John W. Lainhart IV
Inspector General

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

MEMORANDUM

TO: Wilson Livingood
Sergeant at Arms

FROM: John W. Lainhart IV John W. Lainhart IV
Inspector General

DATE: March 5, 1996

SUBJECT: Audit Report - Poor Planning, Questionable Contracting, and Numerous Internal Control Deficiencies Undermine Integrity and Usefulness of House Identification System (Report No. 96-SAA-03)

This is our final report on our evaluation of the House Identification (ID) System and Services. The objectives of this audit were to (1) obtain an overview of the House ID System, (2) determine the effectiveness of management and application controls associated with the House ID System and Services, and (3) determine whether the system satisfies the needs of the House. We also conducted an evaluation of overall planning and the contracting practices used to develop and procure the House ID System. In this report, we identified numerous system security weaknesses and internal control deficiencies that threaten the integrity of the system and made specific recommendations for corrective actions.

In response to our December 29, 1995 draft report, your office fully concurred with our findings and recommendations. The January 31, 1996 management response is incorporated into this final report and included in its entirety as an appendix.

We appreciate the courtesy and cooperation extended to us by your staff. If you have any questions or require additional information concerning this review, please call David I. Berran or me at (202) 226-1250.

Attachment

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

Poor Planning, Questionable Contracting, and Numerous Internal Control Deficiencies Undermine Integrity and Usefulness of House Identification System

Report No. 96-SAA-03
March 5, 1996

RESULTS IN BRIEF

CONCLUSIONS

The Office of House Identification Services (House ID Services) used inadequate planning, questionable contracting, and ineffective contract administration to acquire and implement an identification/access control system that did not meet the House of Representatives (House) needs or justify the nearly half million dollars the House invested in it. Specifically, the House ID System: (1) contained records representing terminated employees and/or misleading information; (2) provided user access/update capability to either of two host computers; (3) maintained inadequate controls to protect against unauthorized transactions, invalid input, or modifications to system data; (4) operated ineffectively and inefficiently when processing data, queries, and reports; and (5) was not covered by a contingency/disaster recovery plan. As a result, the House must contend with a system that (1) provided questionable value in terms of security over and access to House buildings; (2) contained no access control to protect data from unauthorized access or manipulation; and (3) included significant system design weaknesses that diminished the usefulness and reliability of the House ID System. Deficiencies of the House ID System occurred primarily due to inadequate contracting procedures, lack of established System Development Lifecycle (SDLC) procedures, and the lack of technically qualified personnel to properly support and maintain the system.

RECOMMENDATIONS

We recommend that the Sergeant At Arms (SAA): (1) immediately terminate all pending or planned expenditures for system upgrades or modifications except for support and maintenance costs to keep the system operational until a system re-evaluation can be completed; (2) act upon one of the following short-term options to correct identified weaknesses: (a) require Controlled Access Concepts (CAC) to provide the technical support it was contracted to provide by assigning a new representative that is technically qualified to support software as well as the hardware needs of the House ID System or (b) cancel the CAC contract and work with the Office of Procurement to re-compete the contract to acquire a qualified contractor with appropriate technical expertise in Receptor's software and UNIX computers and operating systems; and (3) re-assess overall House needs to determine if the House ID System satisfies House needs and whether continued investment in the current system is warranted, for the long-term. Also, we recommend that the SAA (1) remove the UNIX system passwords from the Computer Operations Guide; (2) assign a database administrator to the House ID System with experience in UNIX, Informix, and relational databases; (3) establish security controls to limit access to Informix Viewpoint and Informix DBA to only authorized users; (4) establish system access controls to eliminate access to system database files and tables directly; (5) require CAC to take immediate steps to correct deficiencies in the House ID System; and (6) order a capacity analysis of the House ID System to determine capacity requirements. Furthermore, we recommend that the SAA, in conjunction with the Chief Administrative Officer: (1) work out an agreement to transfer ID workstation equipment in the House Information Resources security office to House ID Services, eliminating the unnecessary expenditure of House funds; (2) establish a pre-exit clearance procedure for all paid and non-paid employees who are terminated; and (3) establish a business resumption and contingency plan for the House ID System, assign responsibilities to appropriate individuals, and ensure the procedure is routinely tested.

MANAGEMENT RESPONSE

The Office of the SAA fully concurred with the findings, conclusions, and recommendations in this report. The SAA met with the House ID contractor, CAC, on February 8, 1996 to discuss the issues in this report that require their attention. The SAA has given the contractor 9 months to correct the reported deficiencies. Actions on the remaining recommendations will be completed on or before September 30, 1996.

OFFICE OF INSPECTOR GENERAL COMMENTS

The SAA's response to Findings A through E is adequate and satisfies the intent of the recommendations. Therefore, we consider these recommendations resolved and anticipate closing them after the corrective actions promised are implemented.

TABLE OF CONTENTS

I. INTRODUCTION

Background

The U.S. House of Representatives (House), Office of Identification Services (House ID Services), under the oversight of the Sergeant at Arms (SAA), is responsible for issuing identification (ID) cards to permanent staff, interns, Member's families, liaison offices, contractors, and pages. House ID Services supports the House's legislative responsibilities by providing controls over access to House office buildings, including the Capitol. Identification Services prepares and issues new ID cards to all House employees (around 13,000 in total) at the beginning of each Congress and typically issues approximately 12,000 additional ID cards a year to cover new hires, interns, and replacements for lost or stolen IDs.

In August 1992, during the 102nd Congress, the then SAA issued a Request for Proposals (RFP), through House Information Resources[1] (HIR), to acquire an automated identification badging and access control system to replace the existing manual badging process. An agreement between the House and Controlled Access Concepts, Inc. (CAC), was entered into on November 24, 1993 for an indefinite delivery, indefinite quantity contract. The contract specifies an identification/access control system programmed by Receptors, Inc. (Receptors) of California, with CAC as the local vendor. The first purchase order for the House ID System was issued on September 30, 1993, and the first Phase of the ID system was implemented at the start of the 104th Congress in January 1995.

The new identification/access control system was designed to implement new procedures for issuing ID cards and controlling access to House office buildings. Access to the 24-hour entrances and garages was to be controlled by the ID system. As installed, the current system includes two UNIX host computers, six workstations, access control units in HIR, and readers for garage access (not yet activated). Additional workstations were purchased, but installation of the workstations and activation of the garage access readers was postponed until after the SAA completes a security review of the House[2].

The House ID System is composed of a collection of workstations (PCs) that use application software to access information in a database that resides on two UNIX[3] host computers. The House ID System application software was programmed in 'C++' by Receptors and was modified/customized to meet the needs of the House. The application software is used to access and manipulate the database information for the House ID System and is maintained by

[1] On July 14, 1995, the Committee on House Oversight renamed House Information Services (HIS) to HIR.

[2] Upon taking office and being briefed on our *1994/95 Annual Audit Plan*, the current SAA expressed concerns with respect to the House ID System and asked us to give a higher priority to this audit in order to augment his security review.

[3] UNIX refers to an operating system developed by Bell Laboratories that features multi-programming in a multi-user environment.

Receptors. The House ID System database was created by Receptors using the Informix database programming language and formatting rules. The database is mirrored (duplicated) on both hosts to provide continuity in case one host goes down. The host computers, which consist of two servers--a primary and a secondary unit--are UNIX boxes running the SCO UNIX operating system. Receptors provided the hardware components under the contract, including the UNIX operating system. CAC is contractually responsible for hardware maintenance, including all House ID System equipment, and for application software and database support. However, all software development enhancements or corrections to the House ID application software and database are carried out by Receptors' programmers in California.

Future phases of the implementation called for installing access control units at all 24-hour access points and workstations at guard locations. The RFP called for integrating the identification/access control systems for the House, Senate, Library of Congress, and Architect of the Capitol.

Objectives, Scope, And Methodology

The objectives of this audit were to (1) obtain an overview of the House ID System, (2) determine the effectiveness of management and application controls associated with the House ID System and Services, and (3) determine whether the system satisfies the needs of the House. Also included as an objective was an evaluation of the overall planning and contracting procedures used to develop and procure the House ID System.

Our work was limited to developing an understanding of the system development and operational aspects of the House ID System and included a review of contracting practices that led to its procurement. We also conducted limited audit work in HIR because of that organizations' involvement in and support of House ID Services' contract with CAC. In order to perform a comparative systems analysis, we also looked at the Senate's efforts to obtain a similar identification system off the same RFP that resulted in a contract with the software vendor that indirectly provided the same software for the House ID System.

We conducted our review in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. The audit work included such tests and auditing procedures as were considered necessary under the circumstances. We conducted our audit work during the period April 1995 through November 1995.

Our review included the following steps:

-- Reviewing applicable government-wide internal control criteria that address controls in computer based systems.

-- Conducting interviews regarding programming and testing activities and automated controls with House ID and HIR personnel, and with appropriate contract personnel from CAC and Receptors.

-- Reviewing pertinent House ID documents including the RFP, office policies and procedures, badging system specifications, the House ID System contract, a software capabilities overview, and other miscellaneous ID service-related documentation.

-- Developing a system process flowchart to illustrate the sequence of events and processes involved in creating, controlling, and tracking an ID master record.

-- Conducting on-site visits and physical observations of current and planned access control points around the House Campus and random testing of same.

-- Selecting and analyzing two unique random samples of records from the House ID host databases to determine integrity and reliability of the data contained therein.

Internal Controls

During this review, we evaluated internal controls over the House ID System and House ID Services operations. The internal control weaknesses we identified are described in the "Findings and Recommendations" section of this report.

Prior Audit Coverage

The House ID System is a relatively new system and therefore has not been audited by the Office of Inspector General (OIG), the General Accounting Office (GAO), or any other internal or external audit organization. However, a related study, conducted by the U.S. Secret Service under contract to the Sergeant at Arms, looked at the overall security implications associated with public access to House Office buildings--access that would presumably be controlled through the House ID System. That study was not available for our review prior to the issuance of this report.

Price Waterhouse LLP (PW) conducted an audit of selected functions within the Sergeant at Arms' office, including House ID Services (Report No. 95-SAA-14, entitled *Opportunities Exist To Improve Resource Utilization In The Office of The Sergeant At Arms*). However, PW's work in House ID Services was limited to an analysis of staff usage relative to seasonal workload fluctuations and did not touch upon any of the issues discussed in this report nor did it address the House ID System itself.

II. FINDINGS AND RECOMMENDATIONS

Finding A: Planning and Contract Management Weaknesses Contributed to an Ineffective House ID System

Inadequate planning, questionable contracting, and ineffective contract administration resulted in the acquisition and implementation of an identification/access control system that did not meet House needs or justify the nearly half million dollars the House invested in it. As a result, the House must contend with a system that provided less control over access to House buildings by employees or the general public than was originally envisioned and was of questionable value with regard to its security capabilities. These problems developed because the system was not identified as an essential acquisition in any short- or long-term planning document prepared by House staff; was not subjected to the scrutiny of a rigorous needs assessment that is a requirement in all standard system development methodologies that precede most procurements; and was not funded through normal appropriations channels but instead was paid for out of re-programmed funds at year-end.

Planning for House ID System did not adequately assess House needs

Management personnel responsible for developing an identification and fully-functioning access control system did not perform the up-front planning required to identify available systems that would satisfy House needs. We found no evidence of a feasibility study, a needs assessment/requirements analysis, or an alternatives analysis to support the system selected. The House spent approximately $473,000 for a system that is not always used for identification purposes and which provides questionable value regarding access control because system planners failed to adequately assess House needs or recognize the unique, open environment of the House campus.

Although the House did not follow any formal planning requirements, adequate planning guidelines exist in the government and private industry. Federal Acquisition Regulations (FAR) that govern contracting practices for the Executive Branch requires strategic planning. FAR Part 34, Subpart 34.004 requires the program manager to develop an acquisition strategy tailored to the particular major system acquisition program. This strategy is the program manager's overall plan for satisfying the mission need in the most effective, economical, and timely manner. In addition, Office of Management and Budget (OMB) Circular A-130 requires agencies to establish multi-year strategic planning processes for acquiring and operating information technology that meet program and mission needs, reflect budget constraints, and form the basis for their budget requests. While House management was not required to comply with the FAR, a prudent manager should recognize the benefits to be gained by following these guidelines. Such was the case with Senate personnel who stipulated adherence to FAR requirements in developing their contract for the Senate Identification system--one that was nearly identical to the House ID System and which was procured using the same RFP.

The House had no master implementation plan to ensure timely phased implementation of the

House ID System. Specifically, no overall strategic plan existed to provide present or future strategies for funding and implementing the system at the House. Although the RFP for the House ID System stated that both access control and ID capabilities would be implemented, no documentation existed to indicate the timing and planned implementation date for access control. Also, the RFP stated that future integration of the House ID System with the Senate and Library of Congress systems was planned, however, no evidence of joint planning between the House, Senate, and Library of Congress existed. In addition, no long term budgeting or funding issues for the House ID System were considered when contracting for and implementing the House ID System. Instead, all funding provided for the acquisition and enhancements of the House ID System was reprogrammed money spent at year-end. Consequently, scheduled implementation of House ID System enhancements and equipment purchases could not be predicted because funding was not planned or allocated in advance.

Inadequate planning by former SAA management resulted in additional expenditures for an access control system that did not consider the House environment. For example, the access control readers, that cost $188,164.50, installed in the House building garages under the authorization of the SAA were never activated. These access control readers were purchased without determining the practicality of access control implementation. In contrast, the Senate, recognizing the limitation of access control in a public building setting and using the same RFP, opted not to purchase access control and went with a stand-alone ID system.

In our review of system documents and through discussions with House ID personnel, we found no evidence that consideration was given to the practicality of implementing an access control function in public access buildings. Although the RFP outlined the potential of the House ID System to provide access control for entrances of the House, Senate, and Library of Congress buildings, neither the RFP nor any other planning documentation we reviewed provided evidence as to how access control function would function or be integrated with the Capitol Police operation to replace or supplement the need for policemen who now maintain 24-hour access control to the buildings. While a representative of the police was involved in the system selection process and the data element definition for the ID records, Capitol Police management was not consulted on the practicality of using the access portion of the ID system to eliminate the need for them to monitor selected House entrances. Besides which, the SAA did not have the authority to mandate that the House ID System be used to supplement or replace the need for the Capitol Police to monitor entrances either during or after normal business hours. Consequently, the effectiveness of using a computerized access control function in buildings open to the public was not fully considered or documented before the former SAA obtained the access control portion of the House ID System.

Poor procurement practices plagued House ID System implementation

Poor procurement practices plagued the contracting and funding obligation process of the House ID System. Although the House did not have procurement policies and procedures in place, adequate contracting guidelines exist within the government and private industry that establish sound contracting and funding obligation practices. The FAR, Subpart 16.504, defines an indefinite-quantity contract as a contract that will provide for an indefinite quantity, with specified minimums and maximums, to be furnished during a fixed period. In such a contract, any required minimum purchase must be obligated when the contract is executed. Also, 31 USC §1501 (a)(1)(B) states that a contract should be executed before the end of the period of availability for obligation of the appropriation or fund used for specific goods to be delivered, real property to be bought or leased, or work or service to be provided.

The former SAA issued RFP 92-002 on August 3, 1992 for an ID/Badging and Access Control System for the House. CAC, one of five qualified bidders to respond, submitted a Technical Proposal in response to the RFP on September 8, 1992. On September 30, 1993, over a year later, the House issued a purchase order for $265,000, obligating FY 1993 funds, two months before the contract award date of November 24, 1993, as illustrated in Figure 1.

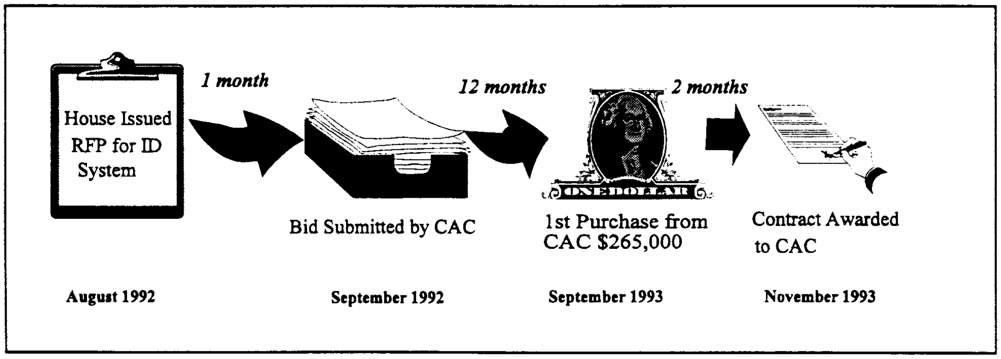

Figure 1 Timeline of Procurement Activities for the House ID System

In addition, the House used questionable award practices to issue the contract for the House ID System to CAC. For example, the SAA issued the contract for the House ID System to the third overall contractor, based on the weighted average of the technical and cost evaluations. Good contracting practices in the Federal government state that contracts should be awarded to the number one contractor in the technical and cost evaluations. In this case, the former SAA did not award the contract to the first overall contractor because the Senate had cancelled their contract with that contractor for non-performance. However, no explanation or justification was given as to the reason the second overall contractor was not awarded the contract for the House ID System with the House.

Also, the House contract, which was awarded as an indefinite delivery, indefinite quantity contract, specified that schedule, cost, and equipment parameters be negotiated separately for each delivery order. Common business practices for contracting in the Federal government, as cited above, establish that specific requirements be provided in the contract for equipment, cost, and schedules for implementation. For example, the Senate identified specific system equipment requirements in their contract for an ID system, such as a specification that Receptors software be compatible with hardware in place at the Senate to eliminate the need to procure additional hardware. However, the House provided no written specifications in the House ID System contract for equipment, cost, or schedules other than a reference to the RFP requirements and a contract minimum value of $265,000, which was met by the first delivery order.

Based upon a review of documentation and in discussions with SAA personnel, we determined that the House did not have procurement policies and procedures in place during the period when the House ID System was contracted. In addition, officials responsible for the procurement of the House ID System did not use sound contracting and fund obligating procedures as established by many Federal government regulations. One highly visible example of the disregard for procurement practices and the intent of the law, was the execution of a purchase order fully 2-months before the contract was formally awarded. Officials responsible for the actions no longer work for the House and we could find no documentation to explain how the action was justified. As a result, we believe the contract was not executed in a reasonable manner.

Inadequate contracting knowledge and procurement procedures resulted in the procurement of a House ID System using questionable procurement and fund obligating techniques. Therefore, the House had no guarantee that it procured the best system in a cost effective manner. Also, poor procurement processes left the House susceptible to appeals by the lower bidders and created the impression that the House had little regard for good business practices in conjunction with year-end spending and fund obligations.

System documentation was incomplete and system testing was not performed

House ID System management did not ensure that Receptors, through CAC, provided adequate system testing results and sufficient system documentation as provided in the contract. Several government regulations exist that emphasize the importance of adequate system testing results and system documentation in order for maintenance and support personnel to effectively ensure the system operates as intended. FIPS Pub 106, *Guidance on Software Maintenance*, Section 4.2.2, states that the documentation of a system is essential to good maintenance and should start with the original requirements and design specifications and continue throughout the lifecycle of the system. Additionally, the guidance requires the inclusion of all pertinent material to support system maintenance and use and it must be easily and quickly retrievable. For system testing requirements, FIPS PUB 101, *Guideline for Lifecycle Validation, Verification, and Testing of Computer Software*, specifies that a validation, verification, and testing methodology is a needed procedure to ensure the production and maintenance of quality software.

No formal system testing was performed for development or enhancements of the House ID System. The local Receptor representative stated Receptors' headquarters in California might have some testing documentation, however, Receptors had provided no evidence of any system testing at the time this report was issued.

System documentation was not provided as specified in the CAC contract or RFP requirements. Although some documentation was received on the House ID System, the technical manual and the House specific SCO UNIX operating system manual was not supplied. Although Receptors was aware of the documentation requirements in the RFP and OIG requests for testing documentation, Receptors was not responsive to House requests. It appears that the contractual arrangement between the House and CAC puts Receptors beyond the reach of the House. However, the House should exercise its rights under the contract with CAC to force CAC to meet the contractual obligations for this information.

As a result, House ID management had no assurance that the House ID System operated as intended. The absence of system test results provided greater potential for the House ID System to have unidentified problems which could result in data loss or serious system malfunctions. Finally, insufficient system documentation made it more difficult for House ID Services and HIR staff to effectively administer and operate the system.

System support and maintenance is not timely or responsive

House ID System support and maintenance were not performed in an effective, timely, or responsive manner because no contractual obligation existed between the support vendor, Receptors, and the House that would force the vendor to provide adequate support and maintenance. As a result, House ID Services operated a system with significant design deficiencies, creating a greater potential for data loss and poor security controls.

FIPS Publication 106, Section 4.1, *Controlling Software Maintenance*, states the goal of software maintenance and support is to keep systems functioning and to respond to user requests in a timely and satisfactory manner. Given the realities of staffing limitations, computer resource limitations, and the user request backlog, this goal is difficult to achieve. The realistic goal, then, is to keep the software maintenance and support process orderly and under control. The specific responsibility of the software maintenance and support manager is to keep application systems running and to facilitate communication between managers, users, and maintainers. Controlling software maintenance and support involves an orderly process in which all requests are formally submitted, reviewed, assigned a priority, and scheduled. This process defines a philosophical approach which can help the software maintenance and support manager bring order to the software maintenance and support environment.

House ID System support from Receptors was virtually non-existent. Specifically, the list of system problems, outstanding as of August 31, 1995, that HIR provided OIG auditors, received little or no reaction from the vendor for system corrections. For example, the 11 items outstanding on the system problem list as of August 31, 1995 were not corrected before this report was issued. Significant problems, such as Host-1 not mirroring Host-2 accurately (See Finding B for detailed discussion) and no security installed for the Informix database, remained unresolved for three months with no compensating controls implemented to protect House ID data loss or deletion.

Also, House ID System maintenance was not performed on a routine basis. Neither Receptors, CAC, nor HIR performed any type of routine preventive maintenance on the host or application software. In fact, the CAC vendor stated that House ID System maintenance was performed on a strictly reactionary basis to something reported as a problem. No preventive maintenance of the UNIX host computers such as performing statistical analysis of hardware failures was routinely performed either.

Furthermore, the House ID System problem list maintained by CAC was not an adequate log for tracking system problems. The system problem list, which was the closest thing CAC had that resembled a problem log, did not track (1) when calls were received, (2) who received the call, (3) who would be servicing the problem, (4) the expected problem resolution date, or (5) the actual resolution date for the system problem. An adequate system problem log should be formalized and contain all pertinent information about system problems and the steps that were taken to resolve them.

House ID System support was hindered by the cumbersome process and structure designed to report system problems. Anytime a system problem was identified, the procedures required that House ID Services report such problems to HIR, who in turn reported them to CAC, who then communicated the system problems to Receptors. This system support structure was created and supported because of the contractual arrangement, i.e., the contract was with CAC not Receptors. Compounding the problem was the fact that CAC's on-site representative assigned to the contract had no experience with Receptors' software or the UNIX computer and operating system. Accordingly, all software and hardware support for the House ID System must be handled by Receptors.

As a result, the House could not directly hold Receptors to any system support or maintenance requirements. According to a CAC representative, Receptors is generally unresponsive to requests for solutions to system problems. For example, House ID personnel reported loss of data entry due to the mirroring problem between Host-1 and Host-2 but Receptors offered no solutions nor proposed corrective action. Consequently, House ID personnel were forced to work with a system that at times did not function very efficiently or effectively. These uncorrected problems, coupled with the design deficiencies described in Findings C and D, created a potential threat to the integrity and security of the system.

Recommendations

We recommend that the Sergeant at Arms:

1. Immediately terminate all pending or planned expenditures for system upgrades or modifications except for support and maintenance costs to keep the system operational until a system re-evaluation can be completed.

2. Act upon one of the following short-term options to correct identified weaknesses:

   a. Require CAC to provide the technical support it was contracted to provide by assigning a new representative that is technically qualified to support software (i.e., has basic database expertise and is generally knowledgeable about Receptors application software concepts) as well as the hardware needs of the House ID System.

   or

   b. Cancel the CAC contract and work with the Office of Procurement to re-compete the contract to acquire a qualified contractor with appropriate technical expertise in Receptor's software and UNIX computers and operating systems.

3. For the long-term, re-assess overall House needs to determine if the House ID System satisfies House needs and whether continued investment in the current system is warranted.

4. Adopt policies and procedures governing procurement actions that are being developed by the Office of Procurement in response to OIG recommendations contained in Report No. 95-CAO-11, for future procurements.

5. Adopt System Development Lifecycle policies and procedures that are being developed by House Information Resources in response to OIG recommendations contained in Report No. 95-CAO-20 for future system development/procurement efforts.

Management Response

On January 31, 1996, the Office of the SAA fully concurred with this finding and all five recommendations (see Appendix). According to the response, several initiatives are either underway or planned to ensure that the effectiveness of the House ID System can be achieved. Actions taken and planned include: (1) suspending two outstanding purchase requests for House ID computer equipment; (2) discussing identified weaknesses/problems with CAC and implementing a corrective action deadline no later than November 8, 1996 and enforcing vendor resolution or the contract with CAC will be terminated; (3) reassessing the overall security needs of the House by a joint Capitol Complex Security Survey utilizing the U.S. Secret Service, the U.S. Capitol Police, and the Sergeant at Arms staff with a completion date of April 1, 1996 and completing a House ID system security and operations needs assessment performed by the National Security Agency to complement the Capitol Complex Security Survey; (4) adopting the policies and procedures developed by the House Procurement Office; and (5) adopting the System Development Lifecycle (SDLC) policies and procedures currently under development by the House Information Resources while complying with the National Institute of Standards and Technology's SDLC guidelines during the interim.

Office of Inspector General Comments

The SAA's actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding B: Data Reliability and System Capacity Issues Contribute to System Inefficiencies

Our review of the House ID System indicated that almost one third of the master database contained records representing terminated employees and/or misleading information. In addition, user access/update capability to either of two host servers in a mirrored configuration, raises internal control and reliability issues regarding the master database residing on these computers. Data processing standards adhered to by Executive Branch agencies and private industry strictly prohibit co-mingling of active and inactive records in any master file and the use of "generic" control records (e.g., Day Laborer) for convenience purposes. House ID System managers also agreed to a contractor recommended six-fold increase in system capacity without benefit of a capacity analysis or before optimizing current storage usage. These conditions existed because (1) House ID personnel had limited systems management knowledge and (2) there were no policies and procedures or an internal control structure in place to ensure compliance with sound database and resource utilization management practices. As a result, the House ID System may be operating at less than peak efficiency; management may be wasting scarce resources on unnecessary system upgrades while needlessly taking up storage capacity; and holders of inactive ID cards may be unknowingly permitted unauthorized access to House offices during non-business hours.

Terminated employees found to be active on House ID database

Using audit data retrieval software, we matched active employee records on the HIR master payroll file against records maintained in the House ID System and identified 1,048 records representing employees who no longer work for the House. Seventy-two percent or 757 records represented terminated employees who were carried on the House ID System as active employees and who still had valid ID cards in their possession. Because there was no formal, automated or manual mechanism of notifying House ID Services of terminations as they occurred, the House ID System viewed these records as representing active employees. House ID Services maintained inactive records on the system to help them identify employees that did not return their ID cards upon termination. Also carried on the House ID System, but not on the payroll or personnel files, were interns and other unpaid staff who would not show up in our match. Therefore, a significant number of individuals could maintain authorized access and be in possession of valid ID cards beyond their termination with the House. Employee ID cards could be used to access House buildings and certain secured areas within those buildings during non-business hours. Since the House had no formal exit/out-processing procedures, there were no assurances that IDs would be returned upon termination of employment. During the audit period, the Office of the Chief Administrative Officer (CAO) implemented CAO-wide exit procedures that included, among other things, the threat of withholding an employee's final paycheck until the ID card was returned. House ID personnel indicated they thought this could be a very effective tool if applied on a House-wide basis.

Former employee ID records that were carried on the House ID System as active not only took up valuable storage space and distorted accurate record keeping but also created a potential false sense of security and could contribute to former employees gaining unauthorized access to House office buildings during non-business hours.

Host-1 or Host-2: Which is more reliable?

House ID System host computers maintained unreliable information because host controls were ineffective. The system was designed using the concept of Host-1 as the primary system and Host-2 as the back up or "mirror" system. Therefore, Host-1 should be the system where all data entry, modifications, and deletions occur for personnel data records with an immediate, on-line back up to Host-2. However, we tested the controls over data entry and deletion between Host-1 and Host-2 and found that records were not updated to the secondary host. For our test, we entered several records into Host-1 and none were mirrored to Host-2. We also reversed the test and entered records into Host-2 which, likewise, were never mirrored into Host-1. In addition, when we deleted records from one host, they were not deleted from the other host, as should have occurred.

Using the Informix Structured Query Language (SQL) query capability, we tested the record counts for personnel records on each host for several different dates and found Host-2 contained more records then Host-1, as indicated in Figure 2, even though Host-1 was considered primary.

Date	Host-1 Record Count	Host-2 Record Count	Difference in Record Counts
10/12/95	17,629	17,632	3
10/13/95	17,627	17,629	2
10/31/95	16,326	17,096	770
11/3/95	16,238	17,199	961
11/6/95	16,138	17,099	961

Furthermore, on one of the dates tested, October 31, 1995, we also performed a count of the number of photo images in the image directories which were also maintained on the host computers. Although the personnel data record counts performed on this date resulted in more records on Host-2 than Host-1, the number of images on Host-1 was greater than the number of images on Host-2, i.e., 12,624 versus 12,397, respectively. The House ID System was designed to link one photo image to each personnel record, consequently, the number of images and personnel records should be the same. We believe the image discrepancy could have occurred because of a defect in the software that processes record deletions. When the data portion of a record was deleted, its matching photo image (which is in a separate file) should automatically be deleted because it was linked to its data record. However, because of the processing defect, the image was not deleted and subsequently cannot be distinguished from the other images in order to be deleted.

As a result of almost non-existent host controls, system users were faced with determining which host contained accurate information and whether all data was effectively recorded. House ID personnel constantly complained to Receptors, through CAC, about data record losses and an inconsistent ability to retrieve data. Personnel data records could sometimes be located on both hosts; sometimes only on Host-1, and sometimes only on Host-2. Consequently, House ID personnel could not be sure that information they entered into the House ID System remained and, therefore, expended extra time and effort locating and/or re-entering ID data that was lost because of the questionable reliability of the host update process.

The House ID System was not reliable because the host access controls and technical support provided by Receptors and CAC were not effective. Multi-host configurations are designed to provide reliable redundancy in the event something goes wrong. Host controls are necessary to prevent users from accessing and entering information directly into the mirror or secondary host, except when authorized in emergency situations. Otherwise, users should only be able to access Host-1 for data entry, modifications, and deletions (See Finding C for a discussion on access controls). Receptors was made aware of this problem, but had not offered any solutions or proposed corrective action. The problem concerning host computer reliability was further intensified when Receptors and CAC provided contradictory statements over the functions and controls of the host computer. The local Receptors vendor stated that Host-1 was the primary system with Host-2 as the mirror system, as stated above. However, the CAC vendor stated that Receptors in California led him to believe that information entered into either host would mirror to the other host, i.e., there was a two-way mirror between Host-1 and Host-2. Unfortunately, the problem has not been resolved and the question as to the reliability of the system still remains.

System capacity: Is there a problem?

Even though the House ID System has been operational for less than a year, the contractor recently recommended a hardware upgrade that will provide almost six times the current storage capacity at a cost in excess of $20,000--all without justification or demonstrated evidence that such an upgrade will correct outstanding operating problems. When the former SAA contracted for the House ID System in 1994, the vendor who was awarded the contract, CAC, proposed a system that would purportedly handle all of the known identification and access control needs of the House as specified in the RFP. The system that was proposed was an off-the-shelf package originally designed for an airport application. According to SAA personnel, the vendor modified this system to meet the requirements of the RFP. However, according to House ID personnel and from audit observation of the system in operation, the system contained "excess baggage" in the form of additional processing modules, input screens, and non-essential data elements that contribute nothing to the House ID System but take additional processing time to bypass and require storage that may be contributing to the capacity problems. The House ID System, which has been on-line for less than a year, was reportedly troubled with capacity problems (according to the contractor) that affect both record storage and processing efficiencies. The contractor's solution was to replace the two 700-megabyte (million byte) file server hard drives with two 4-gigabyte (billion byte) hard drives that would increase storage capacity by a factor of six and cost an estimated $8,750[4] each. (The SAA's office agreed to the OIG's recommendation to suspend purchase of additional computer equipment for the House ID System pending a review of audit recommendations.) According to House ID personnel, however, the contractor provided no support for this solution, i.e., they had not conducted a capacity analysis (or proposed to do one) nor taken into account the effect of removing almost a third of the current database records and correcting other capacity-related anomalies discussed in this report. For example, one of the specifications in the RFP required an image compression capability that would reduce the digitized photo images (the picture part of the ID card that is also stored on the servers) by a ratio of 10 to 1 to reduce storage needs. The contractor bid a high resolution photo compression capability of 20 to 1. However, that capability has not functioned correctly or consistently since the system was installed--it still remains an outstanding problem awaiting correction by the contractor. An analysis and correction of this capability, which the contractor was required to deliver in working order under the basic contract, coupled with a resolution of the capacity issues raised above, may provide a better measure of capacity for determining system needs.

<u>Invalid ID records were misleading and occupied needed storage space</u>

Our review of the House ID System also identified (a) 4,134 records representing employees who never received ID cards (b) 64 records containing duplicate social security numbers (SSNs), and (c) 88 generic ID cards. These records represented approximately one fourth of the House ID System database.

Prior to the 1994 elections, House ID personnel requested and received an electronic file (download) from HIR's Financial Management System (FMS) of all employees on the House payroll in anticipation of issuing new ID cards to them. Of the total number of records downloaded, some 4,134 (24 percent of the master file) records represented House employees that did not return for the start of the 104th Congress. As a result, these individuals never received ID cards, however, they remained on the House ID database as active employees. House ID personnel told us during our December 8, 1995 audit exit briefing that many of these records had already been deleted from the system. With regard to the duplicate SSN records, we found 31 instances, involving 62 records, where the SSNs were the same. The presence of these duplicates indicated an internal control weakness involving edit checks on data entry but also

[4] We conducted a brief review of hardware vendor offerings and noted a consistent price range of between $2,000 and $3,000 for comparable, top of the line, hard drives--a significant difference compared to the CAC price.

represented 31 additional master records that should not be in the database. A review of these records also indicated that they may have been issued more than one ID card but we were unable to pursue that issue due to missing information in the records. In 13 of the 31 cases of duplicate SSNs, both records are listed as active, suggesting that a purge of inactive records based on record status would not eliminate these duplicates. (See Finding D for a detailed discussion on system edit checks.)

We also found that individual offices were given generic IDs which were issued to groups of people, rather than to individuals. The 88 generic IDs were issued under names such as "House Plumber," "Visitor," and "Clerks Office." The ID cards were maintained by the offices rather than individuals. By not issuing the IDs to individuals, accountability for the use of the ID card and access granted by the ID was lost. Anyone could access controlled areas by using these ID cards that did not have names or images attached to the authorization.

Inadequate data entry controls, the absence of database maintenance policies, and questionable judgement regarding the creation of "generic" records contributed to data integrity deficiencies; diluted the reliability of information in the House ID database; and provided inaccurate information to the decision-making process regarding system capacity needs.

Recommendations

We recommend that the Sergeant at Arms, in conjunction with the Chief Administrative Officer, develop a proposal to the House Oversight Committee to establish a House-wide pre-exit clearance procedure for all paid and non-paid employees who are terminated that will require, among other things:

(a) withholding final paychecks for paid employees until ID cards are returned and the exit clearance process completed, or

(b) holding the employing office responsible, both procedurally and financially, for all non-paid employees to successfully complete the pre-exit clearance process and return ID cards.

We recommend that the Sergeant at Arms take action to correct House ID System weaknesses and deficiencies by:

1. Requiring CAC to take immediate steps to correct deficiencies in the Host to Host update process.
2. Requiring CAC to correct the software deficiency that is preventing a simple, one-step deletion of records (photo images and associated data) in the record deletion process.
3. Requiring CAC to eliminate users' ability to access Host-2 to enter, modify, or delete data, except on an emergency basis.
4. Requiring CAC to correct the problems that are preventing consistent operation of the image compression process at the rate proposed in their bid.
5. Requiring CAC to modify House ID software to delete non-essential data elements and screen modules that may be contributing to system capacity problems.
6. Ordering a capacity analysis of the House ID System after all unnecessary records and images have been deleted to develop a basis for determining capacity requirements.
7. Conducting a market research analysis to identify reasonably-priced hard drives if the results of the capacity analysis indicate an upgrade is required.
8. Instituting procedure that prohibit the practice of issuing ID cards to "generic" users and ensure that all cards are issued to authorized individuals with specific information regarding card owners' characteristics, such as accurate social security numbers and specific office locations.

Management Response

On January 31, 1996, the Office of the SAA fully concurred with this finding and all eight recommendations including all subparts (see Appendix). According to the response, an initiative is underway to request the Chief Administrative Officer to develop a proposal for presentation to the House Oversight Committee to implement a House-wide pre-exit clearance for all paid and non-paid House employees. Furthermore, actions taken and planned include: (1) requiring CAC to correct data reliability and system capacity issues no later than November 8, 1996; (2) completing a capacity analysis of the House ID System by July 1, 1996; (3) complying with the Office of Procurement policies and procedures to identify hard drive replacements if the capacity analysis deems it necessary; and (4) recalling and destroying all "generic" ID cards issued by the House ID System by May 1, 1996 and developing a policy prohibiting the issuance of "generic" ID cards.

Office of Inspector General Comments

The SAA's actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding C: Improvements Are Needed in Controls and Security for the House ID System

The House ID System did not have adequate controls to protect against unauthorized transactions, invalid input, or modifications to system data. Internal control policies and procedures that are generally accepted by government and private industry prescribe that an internal control structure should encompass basic security procedures to ensure system and data integrity can be relied upon, adequate segregation of duties, and restricted logical and system access. The House ID System had no audit trail function to track and monitor system transactions; operated under inadequate system security and ineffective access controls; and neither provided for adequate separation of duties nor implemented UNIX security controls properly. In addition, those persons responsible for developing and maintaining security controls over the system were not required to submit to a background investigation themselves, a requirement of many Federal agencies and data center operations in particular. As a result, House ID System data could be created, modified, and deleted intentionally or otherwise, all without detection by House ID Services personnel. Control and security weaknesses occurred because of design deficiencies in the House ID System and the lack of technically qualified personnel to administer security and access functions. Furthermore, failure to require background checks for those responsible for setting policy over security could compromise the integrity of the House ID System.

UNIX security controls were not properly implemented

Password administration controls were not established for the UNIX host computers. Passwords used to provide access to the UNIX host computers were published in the computer operations guide. In addition, UNIX system security settings and log files were not properly implemented. Furthermore, program change controls were not developed for code modifications.

Password administration

Password administration controls were not established for the UNIX host computers. Logon IDs and passwords are shared; passwords are documented in the computer operations guide; and password control settings had not been adequately implemented. There were five logon IDs used for the operations of the UNIX host computers, and all five, including their passwords, were shared by HIR, CAC, and Receptors personnel. Furthermore, the computer room operations guide that supported the House ID UNIX systems contained the passwords used to operate the hardware. Although passwords were removed when the document was given to OIG auditors, standard practices had been established by HIR management that publicized the UNIX passwords in the computer operations guide. In addition, the UNIX host computers had a password control feature that required a minimum character length for the password field. This feature had been set to a one character field. Also, two UNIX system features, that allowed the minimum and maximum timeframes for enforcing passwords to be routinely changed, had been set to zero, which essentially negated this control technique. Furthermore, password guidelines, including a password policy, had not been established to cover password usage and control of system passwords. Without adequate password administration procedures, control mechanisms to prevent unauthorized reading, altering, or destroying of House resources could not be achieved.

UNIX security

In the UNIX environment, mask values are assigned to grant access to files and directories in the system when files are created. For the current UNIX system configuration, the mask value had been defined to allow read, write, and execute rights to the file owner and read and execute rights to the other user categories (i.e., group and world). The mask value should allow read, write, and execute rights to the file owner and no rights for the other user categories. However, access controls for key files for the standard UNIX system directory files were not customized for the House ID System. These files were last modified in 1993, even though the House purchased and received the software from Receptors in 1994. The software was vendor installed and no modifications specific to House needs and control considerations of the ID system were implemented.

In trying to identify what UNIX controls were evident in the House ID System, we looked at three sets of critical files: the binary program files, the special files for input/output devices (I/O files), and the systems administration files. These files perform systems utility functions, configuration for input/output devices, and systems administration functions, respectively. We noted that not all of these files were reconfigured to run on the House ID System when the system was originally installed. For example 90 of 270 files were reconfigured (customized) for the binary program and I/O files and 40 of 292 files in the systems administration directory were reconfigured. When we tried to determine why some of these files needed to be customized while some did not, we were unable to obtain an explanation from House ID personnel because they lacked the technical systems expertise and there was no UNIX systems documentation available for us to review (see Finding A for a detailed discussion on documentation). Therefore, we relied on UNIX documentation that we purchased to determine whether the proper key files were reconfigured to provide adequate security for the House environment. For example, the binary program directory contains utility programs that allow searching for files with special characters and the ability to scan readable program files. Since security was poorly defined, access to these utilities offers users the opportunity to access files they were not authorized to access. In the I/O files, device files contained descriptions of terminals and other devices on the system. For example, users had access to the "kmem'" device, which gave them the ability to alter internal memory, a capability that should be reserved for selected systems programmers. The problem with UNIX security configurations was that no one in an official systems capacity, either in the SAA's office or the HIR representative assigned to the House ID System, could say whether the current configurations are proper, nor could they do anything about them without external support. Meanwhile, the level of security over the UNIX hardware and operating system was uncertain.

Log files

Log files were not established that would document UNIX system activity. The UNIX system contains a number of log files that could be utilized to track user log-ins, log-outs, and every command run by every user. These log files form the basis of the UNIX auditing system. These audit logs were never activated, therefore, transactions were not recorded, audit trails were not maintained, and security-related events were not logged into an audit transaction file. As a result, all system related transactions and events are not traceable and therefore accountability for any users actions, which the logs were designed to provide, cannot be achieved.

Change controls

Program change controls were not in place for software modifications. Program change modifications were performed by CAC at the request of House ID Services. For example, a change was needed to repair a card reader. When Receptors completed the program code modifications, CAC tested the reader to ensure that it was fixed. CAC did not review or scan the program code change but only verified the functioning of the card reader repaired. Also, CAC loaded the completed program change directly into the production environment without first testing the change in a secure environment. Furthermore, when Receptors required access to the UNIX system from a remote location, CAC turned on the modem and waited until Receptors was completed to turn the modem off. No dial back procedures were in place to ensure that valid personnel had accessed the House ID UNIX computers and no log existed of when and why the vendor needed to gain remote access to this system. For UNIX system modifications, system reliance was placed entirely with both vendors, CAC and Receptors.

Internal control policies and procedures that are generally accepted by government and private industry prescribe that access security be properly installed with all parameters appropriately set, e.g., minimum length of passwords, changing passwords routinely, access privileges, change control procedures, etc. Without adequate security administration, security and basic internal controls over hardware and software could be compromised resulting in a potential loss of data and system integrity. Furthermore, FIPS Publication 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Section 5, Systems Security, states that "Closely allied to the access control mechanism is the ability to account for who had access to which data. The control mechanisms form the basis for reports on data usage. These reports, known as audit trails, can be designed to list all system activity, all data accesses, unusual activity, etc. Such a report can be examined to identify unauthorized disclosures of data."

As previously described, the House ID System was purchased from and installed by CAC, a re-seller of proprietary software developed and licensed from Receptors. As stated by the Receptors vendor, their practice when they sell hardware and software is to install both hardware and software with all parameter settings open and unconfigured. They left the responsibility for customization and modification of hardware and software settings to the customer. Although the House contracted with CAC for system hardware and software support, CAC lacked the technical expertise and knowledge to establish or even provide advice on security configuration, implement system controls, and adequately maintain the UNIX host computers. HIR and House ID Services were unaware of the need to implement an internal control structure and security guidelines because of a lack of training in UNIX systems for their support staff and the lack of a clearly assigned systems administrator to support the UNIX systems configuration.

Without implementing an adequate system of internal controls, particularly at the hardware level, management relinquishes its ability to achieve an acceptable level of system reliability and places a great deal of blind trust in the hardware and software vendor. In addition, failure to properly restrict security access or monitor transaction processing within an established set of security guidelines, jeopardizes the integrity of the system.

Separating House ID responsibilities

House ID Services and HIR did not ensure that duties were separated for the data entry, hardware operations, application programming, and security administration functions for the UNIX host computers and application software for the House ID System. In addition, there are no acceptable compensating controls in place to offset the exposures created by the lack of properly assigned or segregated duties. GAO's *Standards for Internal Controls in the Federal Government* establishes requirements for separation of duties. The requirements specify that "duties and responsibilities should be assigned systematically to a number of individuals to ensure that effective checks and balances exist." Job functions for data entry, hardware operations, application programming and security administration should be segregated. This provides checks and balances to ensure that one person's work is verified by another person. In computerized application systems, separation of duties not only involves the division of tasks among people, but the division of tasks among automated processing steps.

Key functions for operating the House ID System were not defined or properly assigned to House ID and HIR personnel. The HIR application programmer assigned to perform computer operations, such as system back-up procedures for the House ID System, maintained full access privileges to the application source code. Allowing the programmer to access the application source code eliminated controls to monitor modifications to the application source code or the UNIX host configuration.

In addition, system users from House ID Services were assigned database administrator functions without the technical expertise to perform this function. For example, House ID personnel were provided access to and were responsible for operating the Informix Database Administration (DBA) module for the House ID System. The Informix DBA module is the administrative module used to set up the House ID database indices and views necessary to effectively perform query and reporting functions on the House ID System. A database administrator would be responsible for setup and administration of the Informix DBA module and would provide in-house technical support on the UNIX host and application system. Although House ID personnel responsible for this function received a three day training class in Informix, the training covered information mainly on how to use the reporting and query function after the views and indices were properly defined using relational database rules and principles. House ID personnel were system users having no technical training or experience in relational databases, Informix, or UNIX that would provide them the necessary skills to adequately setup and administer the House ID System. It is generally recognized in data processing operations that system users should only be involved with data manipulation of the system, not system administration.

Furthermore, the House ID System security administrator performed security functions and data entry functions for the system. One of HIR's security officers, who was assigned as the House ID System security administrator, was authorized to input access control level assignments and monitored door alarms for the House ID System. In addition, the system access level authorized to the HIR security officer provided him user access abilities such as add, delete, and modify for all information and modules of the House ID System--a clear violation of separation of duties control. Also, the HIR security officer maintained an ID workstation--camera, printer, and application software--needed to create House ID cards, even though this was not one of his assigned responsibilities. Consequently, his high level of system access, coupled with the fact that he had access to ID equipment, created the potential for ID cards to be issued without authorization from House ID Services. House ID Services should centralize ID card issuance and eliminate a procurement currently pending for a new camera, printer, and badging workstation, by requesting that HIR transfer its ID workstation and all of its components to House ID Services, an action that will save the House almost $25,000[5] and eliminate a serious internal control weakness.

House ID and HIR personnel did not require House ID System responsibilities be divided appropriately among personnel. Because of this internal control weakness, management could not be assured that potential errors and irregularities, such as the unauthorized processing of records and intentional or unintentional deletion of records in the House ID System, were promptly identified and corrected.

System access and security did not adequately prevent unauthorized data manipulation

House ID System access and password controls did not prevent unauthorized access and manipulation of data. FIPS Publication 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Section 2.2.2, "Risks from Uncontrolled System Access," states that "agencies expose themselves to unnecessary risks if they fail to establish controls over who can access the personal data which is processed on their ADP systems. Outsiders must not have free access to the personal data. The number of agency employees with access to personal data must also be kept as small as possible without hindering the mission of the agency." Also, FIPS Publication 41, Section 5.1, *System Security,* states that passwords are perhaps today's most widely used identification technique for granting system access. Passwords should be attributable

[5] The SAA's office agreed to the OIG's recommendation to suspend this purchase and a second purchase for two computer hard-drives for the House ID System (see page 14) pending review of audit recommendations.

to individuals in order to ascribe individual responsibility and reduce the likelihood of individuals giving out passwords to unauthorized co-workers. In addition, passwords should be easy to remember, but they should not be based on information such as a person's initials or birth date. It is best if the system administrators generate random passwords for users. Furthermore, passwords should be changed at given intervals as well as whenever compromise is known or suspected.

House ID System access controls did not adequately prevent unauthorized access of the data or the system. Specifically, access to House ID System data using Informix was unrestricted. Informix, which has a reporting and query capability, called Informix Viewpoint, and a database administration function, called Informix DBA, was used to access data from the relational database for the House ID System directly, without any access controls. The Informix DBA module, installed on one machine in House ID Services, provided any person who walked up to that machine access to the House ID System database. Any person accessing House ID data through Informix DBA could add, delete, and modify data outside of the application software. Also, Informix DBA would allow a user to completely restructure the database by adding tables, deleting tables, adding a whole new database, or deleting the entire current database, both structures and data. This powerful access privilege coupled with the fact that no screen savers or power-on passwords were used by House ID Services on any terminal, created a significant security weakness and exposure to the House ID System application and data. In addition, we identified several other mechanisms where access to House ID System data was not properly restricted or could be obtained without authorization. For example:

- System access to the House ID System did not restrict users from logging into Host-1 or Host-2. Users should be automatically logged into Host-1 for data entry, modifications, and deletions, unless emergency access is granted to Host-2. (See Recommendations in Finding B for access restrictions.)

- Disk Operating System and File Manager could be used to access House ID System data and files with no user authorization required, providing unlimited access to ID information.

Furthermore, inadequate password controls were used to control access to the House ID System application. We observed that the password file for the House ID System could be viewed by all level-8 system users. Level-8 access for the House ID System provided users the ability to perform all system functions such as additions, deletions, and modifications to data as well as system administration functions for the setup and modification of passwords. Because 6 of 12 users of the House ID System maintained this powerful level-8 access, the practice of maintaining an unencrypted password file seriously reduced the ability for passwords to restrict system access. Good system administration practices would dictate that only the minimum number of level-8 accesses be established in order to adequately limit system access to the functions necessary. In addition, passwords could be easily guessed, could not be changed by users, and were not set to expire at certain time intervals. For example, we interviewed a House ID System user that complained that his password was the same for over a year, that he could not change his password, and it would never expire. While performing audit testing, we also noticed several passwords that could be easily guessed such as vendor location or user name being used as the password.

The House ID System administrator lacked the training and technical understanding of Informix and relational databases to recognize the risk placed on the House ID System when no security or access control was implemented to restrict access directly to the database. In addition, no security administration procedures were established for the House ID System to provide guidance in password or access control usage.

Consequently, the lack of password and access controls for the House ID System provided unauthorized and unauditable access to system data. For example, all database files and database images could be deleted with no audit trail recording access and therefore no accountability for these actions through Informix DBA or File Manager. Further, none of those employees responsible for administering the House ID System--which deals directly with security--are required to submit to any type of background investigation. In September, 1995, the current SAA submitted a proposal to the Chairman of the House Oversight Committee requesting permission to use Capitol Police to conduct criminal and credit history background investigations on current and future employees of the SAA. The authority to require background checks, at least for those personnel involved in developing and/or implementing computer security controls over House systems, is necessary and we support the SAA's position in this regard. (Since the SAA already submitted this proposal, we are not including such a recommendation in this finding.) These serious weaknesses involving access control and security over the House ID System made it difficult to ensure control over data and system resources was maintained and that all system data was accurate and reliable.

Logical access was not restricted

Logical access[6] controls had not been adequately implemented for the House ID System. In addition, application system passwords had not been adequately secured. Without preventing the unauthorized use and access of a system, data integrity can be compromised by allowing the reading, altering, or destroying of any or all data items.

The House ID System is comprised of a combination of related tasks grouped into modules to facilitate the user's ability to operate the system. There are three levels of access assigned to the various users having access to the system enabling certain options for each module. The three levels were intended to (1) restrict the lowest level to inquiry capabilities, (2) restrict the middle level to day-to-day operations (e.g., badge creation), and (3) allow the highest level to perform systems administration tasks (e.g., new user setup, history log access, etc.). We tested the restrictions assigned to the three levels of access by entering into each module. As a result, we

[6] Logical access refers to the use of information-related mechanisms, such as passwords, rather than physical mechanisms, such as a cypher lock or physical recognition device, to provide access control.

noted various inconsistencies.

Thirteen of the thirty-nine modules contained no data. Within these thirteen modules, data fields had been established but House ID Services did not utilize these functions. As a result, the data fields were taking up unnecessary space thereby inefficiently utilizing system capacity (see Finding B for more on capacity issues). In addition, access had not been clearly restricted for each of the three levels. At the lowest level we were able to edit and delete in four modules. For example, we could have deleted the access control panels with the lowest level access. At the highest level we were able to view the password file that was unencrypted. Both of these system access deficiencies created a potential for unauthorized access and modification to important system data. Additionally, six of the twelve users had been assigned the systems administration level. Without consistent systems access administration procedures, data integrity cannot be achieved.

FIPS Publication 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Section 5, Systems Security, states that "While identification can go a long way toward preventing unauthorized use of a system, it is still necessary to have limitations on the use of data. Access controls can serve that purpose. They are the means of preventing a user, once having gained access to the system, from reading, altering or destroying any data he wishes. Lists (or even classes) of users authorized to perform certain activity or to access specified data or combinations of the two can be developed and stored in the computer to insure that only authorized data activity occurs. Implementation considerations are: 1) Some commercially available systems already have data access controls built in. In many cases these controls are not built in. In many cases these controls are not being used because some additional effort is sometimes required in reprogramming current applications. However, if needed, such access controls could provide a significant increase in data protection and, 2) Applications programs can have their own access control mechanisms built in if the operating system does not provide them."

The House ID System had the security capabilities that allowed only authorized users access to the system. However, House ID Services lacked the training and guidance necessary to implement proper security administration procedures and system access controls. Security capabilities should allow only authorized users access to the system and limit that access to specific functions. When user access is unrestricted, the risk to inadvertently destroy data increases, thus placing valuable House ID data and resources in jeopardy.

Recommendations

We recommend that the Sergeant at Arms request the Chief Administrative Officer direct the Associate Administrator for House Information Resources to:

1. Assign a technically qualified UNIX systems administrator to aid in the administration and maintenance of all facets of the UNIX computer systems. The systems administration functions should include, but not be limited to, basic security requirements of unique logon IDs, password administration procedures and guidelines, logging system transactions, removing equivalent host computers, and program change procedures.
2. Remove the UNIX system passwords from the Computer Operations Guide.
3. Implement procedures to ensure that all remote access into House resources is authorized, logged, and performed in a secure environment.
4. Ensure computer operation functions and application programmer functions, relative to the House ID System, are appropriately segregated.
5. Assign a database administrator to the House ID System with experience in UNIX, Informix, and relational databases.

We also recommend the Sergeant at Arms ensure that:

1. Security controls are established to limit access to Informix Viewpoint and Informix DBA to only authorized users.
2. The Informix DBA module is only accessible by the database administrator.
3. System access controls are established to eliminate access to the system outside of the applications software, directly to database files and tables.
4. The number of users with system administrator access to the House ID System is limited to a minimal number necessary to perform system administration functions.
5. Security administration procedures for the House ID System are established that include password and access control procedures.
6. House ID Services changes the access level of the House ID System security administrator to a "read-only" access level.
7. Assign technically qualified personnel to provide access control procedures to include, but not be limited to, reviewing access level capabilities by module and,
8. Implement a structured methodology to ensure that system access is granted based upon job function.

We recommend that the Sergeant at Arms work with the Chief Administrative Officer on a mutually agreeable arrangement to transfer ID workstation equipment in the HIR security office to House ID Services, eliminating the unnecessary expenditure of House funds.

Management Response

On January 31, 1996, the Office of the SAA fully concurred with this finding, its fourteen recommendations, and all subparts (see Appendix). According to the response, several initiatives are either underway or planned to improve controls and security for the House ID System. Actions taken and planned include requesting HIR to: (1) assign a UNIX system administrator by April 1, 1996 to monitor system security, audit logs, and evaluate software changes in a test environment; (2) remove all UNIX system passwords from current and future versions of the Computer Operations Guide and change published passwords immediately; (3) investigate and implement dial-back procedures for remote access with a completion date of July 1, 1996; and (4) assign a database administrator to the House ID System with experience in UNIX, Informix, and relational databases and, if such a person is not available, assign a partially qualified individual and bring him/her to a working knowledge of the database administrator requirements by June 1, 1996. Other actions taken and planned include: (1) limiting access to Informix Viewpoint and Informix DBA to only authorized users via a power-up password by June 1, 1996 until CAC establishes adequate access controls; (2) moving the Informix DBA to an area only accessible to the database administrator by September 1, 1996; (3) establishing security controls to prohibit unauthorized access to the system, database files and tables from outside the application software by July 1, 1996; (4) limiting access to the systems administration function to the systems administrator and granting access on an as-needed basis by April 1, 1996; (5) establishing security administration procedures for password and access controls which will be included in the SAA's System and Operations Manual by September 30, 1996; (6) modifying the House ID system security administrators access to "read-only" in order to monitor alarms; (7) assigning a SAA employee as systems administrator and establishing access control procedures by March 1, 1996; and (8) establishing a structured methodology for access level capabilities to be completed by the SAA systems administrator by September 30, 1996. Finally, the SAA will request the CAO to transfer the HIR House ID system workstation equipment from the Ford Building to House Identification Services by April 1, 1996.

Office of Inspector General Comments

The SAA's actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding D: Efficiency and Usefulness of the House ID System Can Be Improved

The House ID System did not operate in the most cost-effective and efficient manner when processing data, queries, and reports. Sound business practices and Federal regulations that govern this facet of information management, if adopted, would assist the House in implementing an efficient and effective processing environment for its automated systems. However, the House ID System did not (1) contain adequate edit checks to ensure that data entered into the system was valid and access was properly granted; (2) include adequate reporting capabilities to ensure that the information would be generated in an efficient manner; (3) include file archival capabilities which forced House ID Services to establish and maintain a separate database to track and report lost ID data. This occurred because House ID personnel were technically inexperienced users trying to manage a system that was poorly designed and poorly supported. As a result, the House ID System cannot be relied upon to provide the control environment that would satisfy House needs.

House ID System edits were not adequate

The House ID System did not have adequate edit checks to ensure that data entered into the system was valid and access was properly granted. The system did not prevent OIG staff from entering data that conflicted with other data in the same record. For example, the ID card number and the badge number are supposed to be the same, but the system accepted different information for both fields. Additionally, the access granted by an ID card did not change for records where the dates entered should have deactivated the access. Consequently, the reliability of the data contained in the House ID System was diminished.

We tested the House ID System to determine the existence of data validation checks on key fields to assess the reliability and quality of the data entered into the system. In the process, we attempted to enter duplicate records, records with invalid dates, and records without key data elements. We identified areas where the use of validation checks would increase data accuracy but these checks were not present.

Personnel records in the House ID System used the employee badge number and the social security numbers as key fields. The ID card number and badge number are separate fields within the system and were designed to be used for different purposes, however, House ID Services assigned the same value to each field. Our tests indicated that this was not always the case, as we found no edits that verified the card number field as unique or as having a data relationship to the badge number. While we noted the presence of edit checks for the badge number and social security number, we did find duplicate records keyed on these fields (see Finding B for more on duplicate records). Badge number and ID card number fields allowed us to enter hyphens as part of number, but restrictions against letters and other symbols prevented us from entering other data.

In testing data fields and their data relationships, the system required that we enter valid dates, using a four digit year coding convention, with an expiration date that had to be after the effective date. Our test indicated that there were no logical edits against other date fields such as the activation date and the issue date. For example, entering activation dates and issue dates that occurred after the expiration date were accepted without question. Furthermore, entering an expiration date prior to the current date for a personnel record on the system had no immediate effect on access level granted or the employee status. Future activation and effective dates also did not restrict access levels. While the name field had edits that prevented us from entering numbers and symbols, lead spaces were allowed.

Numerous standards exist to ensure that data contained in computer systems is accurate and useful. GAO's *Evaluating Internal Controls in Computer-Based Systems* requires that "on-line data validation and editing should be performed as early as possible in the transaction processing cycle to ensure that errors are detected and corrected quickly. Transactions and data fields should be edited for valid characters, sign, format, content, etc. This editing should be on all data fields even though an error may have been detected in an earlier field of the same transaction." OMB's *Model Framework for Management Control Over Automated Information Systems* establishes control requirements for application systems. These include:

- Transactions are valid--the information system must process only data that represent legitimate events.
- Information is complete--all valid data, and only those data, are to be processed by the information system.
- Information is accurate--data must be free from error during all phases of processing, within defined levels of tolerance.

The Receptors software used by House ID Services had limited edits built in to verify validity during data entry. Because the RFP for the House ID System did not include specific requirements for data verification and system edits, any additional edit checks would require software modifications. House ID Services was not provided documentation that would identify edit checks included in the system so there was no knowledge of what the system could verify or where manual verification should have been performed to ensure accurate data entry.

Without adequate documentation, especially for something as basic as edit checks, potential problem areas might not be identified by House ID Services. Inaccurate data could have been entered into and used by the House ID System since the edit checks were not present. The potential for individuals to have multiple badges or to have access to restricted areas existed. These errors could create additional work for House ID Services to correct information that should have been detected upon original entry.

System reporting capabilities are limited

The House ID System did not include adequate reporting capabilities to ensure that the information needed from the system could be generated, and done so in an efficient manner. The system only included four reports as a part of the application. Three of the four reports included the options for sending the report to the printer or the monitor. The reports included one called "Roll Call" that listed all ID cards accessing a given area by area number of last used reader. This report had no look-up capabilities to identify where card readers were located. The user must know the area number or the reader number in order to produce the report. The "Locate" report could be used to locate a card holder by last name or card number. Limitations were apparent if the last name was common, such as Smith, since first names were not included on the report. Social security numbers were displayed with the results of the query, but usefulness of the information was limited since the social security number would not always be readily available. The "Authorized Readers" report listed the authorized readers for a specified card by social security number. This report did not have any look-up capabilities, thus requiring the user to know the social security number before attempting to generate the report. The "Use It" report was described as a "use it or lose it" function for reporting all IDs not used since a user-defined input date. No guidance was provided with the report. The Reports Help function was not very helpful and did not provide the information that would be necessary for someone to run the report without prior knowledge. None of the four reports addressed reporting needs of House ID Services and were not used regularly.

The contract also required additional reporting capabilities to be provided through the use of Informix software. Data dictionaries, data tables, and table indices had not been provided to House ID Services. House ID Services was handicapped in their attempts to generate reports without knowledge of data relationships. For example, when we requested House ID Services to produce a report of all ID card holders with an access level other than zero, the first version of the report contained 293 ID cards but the final version of the report contained 436 ID cards. It was only after we requested this run that House ID Services started to provide similar access level reports to HIR on a periodic basis. The data tables and indices would have provided the users with the information that would enable them to identify appropriate elements for reporting themselves.

OMB Circular A-123, *Management Accountability and Control,* establishes the requirements to establish a means for monitoring program activity. These standards include that "...transactions should be promptly recorded, properly classified and accounted for in order to prepare timely accounts and reliable financial and other reports. The documentation for transactions, management controls, and other significant events must be clear and readily available for examination." The circular further states this information should be available on a daily and periodic basis for the operation of programs and systems.

House ID Services had not identified what reporting requirements existed for management oversight. Additional management reporting would be useful in monitoring such items as workflow statistics or expired ID cards. House ID Services did not have adequate training or resources so that they could use the Informix software to their advantage. The reporting capabilities included in the Receptors software were not sufficient to provide for management reporting. While House ID Services had Informix software, the available documentation did not provide sufficient information to efficiently generate reports. Without timely accurate reporting capabilities, management does not have necessary information to make decisions, track information, or evaluate the workload House ID Services was handling.

System capabilities did not meet user needs

The House ID System did not include capabilities to meet the needs of House ID Services. Aspects of the system design were resource intensive and not cost-effective. Vendor modifications to the software since the demonstration prior to procurement have eliminated some useful functions of the system. Consequently, the system did not perform necessary functions to facilitate the processing and management of House ID information.

The system had archival abilities when the system evaluation was performed. Under a new release of the software, Receptors eliminated the archival ability without user approval. The loss of this function created the need for House ID Services to look for other means to track historical data. Additionally, the ability to transfer data from one badge number to another badge number when an individual received a new ID card was lost. The password file encryption feature was also lost with the same release.

An application programming error caused the system to change the ID card status from current to temporary when the system was rebooted. In the House environment, all ID cards were issued with an expiration date since staff received new ID cards for each Congress. For permanent employees, the expiration date used was the end of the Congress, while temporary employees had varying ID card expiration dates. Because of the programming error, all master ID records appeared to be for temporary employees with only the expiration date as an identifier. Tracking of temporary and permanent employees was complicated by the application programming error resulting in House ID Services using the actual expiration date of the ID card to determine employee status.

OMB Circular A-130, *Management of Federal Information Resources*, requires that information management planning be included in an integrated manner for managing information throughout its life cycle. In planning system management, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information dissemination, should be considered. The design, development, and implementation of information systems should incorporate records management and archival functions. The House is not required to comply with OMB Circulars but the guidance they provide, if followed, could do much to improve House ID management oversight and system operations.

Receptors released a new version of the software to increase system capabilities but in the process, eliminated archiving, password encryption, and data transfer capability. The original release of the software that the House purchased included an archival capability, among other features now gone, that facilitated the tracking of lost ID cards and former employees. According to documents we reviewed, an HIR representative reviewed the new release and recommended that House ID Services accept it. House ID Services agreed without knowing what functions would be lost. There was no user testing and acceptance. Ironically, Receptors offered to re-install the archival capability for a $6,000 fee. When a problem was reported to Receptors, modifications to the software were made without the approval and, in some instances, without the knowledge of the user. No formal testing of changes was performed by Receptors, CAC, or House ID Services.

House ID Services lost capabilities of the system that were used for information management due to Receptors making changes without House ID Services approval of the change. Alternative solutions to the reporting and tracking requirements of House ID Services were implemented, such as maintaining a separate database for lost IDs and tracking temporary employees by expiration dates. These compensating actions present additional opportunities for errors to occur since the information must be entered more than once.

Lost ID card information not properly maintained

House ID Services maintained a separate lost ID database to track and report lost ID data since the House ID System lacked the historical data and reporting capabilities needed to generate lost ID reports. By duplicating the information in two separate systems, the potential for errors and omissions increased. The records we tested from the lost ID database had a 12.5 percent error rate. This level of error indicated that the information contained in the lost ID database was not reliable and raises questions regarding this separate method of tracking lost ID information.

We tested a random sample of 79 lost ID records to determine the accuracy and reliability of the data maintained in the lost ID database. In the process, we compared the information contained in the lost ID database against the personnel records and the history log for the House ID System. We verified the deactivation dates and status of lost IDs from the history log transactions. We also tested the data related to the replacement ID cards for card holder and issued date.

Of the records sampled, we identified ten records where the data in the lost ID database and the House ID System did not agree. In three of the ten records, ID cards for terminated House employees remained active for up to three weeks after the employee's departure date. House ID Services had no mechanism for receiving notification from Personnel or individual offices regarding the termination and departure of House employees (see Recommendations under Finding A). In five of the ten records, we found that information related to replacement IDs or original ID transactions did not reconcile to the history log for the badge numbers. As a result, inaccurate data for these employees was maintained in the House ID System. The remaining two exceptions we noted were data entry errors in the lost ID database.

The importance of data integrity has been addressed through the establishment of standards to control the factors affecting integrity and reliability of data. OMB's *Model Framework for*

Management Control Over Automated Information Systems establishes control requirements for application systems. These include:

- Transactions are valid--the information system must process only data that represent legitimate events.

- Information is complete--all valid data, and only those data, are to be processed by the information system.

- Information is accurate--data must be free from error during all phases of processing, within defined levels of tolerance.

The House ID System had no capability for maintaining historical data for badge numbers or social security numbers. Because of the few data edit checks they did have, information related to a badge number or social security number must be deleted from the system before the number can be re-entered. Since the archival capabilities of the House ID System were eliminated with the latest release of the Receptors software, the historical data related to a badge number or an individual could no longer be stored. The House ID System could not track the number of ID cards an employee was issued. House ID personnel must manually enter a card count in the new record on the House ID System to show the number of ID cards issued to an individual employee. Also, House ID Services performed no verification of the data entered into the House ID System or the lost ID database.

Duplicative procedures generated more opportunities for errors. Without proper record keeping, the reporting of lost IDs was unreliable. Accurate data relating to which employees have lost IDs and the information on replacement IDs was not readily available. Inaccurate data could result in individuals possessing more than one active ID card.

Recommendations

We recommend that the Sergeant at Arms:

1. Enforce contractual requirements with CAC to provide system documentation, including identification of the system of internal controls over data entry.

2. Request assistance from qualified HIR staff to identify additional edits that are necessary to compliment the edits provided by the contractor.

3. Submit edits developed in Recommendation 2 above, to the contractor of record if and when upgrades are permitted under user-controlled terms and conditions.

4. Implement interim compensating controls, such as supervisory review or data entry verification, to ensure that information maintained in the lost ID database is accurate. These procedures should remain in effect until such time when the need to maintain a separate lost ID database is no longer necessary.

5. Request contractually required documentation from CAC, including database tables and indices, to ensure that information necessary to generate accurate reports is available.

6. Provide adequate training in Informix to House ID System users to allow them to generate necessary reports in an efficient and accurate manner.

7. Identify all management reporting requirements for the House ID System and establish reporting formats to generate necessary reports on a scheduled basis.

8. Implement a formal system of user testing, approval, and acceptance for all proposed changes to the House ID System.

9. Withhold acceptance of changes to the Receptors software that do not correct the problem or that eliminate useful functions as part of the change.

Management Response

On January 31, 1996, the Office of the SAA fully concurred with this finding and all nine recommendations (see Appendix). According to the response, several initiatives are either underway or planned to ensure that the efficiency and usefulness of the House ID System is improved. Actions taken and planned include: (1) requiring CAC to specifically identify the system of internal controls over data entry when they deliver system documentation by June 1, 1996; (2) requesting HIR assistance in determining what additional edit checks are necessary by September 30, 1996; (3) requesting CAC to implement whatever additional edits are identified not later than September 30, 1996; (4) implementing supervisory review/data entry verification of the lost ID database on a daily basis (initiated in December 1995); (5) requiring CAC to provide system documentation pertaining to database tables, indices and other documentation necessary for accurate reports by June 1, 1996; (6) training all supervisory employees in at least the fundamentals of Informix by September 30, 1996, with at least one member trained beyond the fundamentals by December 1, 1996; (7) instructing staff to analyze their needs with regards to the types and frequencies of management reports and generate these reports on a periodic basis by September 30, 1996; (8) developing a formal system of user testing, approval, and acceptance for all proposed changes to the system and including it in the System and Operations Manual by September 30, 1996; and (9) immediately implementing a policy whereby changes to House ID software will not be accepted or installed until the impact of such changes have been found to correct the problem without deleting other useful functions.

Office of Inspector General Comments

The SAA's actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Finding E: Contingency/Disaster Recovery Planning Needs to Be Established

House ID Services and HIR did not establish a contingency/disaster recovery plan for the House ID System. Also, neither HIR nor House ID Services instituted formal tape file rotation procedures for the backup of critical House ID System data files and application software programs. As a result, House ID Services had no assurance that the House ID System would continue to operate in the event of an unanticipated disaster or business interruption. This control weakness developed as a result of House ID Services' unfamiliarity with contingency planning requirements and in part as a result of HIR's failure to consider the House ID System in its overall data center disaster recovery plan.

OMB Circular A-130, *Security of Federal Automated Information Systems*, Appendix III.3.a.[3] mandates that "Agencies shall establish policies and assign responsibilities to assure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users can continue to perform essential functions in the event their information technology support is interrupted. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the installation at which the application is processed." Also, internal control practices that are commonly accepted throughout the government and private industry require the establishment of procedures to help protect critical files, programs, and system documentation from fire or other natural disasters. These procedures should be formally documented, periodically updated and tested, and contain the detailed steps computer operations personnel should take in the event of an emergency. Although the House is not required to follow OMB direction, these requirements provide generally accepted information systems guidance that is appropriate for any well-controlled computer facility. House ID personnel did not develop a contingency/disaster recovery plan for the House ID System nor is it included in a more comprehensive plan developed by the HIR data center--where the system's UNIX hosts are physically located.

Contingency/disaster recovery planning is inadequate

House ID personnel we interviewed knew that their HIR contact was making backup tapes but they were not aware of the additional requirements that constitute a complete, well-thought out contingency/disaster recovery plan. As a result, the concern that a natural disaster (i.e., water pipe damage, power failure, fire, or electrical storms) or other situation (i.e., bomb threat, or terrorist situation) would occur that would limit or prevent access to the House ID Services facility has never been considered. The potential that access to the facility, data files, and processing equipment may be delayed or unavailable in the event of a business interruption needs to be considered. Without a well-designed and thoroughly tested contingency/disaster recovery plan in place, House ID Services and HIR will be ill-prepared to minimize a system interruption in the event of a disaster. Failure to recover in a timely manner would significantly affect the processing of House ID cards and access to system-controlled areas.

Limited backup and recovery procedures that are in place are inadequate

House ID Services established no formal tape file rotation procedures for the backup of critical data files and programs. Currently, daily application data and weekly application image tape backups are performed. The on-site tapes are maintained, unsecured, in the HIR application programmer's office. None of the tapes, however, are maintained off-site, a standard practice in any disaster recovery plan. In addition, a backup person has not been assigned to ensure that what data backups are done are performed routinely and without interruption if the application programmer is not available to generate the backups. Furthermore, a full volume system and application software backup that would protect the House ID System from significant data loss had never been performed.

Without a comprehensive contingency/disaster recovery plan and adequate policies and procedures that address basic issues such as tape rotation, maintenance of on-site and off-site tapes, the performance of full volume backups, agreements for off-site processing, and identification of backup personnel, the probability of a full or even partial recovery of the House ID System in the event of a disaster is questionable at best.

Recommendations

We recommend that the Sergeant at Arms:

1. Establish a contingency/disaster recovery plan for the House ID System and assign responsibilities to appropriate individuals.

2. Develop House ID System contingency/disaster recovery policies and procedures; routinely test the procedures, and ensure they are adequately maintained using the plan established in Recommendation 1 above.

3. Schedule House ID personnel for training in an appropriate contingency/disaster recovery training program.

4. Develop detailed on-site and off-site tape rotation/storage and handling procedures for the system backup tapes.

5. Designate an individual to assist and/or take over the duties of backing up the system, including the UNIX computers, in the absence of the primary backup personnel.

Management Response

On January 31, 1996, the Office of the SAA fully concurred with this finding and all five recommendations (see Appendix). According to the response, several initiatives are either underway or planned to ensure the establishment of an effective contingency/disaster recovery plan for the House ID System. The actions taken or planned include: (1) requesting assistance from HIR or seeking vendor support to develop a contingency/recovery plan for the House ID

System and assign specific responsibilities to qualified individuals by June 1, 1996; (2) requiring that all policies and procedures related to a contingency/recovery plan be included in the System and Operations Manual being developed by the SAA; (3) requiring that a separate document, containing the actual contingency/recovery plan be maintained off-site with standard backup materials, and establishing a time frame for testing such procedures to ensure they are adequate and effective by June 1, 1996; (4) scheduling all House ID personnel to receive training in contingency/disaster recovery procedures by August 1, 1996; (5) implementing detailed procedures for proper handling and rotation of backup tapes for both on-and off-site storage in the House ID System's contingency/disaster recovery plan to be developed in response to Recommendation No. 1 above, which will be accomplished by June 1, 1996; and (6) requiring the system administrator to establish backup personnel to assist and/or take over the duties of backing up the system, including the UNIX computers, in the absence of the primary backup personnel.

Office of Inspector General Comments

The SAA's actions are responsive to the issues we identified and, when fully implemented, should satisfy the intent of our recommendations.

Wilson Livingood
Sergeant at Arms

Office of the Sergeant at Arms
U.S. House of Representatives
Washington, DC 20515–6634

MEMORANDUM

TO: John W. Lainhart
Inspector General

FROM: Wilson Livingood
Sergeant at Arms

SUBJECT: Office of Identification Services Audit Report Response

DATE: January 31, 1996

Having reviewed your memorandum of December 29, 1995 entitled *Poor Planning, Questionable Contracting, and Numerous Internal Control Deficiencies Undermine Integrity and Usefulness of House Identification System*, the following comments represent my official response to your findings and recommendations. On the whole, I agree with your findings and conclusions and concur with your recommendations in general.

Finding A: Planning and Contract Management Weaknesses Contributed to an Ineffective House ID System - With regard to your recommendations of Finding A on page 10 of the report, I would like to address each individually:

1. I agreed with the recommendation by the OIG, and in December 1995 suspended two outstanding purchase requests for House ID computer equipment. No further upgrades or modifications to the system will be considered until after a system reevaluation is completed.
2. We will meet with CAC representatives on February 8, 1996 to discuss what they can do to correct the weaknesses/problems identified in this report. If CAC agrees to correct these problems within a reasonable time frame - no longer than 9 months - I will honor their commitment. On the other hand, if CAC can't meet these requirements, I am prepared to cancel the contract and look to another vendor who can. I have discussed this issue with the Office of Procurement, and they indicated they can provide me with a list of suitable vendors.
3. The Capitol Complex Security Survey, performed by a joint effort of the U.S. Secret Service, the U.S. Capitol Police, and Sergeant at Arms staff over several months during 1995, will assist my office in assessing the overall security needs of the system. The report for this survey should be completed by April 1, 1996. A complete House ID system needs assessment, which will compliment the security survey, was completed on January 20, 1996 by the National Security Agency.

4. Regarding the policies and procedures developed by the House Procurement Office, as of October 1, 1995 all departments under the jurisdiction of the Sergeant at Arms have been complying with these policies and procedures pertaining to future procurements.
5. All departments under the jurisdiction of the Sergeant at Arms will comply with System Development Lifecycle (SDLC) policies and procedures currently under development by House Information Resources. In the interim, we will comply with the National Institute of Standards and Technology's SDLC guidelines.

Finding B: Data Reliability and System Capacity Issues Contribute to System Inefficiencies We find the initial recommendation. on page 15 of the report, suggesting a House-wide pre-exit clearance for all paid and non-paid House employees desirable and necessary from a security standpoint. This office has advocated this pre-exit policy and return of identification badges for some time. As required by the House Oversight Committee, we will request on February 21, 1996 that the Chief Administrative Officer (CAO) develop such a proposal for presentation to the Committee.

In response to Finding A. I indicated that I will meet with CAC in February 1996 to discuss the problems identified in this report. In that meeting, I will require a commitment from CAC to satisfy recommendations 1 through 5 as follows within the next 9 months:

1. Correcting the Host to Host mirroring problem.
2. Correcting the software deficiency that is preventing photo images from being deleted at the same time a record is deleted. The current process will allow an operator to delete both a record and its associated image. but it requires a two-step process.
3. Eliminating users' ability to access the Host-2 fileserver except on an emergency basis -- said emergency conditions to be defined and approved by the system administrator.
4. Requiring compliance with the image compression ratio at the 30:1 rate proposed in CAC's response to the RFP.
5. Eliminating all non-essential data elements and screen modules that may be contributing to the system capacity problem.
6. I will request, from HIR and/or the Office of Procurement, assistance in identifying a qualified individual or vendor to perform a capacity analysis to determine the capacity requirements of the system. said analysis to be completed by July 1, 1996.
7. As of October 1, 1995 all purchases made by the Sergeant at Arms' Office have complied, and will continue to comply, with the Office of Procurement policies and procedures. This will include the purchase of replacement hard drives for this system, if the capacity analysis determines the need.
8. As of May 1, 1996 all "generic" ID cards issued by the House ID System will be recalled, destroyed, and replaced with cards assigned to specific individuals as appropriate. Furthermore, the SAA's System and Operations Manual now being developed will include a policy prohibiting the issuance of "generic" ID cards.

Finding C: Improvements are Needed in Controls and Security for the House ID System - As mentioned in my response to Finding A, I authorized the National Security Agency to perform a computer security study which was completed on January 20, 1996. This agency reviewed and examined the ID system and has agreed to assist my office with ensuring a secure system.

With regard to the recommendations requiring the assistance of HIR:

1. I will request HIR assign a UNIX system administrator to the House ID System before April 1, 1996 to monitor system security and all audit logs produced by the system, and to operate any test environments for evaluating software changes.
2. On December 11. 1995. I requested that (a) HIR remove all UNIX system passwords from the Computer Operations Guide, (b) future versions of the guide not include passwords, and (c) all passwords that have been published are changed immediately.
3. I will request that HIR investigate and implement dial-back access for all remote access to the system to ensure system security. I will request that this be completed by July 1, 1996.
4. The computer operation functions and application programmer functions, presently conducted by a single individual at HIR, will be transferred during the first week of February to the Operations Division in the Computer Center at HIR to ensure proper procedures are followed.
5. I will request HIR assign a database administrator to the House ID System with experience in UNIX, Informix, and relational databases. If a single individual cannot be found with these qualifications, I will request that training be provided to any partially qualified individual to bring him/her up to a working knowledge level. I will request an action date of June 1, 1996 for this to be completed.

With regard to the recommendations to the Sergeant at Arms:

1. By June 1, 1996, security controls will be established to limit access to Informix Viewpoint and Informix DBA to only authorized users using a PC power-up password. This control will serve as an interim security measure until CAC establishes adequate access control with logon ids or passwords, such as a password control capability through Windows, for Informix DBA and Informix Viewpoint.
2. The Informix DBA module will be moved as of September 1, 1996 to an area accessible only to the database administrator with the technical expertise to adequately perform database administration functions available through the Informix DBA.
3. As of July 1, 1996, security controls will be established to prohibit unauthorized access to the system and its database files and tables from outside the applications software, such as accessing files and tables through Informix Viewpoint, Informix DBA, DOS, or File Manager.
4. As of April 1, 1996, system administrator access will be limited to only the system administrator, who is not a user of the House ID system. Access to the system by the vendor will be granted by the system administrator on an as-needed basis.
5. Security Administration procedures, which include policies regarding password and access controls, will be included in the SAA's System and Operations Manual that will be completed by September 30, 1996.

6. The House ID system security administrator (an HIR employee) access to the House ID system was modified on December 11, 1995 to permit "read-only" access to the system to monitor alarms.
7. A qualified system administrator, Jim Kaelin of my staff, will be assigned by March 1, 1996 with duties that include establishing procedures for access control to be included in the SAA's System and Operations Manual referenced in No. 5 above.
8. The assigned system administrator will establish a structured methodology to review access level capabilities by module for each category of system user to be included as part of the SAA's System and Operations Manual. This task will be completed by September 30, 1996.

I will request that the CAO transfer the HIR House ID system workstation equipment in the Ford House Office Building to House Identification Services. I will take this action no later than April 1, 1996.

Finding D: Efficiency and Usefulness of the House ID System Can be Improved - Regarding your recommendations listed on page 32, the following actions will be taken:

1. I will require CAC to specifically identify the system of internal controls over data entry when they deliver all contractually required system documentation to my office before June 1, 1996.
2. I will request HIR assistance in determining what changes to the software are necessary, in the form of additional edits checks, to ensure a more reliable and accurate system. This will be done by September 30, 1996.
3. I will request CAC to implement whatever additional edits are identified as soon as possible but no later than September 30, 1996.
4. As of December 11, 1995, supervisory review/data entry verification of the lost ID database was being performed by a minimum of two people on a daily basis.
5. I will require CAC to provide system documentation pertaining to database tables and indices and whatever other documentation is required to insure that information necessary to generate accurate reports is available. This will be done by June 1, 1996.
6. It is my belief that adequate training of all employees is necessary to ensure a productive workplace. Supervisory employees of the House ID office will receive at least a basic course in the fundamentals of Informix by September 30, 1996, with a goal of having at least one member trained beyond the fundamentals by December 1, 1996.
7. I have instructed my staff to analyze their needs with regards to the types and frequencies of management reports needed from the House ID System. Included as part of the training to be delivered in my response to Recommendation No. 6 above will be the capability to query the system for those reports on a periodic basis or whenever they are needed. I expect to be able to satisfy this recommendation by September 30, 1996.
8. A formal system of user testing, approval, and acceptance for all proposed changes to the system will be developed by September 30, 1996 and included in the System and Operations Manual for the House ID Office.

9. As part of the acceptance process being developed in response to No. 8 above, it will be our policy not accept any changes to House ID software nor allow installation of upgrades or new releases without a thorough briefing as to the impact such changes--both negative or positive--will have on the system. If changes to the vendor's software are not found to correct the problem, or if they delete other useful functions, they will not be accepted. This policy will take effect immediately.

Finding E: Contingency/Disaster Recovery Planning Needs to be Established - I fully concur with your report recommendations regarding contingency/disaster recovery planning and I will include such a plan in the System and Operations Manual to ensure that accurate and complete recovery of data is possible. With respect to your specific recommendations:

1. I will request assistance from HIR or seek vendor support to develop a contingency/recovery plan for the House ID System and assign specific responsibilities to qualified individuals. This task will be completed no later than June 1, 1996.
2. I will require all policies and procedures related to a contingency/recovery plan be included in the System and Operations Manual being developed by my office. I will also require a separate document, containing the actual contingency/recovery plan be maintained off-site with standard backup materials, and establish a time frame for testing such procedures to ensure they are adequate and effective. This will be completed by June 1, 1996.
3. All House ID personnel will be scheduled and receive training in contingency/disaster recovery procedures by August 1, 1996.
4. Included in the House ID System's contingency/disaster recovery plan to be developed in response to Recommendation No. 1 above, will be detailed procedures for proper handling and rotation of backup tapes for both on- and off-site storage. This will be accomplished by June 1, 1996.
5. I will require the system administrator to establish backup personnel to assist and/or take over the duties of backing up the system, including the UNIX computers, in the absence of the primary backup personnel. This backup contingency will be established in February 1996 with assumption of the backup responsibilities by HIR.