies for implementing firewalls between HIS and office-level systems and the Internet.

Deloitte & Touche (D&T) House Information Systems Information Security Plan Report, March 1990: This review analyzed HIS information system security and prepared a plan for improving and maintaining system security. D&T recommended 15 major action items that needed to be accomplished to meet the provisions of the Computer Security Act of 1987 (Public Law 100-235). These action items addressed security administration, security organization, policies and procedures, business continuity, mainframe security, office level systems security, vendor security and personnel security.

The reviews described above included assessment of various aspects of the security environment within the House. A number of findings and recommendations resulted from these projects, however, very few corrective actions appears to have resulted from these reviews and many of the findings and recommendations have not been fully addressed or implemented.

II. FINDINGS AND RECOMMENDATIONS

Finding A: The House Should Establish And Implement A Comprehensive Data Security Program For Both HIS Operations And Office-Level Systems

The House lacked a formal, comprehensive data security program to help manage its information systems processing environment. Further, the HIS security function--responsible for overseeing and implementing House information systems security--was not adequately staffed nor appropriately placed within the HIS organizational structure. In addition, security background checks were not consistently performed for HIS employees and not performed at all for vendors. These deficiencies substantially increase the risk of unauthorized access and modifications to, and disclosure of, House information resources. Consequently, the House was not assured that information resources were sufficiently protected from fraud, waste, unauthorized use, and mismanagement. These deficiencies were attributed to the lack of formal standards, policies, and procedures on House data security administration as well as the lack of employee and vendor security background requirements. Further, the security background check-related deficiencies were attributable to HIS' practice of using inappropriate contractual mechanisms, such as purchase orders, that did not allow for security provisions.

An aggressive, yet balanced overall security program needs to be developed and implemented in order to meet the business and technical risks faced by the House. As the House moves to a more "open" and distributed environment, data security needs to be carefully managed, balancing the Member office needs to access a wide range of information via diverse technologies with an appropriate level of security over sensitive data, such as e-mail or Member correspondence.

Federal government and private industry data security guidelines and practices are well-established

The Office of Management and Budget and the National Institute of Standards and Technology have issued numerous directives, policies, and guidelines calling for Federal agencies to improve the security and privacy of sensitive information in Executive agency computer systems. Congress, itself, 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 private sector, generally accepted security practices include the establishment and implementation of comprehensive information system security programs. Such programs normally encompass proper reporting structure, segregation of duties, establishment of computer and data security standards, policies, and procedures, risk analyses, personnel security requirements, and other security-related issues to ensure effective management and implementation of data security.

A comprehensive data security program and centralized security function is needed to correct weaknesses that currently exist within the House and HIS environment

Data security weaknesses were noted in the House, including the absence of:

- A formal, comprehensive data security program. This program should include:
    - Scope and purpose of the policy and the facilities, systems, and personnel covered by the policy;
    - Data security standards, policies, and procedures;
    - Security strategy and how it links to the House's overall information technology strategy;
    - Objectives of security strategies and methods to achieve success;
    - Accountability and responsibility at all levels of the organization;
    - Definition of violations and penalties for noncompliance;
    - User security awareness program; and
    - User statement of responsibility.
- An appropriately placed, and adequately staffed centralized data security function, headed by an experienced data security officer, to assist in formulating, coordinating, and administering data security standards, policies, and procedures across the House. The security officer function should:
    - Be placed at an appropriate level within the House organizational structure to ensure that the position has the authority to enforce all applicable standards, policies, and procedures for both mainframe operations and office-level systems including LANs, personal computer systems, and other TCP/IP[8] based systems connected to the House network;

[8] TCP/IP (Transmission Control Protocol/Internet Protocol) is a communications protocol developed under contract from the U.S. Department of Defense to internetwork dissimilar systems. It is a de facto UNIX standard, but is supported on almost all systems. It is used by many corporations and most universities and federal agencies.

  - Establish and maintain standards, policies, and procedures (including applicable Federal government standards) for security over HIS operations and office-level systems environments and personnel;

  - Develop and maintain a risk assessment strategy for systems and telecommunications;

  - Participate in House information technology strategic planning efforts, feasibility studies for hardware and software acquisition and upgrades, systems development initiatives, and make recommendations in areas where risks have been identified as significant;

  - Monitor industry developments in data security practices and apply those that meet the needs of the House or are deemed appropriate;

  - Perform centralized maintenance of critical validation tables, such as those used by the User Billing and Chargeback System to reduce the risk of duplication, human error, and unauthorized access to the tables;

  - Regularly review system generated logs and activity reports, including unauthorized access attempts and other violations;

  - Create and maintain access rights including the distribution, update, review, and removal of user identification codes and passwords for users upon hire, transfer or termination; and

  - Act as liaison to other HIS components whose activities have data security implications (e.g., systems development, customer support, technical support, etc.);

- A formal data security compliance structure and enforcement mechanism. This compliance structure should include evaluation of the effectiveness of data security practices, assessment of the continued relevancy of these practices, and maintenance of ongoing user awareness of HIS security standards, policies, and procedures.

- A formal risk assessment model and data classification scheme. The risk assessment model should include an evaluation and assessment of the various risk factors affecting information processing resources, in addition to a data classification scheme that will assist in defining the detective and protective controls required for system resource. A formal, documented data classification system will help ensure that information resources are adequately and efficiently controlled.

The weaknesses described above exist despite the fact that the majority of these issues were previously reported in a March 1990 audit performed by Deloitte & Touche, and referenced in the "Prior Audit Coverage" section of this report (*Deloitte & Touche House Information Systems Information Security Plan Report)*.

Employee background checks were ineffective and expose the House to the risk of abuse and disclosure of sensitive information

Employee criminal background checks were performed in the past by the former HIS Security Officer, but were limited in scope and inconsistently applied. New HIS employees were subject to the background checks, however, the process was not formalized and supporting documentation was not maintained. Existing HIS employees are not subject to criminal background check. Furthermore, security clearances are not periodically updated, as required of Executive branch employees by the Federal Personnel Management Regulations (FPMR).

The impact of the lack of security clearances is evidenced by the example where, in 1988, the House hired an individual who was not a U.S. citizen and had falsified his/her social security card and state driver's license. The individual was employed as a computer operator and had access to payroll checks and other sensitive data for five years, until detected by a Department of State investigation. As a result of this investigation, the individual was immediately terminated without incident.

HIS personnel security standards, policies, and procedures are limited in scope, undocumented, and inconsistently applied with respect to personnel security. Although HIS maintains both security office directives and security policies and procedures documents, these documents focus on physical and data security rather than personnel security. A comprehensive Information Security Plan for HIS was developed in 1990 which addressed personnel security issues but this plan was never implemented (see "Prior Audit Coverage" section, *Deloitte & Touche House Information Systems Information Security Plan Report*, *March 1990*).

Failure to institute requirements for employee background checks could result in the continued hiring of unscrupulous employees and have devastating implications on House resources. Without applying prudent management practices, the House cannot minimize its risk of disclosure, modification, and destruction of sensitive information and resources.

Lack of vendor security requirements exposed the House to unnecessary security risks of disclosure, modification, and destruction of sensitive information

The House did not maintain security requirements for adherence by non-HIS employees (e.g., vendors). Vendors were not required to complete non-disclosure forms and criminal background checks were not required. These deficiencies were found even in the most sensitive environments, such as committees or Members dealing with foreign relations or national security.

HIS' relationships with vendors were based on purchase orders that did not include security provisions. The use of contracts that specify security provisions was not established as a requirement for formalizing relationships with vendors. As a result, no formal standards, policies, or procedures were in place to ensure that security precautions were addressed by vendors.

Failure to develop, implement, and maintain formal standards, policies, and procedures over vendor access to House information systems resources increases the risk that sensitive resources could be read, modified, or deleted.

Recommendations

We recommend that the Chief Administrative Officer immediately prepare proposals, for approval by the Committee on House Oversight, to:

1. Implement a formal, comprehensive data security program.

2. Establish a plan for adequately staffing a formal data security officer function, including a job vacancy announcement for an experienced data security officer, reporting to the Associate Administrator of House Information Resources.

3. Establish a plan for expanding the data security function to include broader authority to address security on all office-level systems including, LANs, personal computer systems, and other TCP/IP based systems connected to the House network. (The data security function should be granted the authority to set minimum data security requirements and to monitor and enforce adherence to such requirements on a regular basis.)

4. Implement an information security awareness program to communicate employee and vendor security responsibilities.

5. Implement a data security compliance structure and enforcement mechanism.

6. Implement a formal risk assessment model and data classification scheme.

7. Review staff positions to determine the associated level of risk and need for employee security clearances; incorporate security clearance requirements into each staff position description; and implement security clearances as required for Executive Branch employees under FPMR.

8. Establish vendor contracts that include provisions to support House security standards, policies, and procedures.

Management Response

On July 11, 1995, the Office of the Chief Administrative Officer (CAO) fully concurred with this finding and all eight recommendations (see Appendix). According to the response, several initiatives are either underway or planned to significantly improve security and integrity issues throughout the House information systems environment. Examples of key actions planned include: (1) developing and implementing a formal, comprehensive data security program; (2) restaffing of the data security function, including hiring a Security Administrator; (3) instituting an internal data security compliance structure and enforcement program; and (4) conducting a risk analysis of House systems and databases. In addition, the CAO intends to establish employee security clearance requirements, and incorporate appropriate security provisions into vendor contracts.

In furtherance of these data security goals, the CAO plans to develop a proposal, for approval by the Committee on House Oversight, to provide HIR's security function broader authority for implementing stronger security controls over House information systems, office-level systems, network facilities, and mainframes.

Completion of a risk analysis is expected by February 1996 and contract award for assistance in preparing a data security compliance structure and enforcement program is expected by December 31, 1996. Milestone dates for completing the remaining tasks are dependent upon the approval of the above proposal and selection of a Security Administrator.

Office of Inspector General Comments

The 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 for selected actions appear reasonable. However, we would appreciate you providing us milestone dates for the remaining actions once a decision has been made on the CAO's data security proposal and the Security Administrator position is filled.

Finding B: Improvements Needed In Disaster Recovery Planning And Testing For HIS Operations And Office-Level Systems

Disaster recovery planning and testing for the IBM mainframe processing environment supported by HIS were inadequate. In addition, no formal disaster recovery planning and testing existed for the telecommunications infrastructure. Furthermore, no formal disaster recovery planning and testing existed for the office-level computer processing environment, supported by both HIS and external vendors. As a result, the House could not be sufficiently prepared to handle potential business interruptions resulting from prolonged computer outages, emergencies, or disasters. The primary factor contributing to these problems was the lack of standards, policies, and procedures for establishing and implementing effective backup and recovery systems for House operations. Further, the deficiency associated with the mainframe processing environment was attributed to HIS' failure to update the disaster recovery plan and schedule periodic testing. In contrast, neither HIS nor any other responsible party within the House addressed disaster recovery planning and testing for the office-level computer processing environment.

Federal government and private industry disaster recovery standards and practices are well-established

Federal government and private industry standards and practices call for the establishment of standards, policies, and procedures for backup and recovery, including periodic testing of plans, of essential data processing operations and other information resources. Disaster recovery plans should anticipate potential business interruptions and disaster or emergency scenarios and cover all significant processes, including cold starts and restart and recovery routines, to limit any adverse impact to House operations. Periodic testing of such plans minimizes the adverse impact to House computing facilities and operations.

HIS Operations

We found that the HIS operations disaster recovery planning and testing for the mainframe data center processing environment was inadequate. In addition, we noted no formal disaster recovery planning and testing existed for the telecommunications infrastructure. Our finding is based on several factors, including the following:

- Business recovery plans addressing "user" requirements in the event of a disaster do not exist (e.g., there was no consideration of user requirements for the Financial Management System (FMS), backup office space, telephone routing, etc.);

- The Integrated Systems and Information Services (ISIS[9]) application and the various electronic mail (e-mail) systems are not included within the plan;

- The business impact analysis has not been updated in order to reevaluate the criticality of certain processes. The initial business impact analysis was developed by HIS and no House offices that would be impacted by a disaster scenario were involved with assessing the criticality of departmental functions (i.e., Member, Leadership, committee, and other House offices);

- The next test of the disaster recovery plan has not been scheduled. The last test was performed on August 1, 1994. Tests should be performed, at a minimum, on an annual basis;

- There has never been a full data center "power-down" test performed;

- No formal business recovery plan exists for the telecommunications infrastructure;

- Redundant network telecommunication links are not in place for the House wide area network;

- There is no physical off-site backup for the Network Control Center[10] (NCC). (In the event of a disaster or sustained outage at the Ford building, no backup site exists for the NCC); and

- There is no backup connection for the existing T1[11] lines for the House connection to the Internet.

Office-Level Systems

For the office-level computer processing environment, both supported by HIS and external vendors, we found that no formal or informal disaster or business recovery planning or testing exists for Member, Leadership, committee, or other House office-level systems. No responsible party within the House or HIS has been given the responsibility, or has assumed the

[9] ISIS is the newer version of the Member Information Network which provides Member, committee, and other House offices with a full range of resources, including news and periodicals, legislative information, Federal funding and statistical data, and administrative services.

[10] The NCC manages the telecommunications network within the House.

[11] T1 lines are communication facilities that handle large volumes of information at high speeds. These lines can carry millions of characters of information, both voice and data, that can be divided into many separate channels on the line.

responsibility for, developing, implementing, testing, and maintaining office-level disaster or business recovery planning.

These office-level systems provide critical support to House offices, such as correspondence management, budgeting, scheduling, etc. The disaster recovery plan for HIS operations does not include any office-level systems and thus would not extend to assist in recovering these systems in the event of a disaster or business interruption that impacted Member, Leadership, committee, and other House offices.

Recommendations

We recommend that the CAO immediately prepare a proposal, for approval by the Committee on House Oversight, to:

1. Implement a comprehensive disaster recovery plan that outlines specific disaster recovery procedures and responsibilities for both HIS operations (including the identification and coordination of a backup arrangement for the NCC), and office-level systems.

2. Implement and update the business impact analysis identifying those business processes and systems that are critical to the business continuity of the organizations supported by HIS, as well as office-level systems and telecommunications links supporting Member, committee, and other House operations currently not addressed by the existing mainframe data center disaster recovery plan. (Member, committee, and other House office representatives should be included in this re-evaluation.)

We also recommend that the Chief Administrative Officer:

3. Evaluate backup and business recovery alternatives that would facilitate recovery of those critical business processes and systems identified by the business impact analysis and select the most appropriate alternative.

4. Implement procedures for the ongoing maintenance of the business impact analysis and business recovery plan as well as comprehensive, routine (e.g., minimum once a year) testing of the plan. Additionally, a full data center "power-down" test should be included in the business recovery plan.

Management Response

On July 11, 1995, the Office of the CAO fully concurred with this finding and all four recommendations (see Appendix). As part of the CAO's overall security program, the CAO intends to conduct a business impact analysis that consider various levels of disaster recovery, including alternatives and associated costs. The results of this effort is expected by March 31, 1996 and will be included in the CAO's data security proposal for approval by the Committee on House Oversight. Furthermore, the CAO promised to implement a "power-down" test to evaluate battery backup and diesel generators capabilities.

Office of Inspector General Comments

The CAO's actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations. Further, the milestone date provided appear reasonable. However, we would appreciate you providing us milestone dates for the remaining actions once a decision has been made on the CAO's data security proposal and the Security Administrator position is filled.

Finding C: Security Controls Over User Access To System Resources Should Be Restricted To Job Responsibilities

The House did not have adequate or appropriate security software controls in place over House information resources. Serious security control deficiencies were identified involving House electronic mail (e-mail) systems, Customer Information Control System (CICS[12]), administration and implementation of ACF2 security software controls, access to sensitive production resources, and the use of a production scheduler. In addition, controls were inadequate over UNIX systems, LANs, standalone microcomputers, fileservers, and correspondence management system (CMS) operating systems and databases. Without effective security controls over information resources and user access to such resources, the House substantially increased the risk of unauthorized access and modifications to, and disclosure of, sensitive House data. Consequently, the House was not assured that information resources were sufficiently protected from fraud, waste, unauthorized use, and mismanagement.

Four factors contributing to these security deficiencies included: (1) inadequate data security strategy and planning processes; (2) a lack of formal standards, policies, and procedures for implementing and administering security software controls that could safeguard access to information resources and enforce segregation of duties; (3) a lack of requirements for conducting periodic, comprehensive security reviews to ensure that systems were properly protected; and (4) insufficient management attention to security issues.

As the House moves to a decentralized computer processing environment, consistent technologies, more efficient technical and maintenance support, and formal procedures are necessary to appropriately secure information resources and improve operations. Reducing the number of different systems, such as correspondence management and e-mail, would greatly enhance the House's ability to safeguard assets and improve electronic communications among Members.

Federal government and private industry security access standards and practices are well-established

Federal government and private industry generally accepted standards and best practices recommend the development and implementation of effective security controls in information processing facilities to ensure integrity, confidentiality, and availability objectives for systems that process, store, or transmit sensitive information. Examples of commonly accepted data security practices include the use of encryption strategies, password authentication procedures,

[12] CICS is a teleprocessing monitor from IBM that provides transaction processing for IBM mainframes. It controls the interaction between applications and users and lets programmers develop screen displays without detailed knowledge of the terminals used. It provides terminal routing, password security, transaction logging for error recovery, and activity journals for performance analysis.

specific security software parameters and settings to enforce segregation of duties and limit access to production and other sensitive system resources, and periodic security reviews to ensure system integrity and control.

Access security software products, such as ACF2, can provide significant enhancements to automated data and information systems security, and reduce unauthorized accesses, if properly implemented. ACF2 can support a number of other management controls through the use of identification codes, such as separation of functions, individual responsibility and accountability, limiting access to data on a need-to-know basis, and recording and reporting of system resource usage.

Improved security over e-mail messages should be developed and implemented

Any privileged user on the House network, including HIS operations personnel and office-level system administrators, could have intercepted e-mail messages by using available mainframe and network analysis tools to: 1) read messages, 2) prevent transmission of the messages, 3) alter messages, recompute the checksum[13] and then send it to the intended recipient, and 4) alter the identity of the message sender. As a result, messages were potentially vulnerable to being read, altered, or destroyed by unauthorized users on the House network. Interception of e-mail messages could have occurred anywhere along the path between the sending and receiving locations when e-mail messages were sent between the various House e-mail systems because no encryption or authentication techniques were available.

Encryption techniques, such as the Data Encryption Standard (DES), are used by protocols[14] as a tool to achieve authenticity, secrecy, or integrity during interaction between two users. DES uses cryptography to encode data for security purposes for transmission over a public network using an algorithm to convert cleartext into a coded equivalent called ciphertext. The ciphertext is decoded (decrypted) at the receiving end with the use of a decryption key. DES encryption ensures the integrity and confidentiality of the message portion of the e-mail, while public authentication key ensure the identity of the message sender.

Within the House information systems environment, eleven different vendor e-mail systems were supported. E-mail messages communicated between offices generally passed through

[13] A checksum is a value used to ensure data is transmitted without error. It is created by adding the binary value of each alphanumeric character in a block of data and sending it with the data. At the receiving end, a new checksum is computed and matched against the transmitted checksum. A non-match indicates an error.

[14] Protocols are the rules governing transmitting and receiving of data.

various communications facilities, including routers[15] and the HIS mainframe. The mainframe translated and directed all messages between the different e-mail systems using an installed software product called Softswitch marketed by the Lotus Development Corporation. Softswitch translated the different protocols used by the individual e-mail systems. Therefore, the potential existed for e-mail messages to be intercepted either at the router level or within the HIS mainframe because DES and authentication techniques were not available to the House. Consequently, opportunities for unauthorized disclosure and modification of confidential e-mail messages existed .

ACF2 security was not in place for all online regions

All HIS production online regions, except for the General Accounting Office region, utilized native internal CICS security instead of ACF2. CICS security had numerous inherent weaknesses such as:

- no automatic mechanism to force regular password changes;
- no online reporting of access violations or attempted access violations;
- no enforceable password standards (e.g., one digit passwords can be used); and
- no limited number of invalid sign-on attempts.

Additionally, new users requiring access to CICS applications were assigned profiles which were copied from a similar existing profile. Furthermore, the CICS security keys assigned were not forwarded to the respective division's security administrator for review. This increased the likelihood that users received greater access than was required to perform their job duties. Also, a cleartext password file containing all user's passwords was maintained.

In addition, FMS was not under the control of ACF2 and relied on a combination of CICS and physical security. CICS security capabilities were used to physically limit access to FMS to only certain terminals located in the offices of the assigned FMS users. While this control feature provided a level of security over FMS, implementation of ACF2 protection over FMS would increase the security and controls surrounding the application. Furthermore, ACF2 protection would then be consistent across the entire mainframe processing environment, as well as consistent with generally accepted government and private sector best practices.

[15] A router is an intelligent hardware device in a network that routes messages between LANs and WANs. Routers see the network as network addresses and all the possible paths between them. They read the network address in a transmitted message and can make decisions on how to send it based on the most expedient route (traffic load, line costs, speed, etc.).

The number of users having powerful ACF2 access privileges was excessive

HIS did not take advantage of ACF2 capabilities and features to restrict the access privileges of, and enforce segregation of duties among, its employees in accordance with job responsibilities. We noted that all individuals within the Operating Systems, Performance and Capacity Planning, Online Systems Support, and Technical Support as well as the Operations Supervisor and the Security Administrator for the Director of HIS Offices, had a powerful ACF2 access privilege (i.e., Non-Cncl privilege). The number of users with this privileged access was excessive. Moreover, this privilege enabled these users to access all IBM mainframe data and went beyond the level of access they needed to perform their job responsibilities and duties effectively. Although access attempts were logged and a report was generated daily for review by the computer center security administrator, specific unauthorized activities could not be prevented or immediately detected. Therefore, all sensitive privileges should be removed from individuals not requiring the capability for routine job functions.

Our review also noted that neither an emergency logon identification (ID) nor corresponding emergency procedure existed in the event of a processing emergency. The purpose of an emergency logon ID is to provide controlled access to system data and files; it is not intended for routine use. An emergency logon ID should be confidential, until used, and then immediately changed by HIS security personnel. The emergency logon ID should have all of the access necessary to perform sensitive system functions. An emergency logon ID should be maintained by the Computer Center shift supervisors. The use of this ID should be documented, reported, and reviewed. Accordingly, ACF2's detailed recording and reporting features (e.g., Trace and Monitor) should be invoked during the use of emergency IDs. This would provide management and the security officer with sufficient information to monitor ID use. The establishment and implementation of such an approach would eliminate the need for granting powerful access privileges.

Failure to limit this access to only those individuals requiring such capability increased the risk that the privilege could be used in non-emergency situations to gain unauthorized access to sensitive data. Such access, in turn, could lead to unauthorized modification and destruction of data.

ACF2 access privileges for divisional security administrators were excessive

Our review identified that divisional ACF2 security administrators were granted excessive authorities by having both security and account privileges. The Security privilege enables a user to perform security officer functions such as insert, list, change, or delete data set and resource access. The Account privilege allows a user to insert, delete, or change logon records. Divisional ACF2 administrators were responsible for writing rules for data sets owned by the division, which required only the Security privilege. Providing divisional ACF2 administrators with the Account privilege allowed them to add unauthorized or fictitious users to the system without properly approved request forms and violated the basic segregation of duties internal control concept.

We noted that no standards, policies, and procedures existed to address this segregation of duties weakness. Removing the Account privilege from the divisional security administrator would ensure centralized control over logon records and provide appropriate segregation of duties.

Failure to remove the Account privilege from the divisional ACF2 security administrators posed a segregation of duties problem and increased the risk of an unauthorized or fictitious user being added to the system without management's timely detection.

Access to sensitive production resources (i.e., application source code, load module, Job Control Language (JCL), and Authorized Program Facility (APF) libraries) by unauthorized individuals existed

The application of system security software features over IBM mainframe systems was not applied uniformly for all data residing on the mainframe. Our review of the ACF2 rules surrounding selected application source, load, JCL, and APF data sets identified application and system programmers with inappropriate access to these sensitive system libraries. In addition, we noted that the HIS programmers, responsible for the FMS, had access to voucher payment and payroll data and were able to change them without leaving an audit trail.

An inappropriate segregation of duties existed within the HIS organization, resulting in individuals having excessive access to House information systems resources that may not be required in order to perform their job functions.

Allowing extensive access to these resources increased the risk of unauthorized access to, and modification of, sensitive data. In addition, unauthorized or inappropriate modifications could have been introduced into production programs which in turn could have adversely impacted processing on House systems. In particular, APF data set access could have allowed an unauthorized person to develop and introduce powerful programs which could then be used to disrupt operations or gain additional unauthorized access.

Production Jobs Were Not Always Run Through the Control/M Production Scheduler

Although all regularly scheduled production jobs executed under the control of the scheduler (i.e., Control/M), we noted that execution of ad hoc jobs was not scheduled. The Control/M batch job scheduling product is used to schedule production jobs. Scheduling all production jobs through Control/M would ensure that only authorized users can initiate job execution and an audit trail of changes is maintained.

Executing jobs that update production data outside of the control of the scheduler increased the risk of inappropriate or unauthorized modification of production data and limits the ability to maintain an audit trail of changes for production job execution.

HIS data security procedures for UNIX needed to be expanded and improved

Although HIS performs a manual security audit on UNIX systems in offices within the House requesting access to the Internet, we noted several deficiencies in the approach used in their review as follows:

- The review was performed only at one time, prior to granting Member, committee, or other House offices access to the Internet. No reviews to verify ongoing security of the system were performed subsequent to this initial review;

- The review was limited in scope and did not include evaluations of several high-risk aspects of UNIX security. This included scanning file systems for vulnerabilities in various sensitive facilities (e.g., world-writable and trusted host files) that would allow unauthenticated access of House systems by other House or remote UNIX systems; and

- The review did not use automated tools to perform more comprehensive evaluations.

The need for expanded data security procedures at HIS was evidenced by our technical review of a sample of HIS operations and office-level systems environments. The security weaknesses noted included the following:

- Several instances where critical files were available to be read, modified, or deleted by any user with access to the system;

- Trusted relationships existed between the systems we reviewed and other systems throughout the House, allowing unauthenticated access to these systems;

- System executable files were not adequately controlled;

- Use of the superuser/root ID was not adequately controlled;

- Password cracking programs used in our testing were able to guess many passwords, indicating that user password control procedures are weak;

- Shared user ID are permitted, indicating weak user account administration policies;

- Access controls to the systems via modems were weak;

- Available system logging mechanisms were not used; and

- Office-level physical security of computers, disk storage, and backup media was inadequate.

These factors combine to create an insecure environment for the information stored on many HIS and office-level UNIX systems. Failure to adequately secure these systems increases the risk of unauthorized access and the potential for disclosure, modification and destruction of sensitive system resources.

Office-level systems security over LANs and standalone microcomputers needed to be improved

During our review of office-level systems security, we examined a number of LAN and standalone computer systems in Member, committee, and other House offices and found repeated instances of inadequate and inappropriate security implementation of access control settings. These security weaknesses were noted throughout the House office-level systems environment and included Novell Netware, Windows NT, DOS, and Windows operating environments. Weaknesses included:

- Inadequate and inappropriate user ID and password controls;

- Excessive system and file access;

- Unsecured remote dial-in (modem) access;

- Limited intruder detection lockout;

- Inadequate and inappropriate system configurations and documentation; and

- Limited system documentation (e.g., security procedures, disaster recovery plans, etc.).

In addition, we noted that the use of the "SUPERVISOR" and "ADMINISTRATOR" user IDs was not adequately and effectively controlled. The weaknesses we noted included:

- Inadequate password length and change interval over these sensitive IDs;

- Sharing of passwords;

- Continuous vendor access to systems with these privileges; and

- Excessive number of users with these privileges.

No standards, policies, and procedures existed to address these access weaknesses. These factors combine to create an insecure environment for the information stored on many Member, committee, and other House office-level LAN and standalone microcomputer systems.

Failure to adequately secure these systems increased the risk of unauthorized access and the potential for disclosure, modification, and destruction of sensitive system resources.

No physical or environmental controls exist for file servers

During our review, we observed at various House offices that adequate and appropriate physical and environmental controls were not in place. Instances of physical control weaknesses included failure to secure access to microcomputers, servers, printers, communications equipment, and other computing facilities. Environmental control weaknesses included limited consideration of the effects of temperature, humidity, heat, and smoke on computing facilities.

The House did not establish formal standards, policies, and procedures for physical and environmental controls for the office-level systems environment. Physical controls include ensuring that computer resources (i.e., hardware, software, and documentation) are adequately protected from physical access. Use of locked doors, closets, and storage cabinets are examples of ways to physically secure resources. Environmental controls include facilities to ensure that system resources are protected from such elements as heat, humidity, smoke, water, and fire. Use of temperature control and sensory devices are examples of ways to environmentally protect system resources.

Failure to implement physical and environmental controls increased the risk of unauthorized access to system resources and disruptions of operations.

Operating system and database level controls of a Correspondence Management System were inadequate

Our technical review of a CMS operating environment revealed that much of the correspondence data stored on the system was accessible by any user from outside the application (e.g., using operating system commands) and that application controls meant to prohibit this type of access were not effective. In addition, the vendor was allowed to have privileged access to the Member systems in an uncontrolled manner on a routine basis.

The House and HIS have not developed standards, policies, and procedures to (1) reduce the permissions granted to users to access this CMS' data files at the UNIX operating system level, (2) eliminate all user access to the operating system, and (3) utilize other access controls that prohibit ad hoc user access to data.

Failure to effectively control access to CMS systems increases the risk that system data could be read, modified, or destroyed by unauthorized users, including House users and individuals gaining access externally.

Recommendations

We recommend that the Chief Administrative Officer immediately prepare proposals, for approval by the Committee on House Oversight, to:

1. Implement an e-mail system that supports DES encryption.

2. Establish data security procedures for LANs, standalone computers, and other distributed computing systems, including UNIX, Novell Netware, Windows NT, DOS, Windows, fileservers, and any other operating environments supporting House systems to improve office-level security.

3. Implement appropriate physical and environmental controls surrounding microcomputers, servers, printers, communications equipment, and other computing facilities for Member, committee, and other House offices.

In addition, we recommend that the Chief Administrative Officer:

4. Establish the following controls to improve House Information Resources' management and implementation of ACF2 security:

   - Implement ACF2 over all online mainframe applications, including FMS;

   - Remove the online access to the CICS password file;

   - Administer all passwords through ACF2;

   - Justify the need for all special ACF2 access privileges;

   - Limit the "Non-Cncl" privilege to only those users who require access;

   - Create an ACF2 emergency logon ID for occasions that require sensitive access;

   - Record and review detail activities during use of emergency logon IDs;

   - Remove the Account privilege for divisional security administrators; and

   - Review and restrict, where appropriate, ACF2 access privileges to production libraries.

5. Schedule all production jobs, including ad hoc jobs, through the Control/M scheduling software package.

6. Enhance controls surrounding CMS systems to ensure that users can only access data through the designed application features and not by other means that circumvent the application system.

7. Develop a plan for approval by the Committee on House Oversight to perform periodic security reviews to ensure that adequate controls are in place to protect House data and other sensitive system files.

Management Response

On July 11, 1995, the Office of the CAO fully concurred with this finding and all seven recommendations, including individual subparts (see Appendix). As indicated in the response, the CAO intends to implement corrective actions to address our recommenations. Examples of major initiatives planned include: (1) exploring the feasibility of implementing DES encryption for House e-mail systems; (2) revising security guidelines, including appropriate physical and environmental controls over desktop and in-office systems; (3) establishing an audit service for providing periodic security reviews, and security consultation to offices; (4) reviewing and implementing more stringent ACF2 controls over House information resources; (5) utilizing Control/M for scheduling all production and ad hoc jobs; and (6) requiring vendors to ensure that system access controls cannot be circumvented. In addition, the CAO indicated that, as a part of the overall security program, periodic progress reports will be submitted to the Committee on House Oversight.

Completion of the first three actions described above are expected by December 31, 1995. Milestone dates for completing the remaining tasks are dependent upon the approval of the CAO's proposal for improving data security (discussed in the Management Response section of Finding A) and selection of a Security Administrator.

Office of Inspector General Comments

The 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 for selected actions appear reasonable. However, we would appreciate you providing us milestone dates for the remaining actions once a decision has been made on the CAO's data security proposal and the Security Administrator position is filled.

Scot M. Faulkner
Chief Administrative Officer

APPENDIX

Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515–6860

MEMORANDUM

TO: Robert B. Frey III
Deputy Inspector General

FROM: Thomas J. Simon
Director of Internal Controls and Continuous Improvement

DATE: July 11, 1995

SUBJECT: Draft Audit Report - Computer Security

We appreciate the opportunity to comment on your draft report. We deeply appreciate your efforts and are in general agreement with the findings and recommendations. Specific comments on each recommendation follow. If there are any questions or additional information required regarding this reply, please contact me at (202) 226-1854.

Finding A

Recommendation 1: HIR is actively recruiting a Security Administrator to develop a formal comprehensive security program. The office will have four positions. In the meantime, several security-related initiatives have been launched.

Recommendation 2: A Security Administrator position reporting to the Director has been established in the new HIR structure and active recruitment is in process to fill that position.

Recommendation 3: An early task of the Security Administrator will be to prepare proposals for the Committee on House Oversight to strengthen the security safeguards for office systems and shared network facilities and to provide for the appropriate monitoring and enforcement activities. Completion of this work is dependent on the hiring date of the Security Administrator.

Recommendation 4: A security awareness program will be developed and implemented under the guidance of the Security Administrator. Vendor briefings on security issues have recently been completed as a first step in a new on-going dialog on security issues.

Recommendation 5: HIR intends to institute an internal data security compliance structure and enforcement program. Use of qualified contractor support both in preparation of the program and in evaluation of its effectiveness is anticipated. Contract award is scheduled prior to December 31, 1996.

Recommendation 6: A risk analysis of existing and proposed systems and databases will be conducted and completed no later than February 1996. As appropriate, detection and protection mechanisms will be incorporated.

Recommendation 7: An on-going review of the security implications of all position descriptions and specific staff assignments will be conducted as part of the overall security program. As needed, security clearances will be obtained through the Sergeant at Arms.

Recommendation 8: Appropriate security provisions will be incorporated into all contracts into which HIR enters.

Finding B

Recommendations 1, 2, 3 & 4: Business impact and cost analyses for various levels of disaster recovery protection will be prepared as part of the overall security program and result in a proposal to the Committee on House Oversight as to alternatives and associated costs. Policies regarding HIR access to Member and Committee office systems will be addressed. (It should be noted that the need and urgency for comprehensive disaster recovery plans and programs, though fully appreciated and well understood, were not attainable in the past due to budgetary and staffing limitations.) This issue will be addressed anew and recommendations could be expected by March 31, 1996.

The recommendation for a "power-down" test to evaluate the battery backup and diesel generator capabilities will be implemented .

Finding C

Recommendation 1: HIR will conduct an analysis of the need and potentially substantial cost of implementing DES encryption capable e-mail systems within the House and provide a report to the Committee on House Oversight by December 31, 1995.

Recommendation 2: HIR will review existing security guidelines and provide an audit service for in-office systems, as part of the overall security program, and issue revised guidelines with renewed emphasis on providing guidance to offices on measures that can be taken within the office to reduce risks and improve security by December 31, 1995.