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: June 15, 1999

SUBJECT: Audit Report - Additional Controls Needed Over The Windows NT Environment At The House (Report No. 99-CAO-04)

This is our final report on the effectiveness of general controls over the Windows NT client/servers owned by the Chief Administrative Officer and administered by House Information Resources. The purpose of this review was to:

- conduct a high-level assessment of the Windows NT network installation, operation, and oversight to identify inherent vulnerabilities;
- conduct a network security review of the physical and logical controls associated with the Windows NT network to include testing for known vulnerabilities; and
- review the administrative, operational and security policies, to include a comparison against criteria.

During this audit, we found no serious breaches of security. However, we did disclose that control processes need improvement to ensure the continued successful implementation of the House's strategy to use the Windows NT client/server environment to serve its information technology (IT) needs.

In this report, we identified 26 weaknesses and made 52 specific recommendations for corrective actions in three major areas. These areas are (1) planning and organization, (2) delivery and support, and (3) monitoring. 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. Monitoring consists of management's oversight of the organization's control process and independent assurance. The weaknesses identified in these areas are discussed in Exhibits 1 through 3 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 three areas were material and substantially increase the risk of unauthorized access, modification to, and disclosure of House information. Furthermore, deficiencies related to physical access to the data center increase the risk of unauthorized access and theft or destruction of hardware, software, and information.

In response to our December 21, 1998 draft report, your office concurred with the reported weaknesses and recommendations. The March 25, 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 me or Christian Hendricks 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

Since 1993, the U. S. House of Representatives has been developing and implementing a mainframe migration plan that will ultimately provide computer services in a client/server environment. The Chief Administrative Officer's (CAO) Strategic Plan 1999-2003 addresses the migration to client/server technology, as a solution to its Information Technology (IT) needs. In this migration, Microsoft Windows New Technology (Windows NT) products are replacing UNIX and Netware systems architecture. Windows NT is an advanced 32 bit server operating system that provides multi-processing, multi-tasking, and multi-platform support. The system comes with two versions, Windows NT Server operating system (Server) and Windows NT Workstation client operating system (Client). The Windows NT Server could be used as a client operating system; however, the Workstation is more suited to the task because it costs less and allows for more centralized security.

The Windows NT Servers and Workstations are connected to a network and arranged into domains. A domain is simply a group of logically connected computers running Windows NT that share a single user account database. The Windows NT network currently provides House Members, Committees, and staff with several information network services such as e-mail, World Wide Web access, common software applications and training. Windows NT servers are located in various offices throughout the House Office Buildings (HOB), with the majority of the servers being located in the computer room on the 6th floor of the Ford HOB.

House Information Resources (HIR) is responsible to the CAO for the effective management of Windows NT security issues for the House. Windows NT system security features are located in the Local Security Authority, Security Account Manager, Security Reference Monitor, and logon processes. System security is administered by limiting access to objects, such as files and printers, to ensure that applications and users only gain system access where they are authorized. System administrators assign permissions to users and groups to grant or deny access to objects and set rights to control the actions that a user or group can perform on the system. The HIR Office of Security provides specific security guidance for Windows NT system administrators through House Information Security Policies (HISPOLs) and the Windows NT Security checklist.

Objectives, Scope, And Methodology

The overall objectives of this review were to evaluate the effectiveness of the general control environment of the Windows NT client/servers owned by the CAO and administered by HIR. The primary purpose of this review was to:

- conduct a high-level assessment of the Windows NT network installation, operation, and oversight to identify significant inherent vulnerabilities;

- conduct a network security review of the physical and logical controls associated with the Windows NT network, to include testing for known vulnerabilities; and

- review the administrative, operational and security policies, to include a comparison against criteria and development of recommendations for improvements.

We conducted this review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. We performed the following specific tasks:

- Gathered House documentation relating to Windows NT hardware and software acquisition, development, and implementation; network hardware and software; communications controls; domain and trust relationships; server and workstation configuration; logical security; utilization and activity reporting; network operating system and registry maintenance; and backup/recovery.

- Gathered House documentation relating to administrative, operational and information security policies, standards, and procedures for the Windows NT network, including HISPOLs and the Windows NT Security checklist.

- Gathered logistical data (i.e., system administrator contacts) needed to perform testing.

- Performed a high-level inventory of software and hardware.

- Performed a preliminary assessment of data and identified potential risks.

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

- Used PricewaterhouseCoopers' proprietary Windows NT vulnerability scripts and third-party automated tools *Internet Security Scanner (ISS)* and *DumpACL* to gather configuration data and tested for known vulnerabilities.

- Conducted a physical security review of the Windows NT network, based on potential risks.

- Conducted a detailed analysis of Windows NT policies, procedures, and standards to identify weaknesses.

- Compared results with best practices and Federal policies and standards.

There were 65 servers owned by the CAO and administered by HIR; 26 were in a test environment and 39 were in production. Per HIR's request, the 26 servers in the test environment were excluded from the scope of this review. All of the 39 production servers were selected for detailed review. This review was conducted from June 1998 through September 1998.

In addition to the *Government Auditing Standards,* we applied other federal and private industry criteria. We also used the Information Systems Audit and Control Foundation (ISACF) IT guidance "Control Objectives for Information and Related Technology" (COBIT), the IT Management and Reform Act of 1996, the National Institute of Standards and Technology (NIST) Standards, ISACF's Computerized Information Systems (CIS) Audit Manual, the National

Security Agency (NSA) Guide to Implementing Windows NT in Secure Network Environments, and the Microsoft Windows NT Security Guidelines.

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 evaluates and adopts 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 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

Within the scope of this review, we evaluated Windows NT general controls used to assure the confidentiality, integrity, availability, and compliance. No serious breaches of security were found. However, this audit disclosed significant weaknesses in the Windows NT server environment security access controls, security program and functions, and business continuity planning. If not corrected, these weaknesses pose a threat to the successful migration of services from the mainframe to the Windows NT client/server environment. The overview of significant control weaknesses is arranged into three CobiT domains and summarized in and detailed in Exhibits 1 through 3.

Prior Audit Coverage

There were no prior comprehensive audits specifically related to the overall Windows NT controls evaluation.

II. RESULTS OF REVIEW

During this audit, we found no serious breaches of security. However, the control processes need improvement to ensure the continued successful implementation of the House's strategy to use the Windows NT client/server environment to serve its IT needs. We identified three major areas that need improvement: (1) planning and organization, (2) delivery and support, and (3) monitoring. Planning and organization covers strategy, tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Delivery and support is concerned with the delivery of required services that range from traditional operations over security and configuration aspects to training. Monitoring IT processes should be regularly assessed over time for their quality and compliance with control requirements. Collectively, deficiencies in these three areas were material and substantially increase the risk of unauthorized access, modification to, and disclosure of House information. Furthermore, deficiencies related to physical access to the data center increase the risk of unauthorized access and theft or destruction of hardware, software, and information.

The prevailing reasons for many of these deficiencies were attributed to the lack of certain formal data center security standards, policies, and procedures; lack of segregation of duties; non-compliance with key vendor guidelines for Windows NT integrity; and lack of a formal comprehensive data security program.

Overall, we identified 26 weaknesses and provided 52 recommendations for improving the Windows NT general control environment of HIR. We categorized the recommendations associated with the weaknesses identified by a priority of High, Medium, or Low. High represents significant security and general control weaknesses that could adversely impact Windows NT computer operations and should be addressed immediately or consideration should be given to shutting down the Windows NT server. Medium represents security and general control weaknesses that could adversely impact aspects of Windows NT computer operations, but does not need to be addressed immediately. Low represents general control weaknesses that could improve controls over Windows NT that should be addressed. The table below illustrates the number of control weakness by CobiT domain, number of recommendations, and overall risk ranking, for each CobiT domain referenced. Details of the control weaknesses are described in Exhibits 1 through 3. The Exhibits to this report are "Confidential" and may not be disclosed or released to anyone other than auditee management except by approval of the House Office of Inspector General.

CobiT DOMAIN	EXHIBIT	CONTROL WEAKNESS NUMBER	NUMBER OF RECOMMENDED ACTIONS	OVERALL RISK RANKING
Planning and Organization	1	5	11	MEDIUM
Delivery and Support	2			
Ensuring System Security		9	20	MEDIUM
Managing Performance, Capacity, and Configuration		3	3	MEDIUM
Managing Facilities and Operations		3	8	MEDIUM
Monitoring	3	6	10	MEDIUM
Total		26	52	

Summary of Domain Weaknesses

Based on our interviews, review of relevant documentation, and detailed tests performed, the overall assessment is deemed to be medium. During this review, HIR started the process of drafting HISPOLS, policies, and procedures to implement an effective Windows NT environment for the House.

Planning and Organization

Effective planning and organization is essential to achievement of the House's strategic objective to migrate from a mainframe to a Windows NT client/server environment. The CAO's Strategic Plan 1999-2003 made a commitment to use the client/server technology as the solution to its information processing needs and communicated the House vision for this new processing environment through it mission statement and charter. HIR drafted a Technological Infrastructure Plan[1] in support of the CAO Strategic plan. However, improvements in the Technological Infrastructure Plan are needed to ensure the availability, reliability, and effectiveness of the Windows NT resources. Specifically, the plan needs to identify how assets such as applications, technology, and facilities are to be procured, connected, operated, safeguarded, backed up, and supported. The HIR organizational structure also needs changes to support the Windows NT client/server environment and ensure that the confidentiality, integrity, compliance, and reliability of the data are maintained. We noted the following problems with HIR's efforts to institute a proactive management approach:

- HIR's Technological Infrastructure Plan did not adequately address the need for multiple, redundant servers to provide user authentication in instances when a server is down, backup procedures for Windows NT servers, and support for migration strategies for Windows NT client/servers.

- HIR Backup domain controllers were not designated for all Windows NT domains that provided authentication on the network as a potential contingency control mechanism.

[1] The HIR Technological Infrastructure Plan supports the CAO Strategic plan by addressing technological aspects such as systems architecture, technological direction, and migration.

- The Office of Security had not established a viable, proactive security program to address the issues and concerns associated with a client/server environment.

- The proposed placement of the Quality Assurance (QA) function violated the standards of independence established by best business practices within IT standards. Under the current organization, the sole HIR QA position is placed in the Office of Security. This placement does not provide adequate separation of duties and responsibilities to ensure the independence and objectivity of the QA function to meet the needs of the organization.

- Some HIR Windows NT servers examined did not have the Random Access Memory (RAM) and disk space required to provide uninterrupted service. Specifically, 13 of 39 Windows NT servers did not have disk fault tolerance features, such as continually recording server data to a second hard disk, sufficient RAM capacity, or sufficient hard disk space available to ensure uninterrupted service.

These weakness are material in that they impact HIR's ability to effectively and efficiently maintain the client/server environment. HIR management must maintain a system that meets user expectations for availability, reliability, and integrity. The absence of redundant servers to provide user authentication if a server goes down, and lack of procedures for backup, contingency, and support in the Technological Infrastructure Plan could effect data accuracy and timeliness and presents a risk to the organization.

These weaknesses associated with planning and organization noted above occurred because HIR had not yet developed a technical business process to standardized HIR Windows NT operations, or a cohesive technology security policy. In addition, the QA role lacked independence and system administrators were not emphasizing the importance of configuration management and performance issues.

We recommended that the Chief Administrative Officer take eleven actions to improve the planning process and organizational structure. These actions include: assigning resources necessary to develop a technical business process to implement the Technological Infrastructure Plan, standardizing HIR's Windows NT operations, and developing a technology security policy; repositioning the QA role within HIR to a more independent position; and emphasizing the need for HIR system administrators to consider configuration management issues, such as improving logging and performance procedures and designating backup controllers for Windows NT operations. (See EXHIBIT 1: Planning and Organization, for detailed recommendations in this area.)

Delivery and Support

Effective controls over HIR's Windows NT environment are essential to safeguard against unauthorized use, disclosure, modification, damage, or loss to hardware, software, or data. Security administrators should develop and implement a system of logical access controls that ensures access to Windows NT systems is restricted to authorized users. HIR relies on HISPOLs and Windows NT checklists to manage the physical security and access controls over the Windows NT environment. Although no serious security breaches were found during this review,

HIR needs to improve policies, procedures and the checklists to ensure the effectiveness of Windows NT system security, manage performance, capacity, ensure standard configuration, and manage IT facilities and operations. Weaknesses noted in delivery and support are summarized below in three categories: (1) ensuring system security, (2) managing performance, capacity, and configuration, and (3) managing facilities and operations.

Ensuring System Security. Management provides system security by installing and managing safeguards that ensure the overall effectiveness of the Windows NT environment. HIR needs to address the following problems to improve system security:

- Virus checking software was not maintained on two critical, high volume HIR Windows NT servers. The two servers, E-mail Messaging and Group Messaging, are used by the majority of accounts on the Windows NT network.

- HIR individual and group account management procedures were not effective to adequately limit user access to the Windows NT resources. We found numerous instances of non-compliance with account management best practices.

- HIR user activities were not restricted through the proper use of home directories, logon scripts or workstation and time restrictions in 32 of the 39 servers reviewed. Additionally, we found users and groups possessed excessive rights in 21 of the 39 servers reviewed.

- HIR servers in the Windows NT network environment did not adequately authenticate a user's request for data, which violates the trust of the other servers on the network.

- The "EVERYONE" default group access permission allowed sensitive data on the Windows NT network to be shared without the knowledge of the users.

- Services were configured inconsistently in the HIR Windows NT network, which violates the trust between servers on the Windows NT network. Specifically, we noted weaknesses affecting passwords, system authentication and settings such as the Message and Alert Service functions.

- Eight of 39 HIR Windows NT servers examined were not properly formatted in accordance with House policy.

- Five of 16 HIR system administrators who have Windows 95 workstations used the Windows NT management tools to create user accounts from their workstations and thus could be accessed by anyone assigned to the "EVERYONE" default group.

- Systems administrators were not using standard naming conventions to identify users and resources. Instead, system administrators were using his or her own naming convention to identify their organization and servers.

The above weaknesses occurred because HIR did not have anti-virus software protecting all Windows NT servers and had not evaluated the applicability of best business commercial practices

provided by CobiT, NSA, and Microsoft. Specifically, the House had not adopted a standard Windows NT configuration, trust relationships between servers were not consistent, and the Windows NT security checklist was either not adequately developed or properly followed.

We recommended that the CAO take 20 actions to improve system security by resolving HIR Windows NT issues affecting use of anti-virus programs; evaluating the use of business practices provided by CobiT, NSA, and Microsoft; standardizing the HIR Windows NT configuration, improving the development of secure trusted relationships, and developing and implementing an improved HIR Windows NT security checklist to provide a more secure operating environment.

Managing Performance, Capacity, and Configuration. To properly manage the Windows NT environment, standards must be set as they relate to performance, capacity, and configuration structure. The CAO needs to improve the Windows NT services described below in order to assure a more effective migration of services from the mainframe to the Windows NT environment:

- We found unlicensed demonstration software on 3 of 39 HIR servers reviewed. System administrators had installed the software on a trial basis for a limited time, but the software trial period expired before the purchase request was approved and paid.

- HIR had no configuration inventory of Windows NT hardware, operating system and application software, and facilities locations or data files.

- Maintenance reports for the Windows NT servers were not consistently maintained for the 39 HIR servers reviewed.

These weaknesses occurred because Windows NT procedures and the checklists had not been adequately developed to enforce Windows NT compliance with HISPOLs, require inventories of Windows NT assets, and ensure proper maintenance of Windows NT assets.

We recommended the CAO take three actions to improve system security by developing Windows NT procedures and improving the checklists to enforce compliance with Windows NT best practices and HISPOLs; require inventories of Windows NT assets, and ensure proper maintenance on Windows NT assets.

Managing Facilities and Operations. Managing physical surroundings and supporting operations are important aspects associated with the effective delivery of services within the Windows NT environment. The CAO needs to improve the Windows NT environmental facilities and operations described below:

- In the absence of approved HIR policies and procedures for server security, system administrators were implementing ad hoc procedural and physical security measures.

- HIR system administrators created Emergency Repair Disks in different ways and storage was not consistent. For example, the Messaging Systems group used the '/s' parameter when creating the disks but the Internet Services group did not. Some of the Messaging Systems

group and the Internet Services group updated the disks whenever a change occurred on the system but others did not. Also, not all of the system administrators stored the disks in a locked storage area.

- Three servers did not have the latest service packs installed. Along with other needed upgrades and corrections, service packs implement Microsoft's Year 2000 fixes.

These weaknesses occurred because Windows NT policy and procedures were either not developed or were inadequate. Additionally, system administrators did not always adhere to established Windows NT security procedures.

We recommended the CAO take eight actions to revise HISPOLs to improve physical security, develop procedures to ensure preparation of effective emergency repair disks, and implement vendor provided service packs when appropriate to improve security over HIR Windows NT.

These weaknesses are material in that they impact the House's ability to deliver effective Windows NT services. If Windows NT servers are not effectively configured it (1) increases the risk of a disk loss or corruption of sensitive data and services, (2) causes resources and data to not be uniformly managed or secured within HIR, and (3) allows any user to become a system administrator in several HIR Windows NT domains or to read the recipient, sender date and time, of all electronic mail sent in the House Exchange domain. (See EXHIBIT 2: Delivery and Support, for detailed recommendations in these three areas.)

Monitoring

Management's monitoring of the Windows NT server's operational performance and general control procedures helps ensure that the server's system of controls is efficient and effective. Management should design procedures to detect, log, and monitor access control activity and key performance and general control vulnerabilities. HIR delegates monitoring of the Windows NT environment to systems administrators and the security division. HIR security was monitoring operational performance of Windows NT operations. However, monitoring actions were needed to improve the detecting, logging and access controls to ensure the availability, reliability, and effectiveness of the Windows NT resources. Specifically, HIR needs to develop a re-certification program and regularly test servers, perform risk assessments to determine the applicability of vendor provided security controls, and develop checklists to improve logs and retention periods for security data collection. We noted the following problems with HIR's efforts to institute a proactive management approach:

- HIR did not perform regular security monitoring and compliance testing to re-certify the compliance of Windows NT servers with House security policies.

- Registry settings that could enhance domain security were not completely addressed in the HIR Windows NT security checklist.

- Access activities associated with system, file, and directories; registry access; and printer and remote access failures were either unrecorded, or recorded inconsistently from server to

server. Of the 39 HIR servers reviewed, only 28 had the Windows NT policy setting activated and only one server had the object setting enabled. Both settings need to be enabled to effectively audit access activities.

- Windows NT server settings concerning logs of system and application events were not consistent between HIR servers. We found no standard settings or guidelines on how events were to be recorded, reviewed, or retained, which resulted in inconsistent monitoring activities.

- The File Transfer Protocol (FTP) features were used on 4 of 39 HIR servers reviewed. The FTP logging features that provide monitoring of FTP activities were not enabled on any of those four servers. In addition, the Web site banner on one of the 4 servers contained no warnings about unauthorized access.

- The "FullPrivilegeAuditing" setting used to log the activities of the backup operator group was not activated on 17 of 39 HIR Windows NT servers reviewed. As a result, the backup operator group activities were not monitored.

Proper monitoring activities provide assurance that the Windows NT system general controls are working. If not corrected, the weaknesses in monitoring will reduce the confidentiality, integrity, availability, and reliability of information produced by the system. While these weaknesses did not occur in all servers reviewed, they affect the entire network because the individual servers share resources and data in a trust relationship.

These weaknesses occurred because the HIR Windows NT servers did not have sufficient logging and monitoring capacity. In addition, the Windows NT security checklist prepared by the HIR Office of Security did not provide the systems administrators with comprehensive guidance on monitoring the systems' internal and external use. Also, the Windows NT security checklist needs detailed guidance on the proper monitoring settings and procedures for reviewing the data recorded.

We recommended that the CAO take ten specific actions to improve the HIR Windows NT logging and monitoring capacity, revise the HIR Windows NT security checklist, and develop additional security settings for HIR Windows NT servers. (See EXHIBIT 3: Monitoring, for detailed recommendations in this area.)

Conclusion

During our review, HIR started the process of drafting HISPOL policies and procedures to implement an effective Windows NT environment for the House. However, the general control deficiencies described in this report for the servers owned and managed by the CAO could have a significant impact on the House's IT management if not corrected timely. HIR needs to amend its HISPOLs, in order to set the standard for other Windows NT users within the House to follow. Specifically, HIR needs to amend the Windows NT security checklist by standardizing Windows NT operations to ensure the confidentiality, integrity, availability, compliance, and reliability of Windows NT data.

Management Response

On March 22, 1999, the CAO fully concurred with all 26 weaknesses and 52 associated recommendations. Subsequent to the audit, the CAO revised HISPUB 002.0, *Windows NT 3.51/4.0 File Server Security Analysis Checklist* to address security policy issues for Windows NT client/servers in response to Recommendations 3A, 3B, 12, 25A, and 25C. On March 26, 1999, revised HISPUB 002.0 was posted to the HIR web site for dissemination to authorized staff. Additionally, the CAO, in response to Recommendation 4, directed the reassignment of the Quality Assurance Evaluator position from the Director of Security to the HIR Deputy Associate Administrator.

The response also indicated that numerous other corrective actions were underway or planned for addressing the remaining 46 recommendations. These include: (1) developing a Technological Infrastructure Plan; (2) assigning adequately trained personnel to implement the Technological Infrastructure Plan; (3) addressing contingency areas such as redundancy resilience, adequacy and evolutionary capability in the Technological Infrastructure Plan; (4) ensuring acquisition and procurement support for the Technological Infrastructure Plan; (5) assessing HIR's Windows NT domain configuration and obtaining backup domain controllers for each domain; (6) incorporating infrastructure contingency procedures in the Technological Infrastructure Plan; (7) improving the dissemination of security information to the House community; (8) assessing fault tolerance tools and practices in the Windows NT environment, deploying tools that meet user requirements, and establishing acceptable levels of fault tolerance; (9) developing procedures to monitor disk space utilization on Windows NT servers, with a minimum of 20 percent free space, and ensuring that servers have sufficient memory capacity to perform efficiently; (10) evaluating alternative anti-virus software products for use on Windows NT Exchange servers; (11) addressing HIR Windows NT naming conventions in the Technology Infrastructure Plan; (12) revising HISPUB 002.0 to improve Windows NT security; (13) incorporating a Windows NT configuration inventory in the Technological Infrastructure Plan; (14) developing Windows NT maintenance reporting requirements in the Technological Infrastructure Plan; (15) moving the CAO backup domain controller and Client Services test server to a secure location and reconstructing walls in the computer room to prevent unauthorized access; (16) assessing the operating system versions installed on all Windows NT servers to procure necessary upgrades for the current operating system release; (17) adopting a system recertification program that regularly monitors and tests servers for compliance with House policies and guidelines; and (18) developing an oversight program for HIR system administrators.

Office of Inspector General Comments

The actions taken by the CAO for Recommendations 3A, 3B, 4, 12, 25A, and 25C are responsive to the issues identified and satisfy the intent of the recommendations. We therefore consider them closed. The actions taken and planned for the remaining 46 recommendations are responsive to the issues identified and, when fully implemented, should satisfy the intent of the recommendations. Further, the milestone dates provided for completing these actions appear reasonable.