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

MEMORANDUM

TO: James M. Eagen III
Chief Administrative Officer

FROM: Robert B. Frey III
Deputy Inspector General

DATE: October 8, 1999

SUBJECT: Audit Report – Additional Security Controls Needed Over The House's High Speed Legislative Branch Network (CAPNet) Connection (Report No. 99-CAO-08)

This is our final report on the effectiveness of security controls over the House's CAPNet connection. The purpose of this review was to:

- Conduct a high-level risk assessment of the House CAPNet environment, installation, operation, and oversight to identify significant inherent vulnerabilities;

- Conduct a network security review of the physical and logical controls associated with the House CAPNet environment; and

- Review the House CAPNet administrative, operational and security policies, compare those policies against best practices, and develop recommendations for improvements based upon proactive management approaches.

During this audit, we found no serious breaches of security. However, HIR's management of CAPNet assets needs improvement. Until a technical risk assessment is completed for House CAPNet assets, an increased risk of unauthorized access, modification, and disclosure of House information exists. Although House CAPNet assets were included in a contract to perform an overall risk assessment, the technical risk assessment has not yet been completed.

In this report, we identified 10 weaknesses and made 16 recommended actions for corrective actions in two COBIT areas. These areas are: (1) planning and organization and (2) delivery and support. Planning and organization covers the strategy, tactics, and identification of the way IT can best contribute to the achievement of the business objectives. Delivery and support includes the delivery of required services that range from traditional operations over security and configuration aspects to training. The weaknesses identified in these areas are discussed in Exhibits 1 and 2 and are

"Confidential" in nature. Therefore, they may not be disclosed or released to anyone other than auditee management except by approval of the House Office of Inspector General. Collectively, deficiencies in these areas increase the risk of unauthorized access, modification to, and disclosure of House information.

In response to our June 1, 1999 draft report, your office concurred with the reported weaknesses and recommendations. The September 13, 1999 management response 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.

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 Christian Hendricks or me at (202) 226-1250.

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

I. INTRODUCTION

Background

Networks are a combination of hardware, software, and transmission media that comprise a system of interconnected computers and the communications used to link them. A network's backbone is the main transmission medium that provides network connections. The high speed Legislative Branch Campus Network (CAPNet) was created to electronically exchange unclassified information among Legislative branch members. CAPNet members include the U.S. House of Representatives (House), the U.S. Senate, the Architect of the Capitol (AOC), the Congressional Budget Office (CBO), the Library of Congress (LOC), the Government Printing Office (GPO), and the General Accounting Office (GAO). CAPNet members are individually responsible for purchasing and maintaining the hardware that is connected to the CAPNet backbone.

During the 1990s, CAPNet members facilitated the initial establishment of router connections to the network through technical working group meetings. Technical standards for interface card specifications, connectivity, router IP addresses, routing information and protocols were communicated through these meetings. Once network connections were in place, campus-wide participation at technical working group meetings occurred at the request of individual members. No documented specifications, agreements, or meeting minutes were available from this original working group. While there are some collective standards and practices to govern the continued use of CAPNet by its members, internal standards and practices of member organizations influence CAPNet operations. Currently, technical issues are addressed whenever coordination is required through the CAPNet Engineering Task Force (CETF), which last convened in January 1998 at the request of the then Committee on House Oversight[1]. This task force, comprised of technical telecommunication experts from each Legislative branch organization, does not have a current charter, nor are its proceedings available.

The House Information Resources (HIR) Communications group is responsible for the House's CAPNet connections. Within this group, the Network Control Center monitors the health of the network. Its staff assures timely access to House services and works closely with Network Installation and Maintenance (NIM), Network Configuration Management (NCM), and Network Systems Engineering (NSE) entities within the Communications group to analyze and resolve any network related problems. The NIM team is primarily responsible for installation, maintenance, and trouble-shooting. The NCM team is responsible for managing, controlling and trouble-shooting physical and logical configurations and works closely with NSE to define operational requirements of new services and equipment. The NSE team also provides in depth technical support for diagnosing problems.

[1] At the start of the 106th Congress the Committee on House Oversight was changed to the Committee on House Administration.

The House currently has two Cisco 7000 series routers on the CAPNet, which perform some network access control through packet[2] filtering services. A router filters packets as they pass between the router's interfaces, implementing rules based on firewall policy that relate to source and destination Internet Protocol (IP) addresses and ports. The House CAPNet employs Cisco software to manage its router configuration and is the only CAPNet member that maintains two router connections--significantly improving reliability with regard to House CAPNet resources. CAPNet transmission links use Fiber Distributed Data Interconnect (FDDI) technology.

Good management is essential for CAPNet's operational success and growth. However, this is difficult to achieve because all seven legislative entities support differing goals and objectives for CAPNet. Although this audit originally encompassed only House CAPNet assets, all other CAPNet members voluntarily participated. Their participation proved vital to the success of an overall CAPNet risk assessment and our ability to provide meaningful recommendations for the House.

Objective, Scope, And Methodology

The overall objective of this review was to evaluate the effectiveness of the general control environment of the House's CAPNet connection. The primary purpose of this review was to:

- Conduct a high-level risk assessment of the House CAPNet environment, installation, operation, and oversight to identify significant inherent vulnerabilities;

- Conduct a network security review of the physical and logical controls associated with the House CAPNet environment; and

- Review the House CAPNet administrative, operational and security policies, compare those policies against best practices, and develop recommendations for improvements based upon proactive management approaches.

As part of this review, we assessed House CAPNet assets that consisted of two Cisco 7000 series routers, a configuration server and a logging server. The review encompassed the period November 1998 through March 1999.

In conducting this audit, we performed the following specific tasks:

- Reviewed documentation relating to House CAPNet hardware and software acquisition, development, and implementation; network topology; location of House CAPNet resources and data paths; communications controls; CAPNet member relationships; server configuration; logical security; utilization, and activity reporting; router maintenance; and backup and recovery procedures.

[2] A packet is a block of data for data transmission that contains both routing information and data.

- Gathered documentation relating to House CAPNet administrative, operational and information security policies, standards, and procedures, including the House Information Security Policies (HISPOLs).

- Determined the extent of detailed analysis and testing required for evaluation.

- Used UNIX vulnerability scripts and third-party automated tool, *Internet Security Scanner (ISS)*, to gather configuration data and test known potential risks.

- Conducted a physical security review of the House CAPNet assets.

- Conducted detailed analyses of House CAPNet policies, procedures, and standards; and identified weaknesses.

- Compared current House CAPNet operations with best practices observed in industry and government, and Federal policies and standards.

The audit work was conducted in accordance with the *Government Auditing Standards* issued by the Comptroller General of the United States and included such tests as we considered necessary under the circumstances. In addition to the *Government Auditing Standards*, we applied other Federal and private industry criteria. Such criteria included the Information Technology Management and Reform Act of 1996, National Institute of Standards and Technology (NIST) Standards, the Information Systems Audit and Control Foundation's Computerized Information Systems (CIS) Audit Manual, and the Information Systems Audit and Control Foundation's Control Objectives for Information and Related Technology (COBIT).

The COBIT framework consists of four domains, each containing processes and control objectives. The four domains are Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. HIR evaluated and adopted applicable COBIT criteria and best commercial practices as part of its business process.

COBIT domains applicable to this audit are:

- **Planning and Organization.** This domain covers strategy and tactics, and concerns the identification of the way information technology (IT) can best contribute to the achievement of business objectives. The realization of the strategic vision needs to be planned, communicated and managed for different perspectives. Proper organization as well as technological infrastructure must be in place.

- **Delivery and Support.** This domain is concerned with the actual delivery of required services, which range from traditional operation over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up.

- **Monitoring.** All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses management's control process

and independent assurance provided by internal and external audit or obtained from alternative sources.

Internal Controls

We evaluated the general controls over the House CAPNet assets to assure the confidentiality, integrity, and availability of House information. No serious breaches of security were found. This audit disclosed certain weaknesses in the House CAPNet environment related to the need for a technical risk assessment and a security checklist to establish a uniform evaluation process. These weaknesses, if not corrected, could pose a threat to the House's information resources environment. The control weaknesses identified for HIR are arranged by COBIT domain and detailed in confidential Exhibits 1 and 2.

Prior Audit Coverage

The Office of Inspector General (OIG) first addressed computer security and control issues in a July 18, 1995 audit report entitled, *Internet Security Weaknesses*, (Report No. 95-CAO-03). This report concluded that Internet security weaknesses associated with House CAPNet could expose House computer systems, including Member, Committee, and House Officer systems, to unauthorized access, disclosure, modification, or destruction. The audit recommended that HIR install firewall systems between the House's internal network and all other agencies connected to CAPNet to protect House systems from unauthorized access attempts from computers in the other CAPNet agency networks. In response to these recommendations, management took action to install and configure a Cisco7000 series router to serve as a firewall between the House network and CAPNet. The router was configured to filter data packets on a "deny unless specifically granted" basis. Based upon a proactive and preventative approach, industry standards currently indicate that firewall design offers both packet filtering and proxy services. Therefore, firewall issues are reemphasized within this report. (See Exhibit 3 for the status of prior audit recommendations.)

II. RESULTS IN BRIEF

During this audit, we found no serious breaches of security. However, HIR's management of CAPNet assets need improvements in two COBIT areas (1) Planning and Organization, and (2) Delivery and Support. Until a technical risk assessment is completed for House CAPNet assets, an increased risk of unauthorized access, modification, and disclosure of House information exists. House CAPNet assets were included in a contract to perform an overall risk assessment. However, a technical risk assessment has not been performed. The COBIT domain, Monitoring, was deemed to be sufficient because HIR has processes in place that address logging, change management, monitoring, and backup.

Overall, we identified 10 weaknesses and provided 66 recommended actions to improve the general controls for House CAPNet assets that HIR manages. The prevailing reasons for the deficiencies identified in this report were specifically attributed to the fact that a technical risk assessment for the House's CAPNet connection was not yet completed at the time of our review and a security checklist was not yet established to maintain a uniform evaluation process. We

categorized the recommendations associated with identified weaknesses as high, medium, or low priorities. High represents significant security and general control weaknesses that could adversely impact aspects of House computer operations unless controls are immediately implemented. Medium represents security and general control weaknesses that could adversely impact aspects of House computer operations unless mitigating controls are employed. Low represents minor general control weaknesses that could be improved with additional controls. The table below illustrates the number of control weaknesses by COBIT domain, number of recommendations, and overall risk ranking. Details of the control weaknesses are described in Exhibits 1 and 2. In addition, management comments are included in their entirety as an Appendix to the report. The Exhibits and Appendix to this report are 'Confidential' and may not be disclosed or released to anyone other than the auditee without the approval of the House OIG.

COBIT DOMAIN	EXHIBIT	NUMBER OF CONTROL WEAKNESSES	NUMBER OF RECOMMENDED ACTIONS	OVERALL RISK RANKING ASSIGNED[3]
Planning and Organization	1	1	2	MEDIUM
Delivery and Support	2			
Routers		4	15	MEDIUM
Configuration Server		3	25	MEDIUM
Logging Server		2	24	MEDIUM
Total		10	66	

Summary of Domain Weaknesses

Based on our interviews, reviews of relevant documentation, and detail tests performed, the overall risk to the House was deemed to be medium. During our review we made 66 recommendations, 50 of which management took immediate, appropriate action to correct. As a result, this report contains 16 recommendations, two in the Planning and Organization domain and 14 in the Delivery and Support domain, to improve the general controls for HIR managed CAPNet assets.

Planning and Organization

Effective planning and organization is essential to achievement of the House's strategic objectives. The CAO's 1999-2003 Strategic Plan committed to use current network technology to meet its client/server information processing needs and communicated the House's vision for this processing environment through its mission statement and charter. Planning improvements, however, are needed to improve upon the integrity, confidentiality and availability of House data and services dependent on CAPNet transmission.

Specifically, HIR could improve security between its trusted internal House network (BUDNET) and the untrusted, external network (CAPNet) by assessing proxy firewall functions between these two networks. Firewall functions are currently limited to packet filtering. Packet filtering may not provide the level of access security needed to protect the House's information resources

[3] Overall risk rankings are categorized according to the highest risk identified within each weakness.

as a long-term solution and as firewall security approaches evolve. Proxy functions are essential to any risk assessment activities.

The absence of a security checklist exists because HIR has not yet completed at the time of our review a technical risk assessment of House CAPNet assets. The overall risk assessment framework should incorporate regular assessments of relevant information risks to the achievement of business objectives and provide a basis for determining how identified risks should be managed to an acceptable level. A security checklist would standardize House CAPNet operations with other HIR functions and serve as a basis for future reviews. The checklist is material in that it impacts HIR's ability to secure internal House networks from CAPNet vulnerabilities.

We recommended that HIR take two actions to improve the COBIT planning process and organizational objective. These actions include assessing risk posed by CAPNet and establishing a security checklist for House CAPNet assets. (See Exhibit 1 for the detailed recommendations in this area.)

Delivery and Support

Effective controls over the House's CAPNet routers, configuration and logging servers are essential to safeguard against unauthorized use, disclosure, modification, damage, or loss of hardware, software, or data. Network and security administrators should develop and implement a system of logical access controls that ensures access to House CAPNet assets is restricted to authorized users. HIR relies on HISPOLs to manage the physical security and access controls over the House CAPNet environment. Although no serious security breaches were found during this review, HIR needs to (1) improve policies and procedures to ensure the effectiveness of House CAPNet security internally, (2) provide for a standard configuration in the House CAPNet community, and (3) collectively manage House CAPNet resources. Management provides for system security by installing and managing safeguards to ensure that the overall effectiveness of the House CAPNet environment is maintained. During our House CAPNet risk assessment, network security review, and policy review we identified the following delivery and support weaknesses related to the use of the House's CAPNet routers and supporting servers.

- Routers
    - The routers did not properly control password access in accordance with user account management controls;
    - One router was not configured fully for event logging;
    - The routers did not apply adequate traffic filtering; and
    - Security settings preset by the vendor were not changed during installation to adequately limit access to House systems.
- Configuration Server

- The configuration server did not limit access in accordance with user account management controls;

- The configuration server did not limit unauthorized access in accordance with identification, authentication, and access configuration controls; and

- The configuration server was hosting non-essential services that may provide unauthorized access to the information systems.

- Logging Server

  - The logging server was hosting non-essential services that may provide unauthorized access to the information systems; and

  - The logging server did not adequately control access to House systems in accordance with user account management controls.

The above weaknesses exist because HIR did not incorporate essential security principles into a security checklist for House CAPNet assets. Specifically, HIR had not developed standards related to user account management requirements, access and privilege rights, system security functions, and security surveillance. These weaknesses impact the HIR's ability to deliver effective House CAPNet services. If House CAPNet servers are not effectively configured, it could cause resources and data to not be uniformly managed or secured within HIR and increase the risk of loss or corruption of sensitive data and services.

We recommended that HIR take 14 actions to improve system security, standardize the configuration, and improve the development of secure trusted relationships to provide a more secure operating environment. (See Exhibit 2 for detailed recommendations in this area.)

Conclusion

CAPNet, which currently disseminates unclassified information to the public, was not designed to be a trusted system. Its internal control environment is not the sole responsibility of HIR because its network management is decentralized amongst the Legislative branch members. Each organization that is connected to the network is responsible for purchasing and maintaining its own hardware, software, and network connection. As a result, weaknesses in the overall CAPNet internal control environment can have a serious effect on the security of the House's information resources. Therefore, HIR should protect sensitive House information resources from unauthorized access via other CAPNet members' connections.

Our review identified areas where House CAPNet assets are vulnerable and HIR security controls can be improved. We recommended that HIR perform a technical risk assessment to identify House CAPNet vulnerabilities and incorporate security provisions into the assessment to determine their impact on House information systems. Also, HIR can improve the security configuration of the two House CAPNet routers, the configuration server and the logging server

by defining effective, efficient internal control techniques in procedures and practices to include a security checklist to standardize operations. HIR has already corrected 50 of the weaknesses identified during the audit. The remaining 16 recommendations in this report, when implemented, should increase the security controls over House CAPNet resources.

Management Response

On September 13, 1999, the CAO fully concurred with all 10 weaknesses and 16 associated recommendations. The response indicated that corrective actions were taken or planned for all recommendations. These include: (1) completing a technical risk assessment of the House CAPNet connection; (2) 10 actions for developing a CAPNet security checklist with appropriate requirements for the router, configuration server and logging server; (3) documenting and minimizing FTP access; (4) encouraging other CAPNet Engineering Task Force participants to provide compensatory controls or disabling the generation of ICMP unreachable messages; (5) two actions for analyzing operational requirements and current hardware and configurations to assess the feasibility of providing encrypted Telnet; and (6) requesting funding for a dedicated server to perform router maintenance.

Office of Inspector General Comments

The actions taken by the CAO for Recommendations 1A, 1B, 2, 3, 4A, 4B, 5A, 6, 7, 8A, 9A, and 10 are responsive to the issues identified and satisfy the intent of the recommendations. Upon verification, we will close the recommendations. Actions planned for Recommendations 5B, 8B, 8C, and 9B are responsive to the issues identified and when implemented will satisfy the intent of the recommendations. Further, the milestone dates provided for completing these actions appear reasonable.