John W. Lainhart IV
Inspector General

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

**MEMORANDUM**

TO: Jeff Trandahl
Acting Chief Administrative Officer

FROM: John W. Lainhart IV
Inspector General

DATE: March 24, 1997

SUBJECT: Audit Report - Weak Telecommunications And Information Systems Security Controls Compromise House Information Resources (Report No. 97-CAO-04)

This is our final report on the audit of telecommunications security at the U.S. House of Representatives (House). This audit is the first of five audits performed on the House telecommunications environment. The objective of this audit was to assess the effectiveness of data, voice, video, and wireless communications (i.e., telecommunications) security at the House. In this report, we identify numerous security-related problems and issues, and make 33 recommendations for corrective actions.

In response to our September 30, 1996 draft report, your office concurred with the findings and all 33 recommendations. Your office's formal written response is incorporated in this 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 completed planned actions appear reasonable. However, we would also appreciate you providing us milestone dates for Recommendations F.3, H.1, H.5, H.6 and J. We request that this information be provided by April 25, 1997.

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

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

**WEAK TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY CONTROLS COMPROMISE HOUSE INFORMATION RESOURCES**

***Report No. 97-CAO-04***
***March 24, 1997***

## RESULTS IN BRIEF

## CONCLUSIONS

Since the comprehensive House audit in July 1995, the U.S. House of Representative (House) has made progress toward improving controls over the integrity, confidentiality, and availability of information and systems. The House re-established its information systems security function under the House Information Resources (HIR) organization during the first half of Calendar Year 1996. The new security staff led by an experienced security manager has developed and is continuing to develop a number of initiatives designed to improve security controls over House information technology and information resources. Examples of these initiatives include: (1) preparing an information security policy for the House; (2) developing requirements for personnel security background checks and clearances; (3) developing security policies over voice and data systems; (4) establishing a secure dial-in modem bank; (5) assessing physical security control requirements over equipment and facilities; (6) performing security reviews; and (7) instituting penetration testing procedures.

The Communications Group has security responsibilities with respect to the House Campus Network, Internet[1] "firewall[2]," and telephone system. This Group has also implemented corrective actions to improve security resulting in better physical controls over the Network Control Center (NCC[3]) and access controls over the House's connection to CapNet[4].

Notwithstanding the progress made thus far, significant efforts are needed to improve security controls over the integrity, confidentiality, and availability of information and systems at the

[1]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.

[2]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.

[3]The Network Control Center manages the telecommunications network within the House.

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

House. Security weaknesses were noted in certain areas of the House telecommunications environments, posing risk of unauthorized access, modification, and destruction of telecommunications and information resources at the House. Several of the security weaknesses identified can greatly impact the effectiveness of HIR Security staff's and the Communications Group's abilities to carry out security responsibilities and activities as intended by the House. Without effective security controls, the House cannot be assured that information resources are protected from fraud, waste, abuse, and unauthorized use.

Since the House's telecommunications system is an integral component of Member, Committee, and other House office information and computer operations, this report not only addresses telecommunications security issues but also focuses on information systems-related security weaknesses that affect telecommunications security. The security weaknesses identified encompassed the areas of information systems security architecture; security staffing, tools, and training requirements; security administration; computer and telecommunications security training and awareness; dial-in security; logical security access; Private Branch Exchange (PBX[5]) security; telecommunications physical security; Committee and Subcommittee room wiring infrastructures; and Internet-related procedures. The following is a high level synopsis of security weaknesses included in this report:

- The House lacks a well defined information systems security architecture, including policies and procedures, that outlines a minimum baseline to operate from. Part of this missing baseline includes security plans, a data classification/ownership policy, and risk assessments to identify sensitive or critical data for protection.

- Although the House re-established its information systems security function within HIR in January 1996, security reviews have not been performed in sufficient quantity and on a frequent enough basis to adequately cover the most vulnerable areas and prevent or detect unauthorized access or intrusions. HIR Security does not have security analysis software to perform detailed testing of office systems for compliance with House security standards. Further, the day-to-day operational security responsibilities and duties are diverse, leaving little time for proactive security activities.

- HIR Security functions involving mainframe access security software is inappropriate for controlling information resources. Non-security personnel, such as systems administrators within the Enterprise Computing Group, are allowed to perform critical access security functions, such as writing rules and reviewing audit trails. These capabilities provide non-security personnel the ability to access, view, or modify House data on the mainframe without leaving an audit trail.

[5]PBX is an automatic or manual private telephone exchange for transmission of calls to and from the public telephone network.

- Computer security training available to House offices needs improvement. Computer security training is required for all offices when they are initially connected to the Internet. However, all employees in those offices are not required to attend the training. Therefore, according to the HIR Security Manager, at a minimum, only the office managers and systems administrators attend the training. In addition, computer security training is not mandatory for those offices not connected to the Internet. Furthermore, there are no requirements for employees to receive appropriate follow-up training in, and awareness of, accepted computer security practices. Similarly, House employees have not received sufficient training and awareness on the secure use of House telephone services in accordance with established policies and procedures.

- Remote access security is inconsistent within the House which creates a security exposure.

- Mainframe logical access controls are not sufficiently administered to restrict users from gaining access to House network resources (i.e., certain communications and teleprocessing monitors). For example, many HIR support staff have unnecessarily broad access privileges which provide them the ability to access these network resources beyond the scope of their authorized duties and responsibilities.

- PBX system security needs improvement to reduce the potential for toll abuse at the House. HIR relies heavily on telecommunications service providers to monitor toll fraud abuse. Allowing others to monitor for toll fraud at the House increases the risk of unauthorized toll use and abuse.

- Physical security controls are inadequate to properly safeguard various telecommunications facilities within the House. (These control deficiencies were also disclosed in HIR Security's September 1996 report entitled *A Report of the Communications Closets of the U.S. House of Representatives*.)

- The current wiring policy for voice, data, and video wiring in House Committee, subcommittee, and other event rooms is unmanageable and provides little assurance of security. Individual broadcasters have been allowed to unilaterally install and/or make arrangements with telecommunications service providers to install and provide cabling and specialized circuits for any given event without coordinating with HIR. This, in turn, has greatly impacted the House's ability to maintain control over its telecommunications wires and cables when a media event occurs in a Committee, Subcommittee, or any other room in the House complex.

  At the request of the Committee on House Oversight, audit work also included an assessment of the Communications Group's *Committee and Event Room Wiring Proposal.* Based on our review, we recommend its approval by the Committee.

- During the telecommunications audit, we performed limited penetration tests of the House firewall and were unable to penetrate it. From this perspective, the Communications Group should be commended on their efforts and commitment for ensuring that House information is properly protected. However, in reviewing the strength of the Internet security environment, we noted that HIR could strengthen its Internet administration functions by providing well-designed and tested procedures for ensuring that the Communications Group and Security staff quickly respond to penetration attempts or security violations.

## RECOMMENDATIONS

We made a total of 33 recommendations to the Chief Administrative Officer to strengthen security controls over the House's telecommunications and information resources.

## MANAGEMENT RESPONSE

On January 21, 1997, the Acting CAO fully concurred with the findings and all 33 recommendations in this report. According to the response, numerous actions were completed or are planned to significantly strengthen telecommunications and information systems security at the House.

## OFFICE OF INSPECTOR GENERAL COMMENTS

The Acting CAO's completed and planned 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 completing the planned actions appear reasonable. However, we are requesting that the Acting CAO provide us milestone dates for certain recommendations that did not contain milestone dates by April 25, 1997.