United States General Accounting Office

GAO

Report to the Majority and Minority Leaders, U.S. Senate

December 1995

FINANCIAL MANAGEMENT

General Computer Controls at the Senate Computer Center

GAO/AIMD-96-15

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-266231

December 22, 1995

The Honorable Bob Dole
Majority Leader
United States Senate

The Honorable Thomas A. Daschle
Minority Leader
United States Senate

As you requested, we audited the statements of disbursements, receipts, and financing sources for the Office of the Secretary of the Senate and the Office of the Sergeant at Arms and Doorkeeper for fiscal year 1994 and reported thereon.[1] As part of our audit work, we evaluated and tested the general computer controls over the financial systems maintained and operated by the Senate Computer Center (SCC) that processed financial information for the two offices.

General computer controls affect the overall security and effectiveness of computer systems and operations as opposed to being unique to any specific computer program, office, or operation. They include an entity's organizational structure, operating procedures, software security features, and physical protection. Such controls are designed to ensure that (1) access to sensitive data is restricted to prevent unauthorized changes and disclosure, (2) only approved changes are made to computer programs, (3) computer staff duties are properly segregated to reduce the risk of undetected errors or fraud, and (4) back-up and recovery plans are adequate to continue essential operations in the event of an emergency.

We identified general computer control weaknesses which, although mitigated by compensating controls for the financial statements we audited, could affect the security and reliability of computer operations for other Senate offices. Accordingly, we are reporting separately on the results of our computer control testing. This report summarizes our findings, which we discussed in detail with SCC management. Also, we identified weaknesses in controls over external access to Senate computer resources, which we are reporting in a separate letter with limited distribution due to its sensitive nature.

[1] Financial Audit: Office of the Secretary of the Senate for the Fiscal Year Ended September 30, 1994 (GAO/AIMD-95-185, July 12, 1995) and Financial Audit: Office of the Sergeant at Arms and Doorkeeper of the Senate for the Fiscal Year Ended September 30, 1994 (GAO/AIMD-95-186, July 12, 1995).

Results in Brief

SCC's general computer controls did not adequately protect sensitive data files and computer programs, such as those related to payroll and personnel, from unauthorized disclosure and modification. Specifically, we found weaknesses in SCC's ability to (1) restrict access to sensitive data, programs, and other computer resources, (2) monitor the activity of users and programmers, (3) control changes to software, (4) segregate data processing duties, and (5) provide for continued processing in the event of emergencies or service interruption.

In addition, the Senate did not have a comprehensive strategic plan for securing Senate computer resources that included SCC, the Office of Telecommunications, and system users. The lack of such a strategic plan contributed to the weaknesses we found and could lead to significantly greater security exposures as the Senate moves from a centralized mainframe processing environment to a decentralized network environment distributed throughout the Senate.

The effect of the general computer control weaknesses on the statements of disbursements, receipts, and financing sources for the two Senate offices we audited was mitigated by certain management controls. For example, the Senate Disbursing Office, a part of the Office of the Secretary, performs various control procedures to ensure that data are properly authorized and entered into the system, including comparison of system reports with supporting documents. Also, both offices review monthly disbursement reports and reconcile certain disbursement information to their own independent records.

Background

The overall effectiveness of the Senate's computer controls is dependent on the controls implemented by (1) SCC, which operates the Senate mainframe computer, (2) system users, which include all Member offices and Senate Committees, and (3) the Office of Telecommunications, which maintains telecommunication equipment and networks that link system users to the SCC mainframe and to other users.

In addition to processing financial systems, such as payroll and other disbursements, the SCC mainframe processes other important and confidential information, such as Senate personnel files, LEGIS—a text retrieval system for bills and other legislative information, and Capitol Police and other administrative files.

System users operate about 260 local area networks (LANs) in the Washington, D.C., area and across the country that communicate with the mainframe and perform data processing functions for users. Overall, there are approximately 580 user accounts that allow access to one or more programs run by SCC.

Objective, Scope, and Methodology

Our objective was to evaluate and test the general computer controls over the financial systems maintained and operated by the Senate Computer Center (SCC) that processed financial information for the Office of the Secretary of the Senate and the Office of the Sergeant at Arms and Doorkeeper. General computer controls, however, also affect the security and reliability of financial and nonfinancial operations processed by SCC for other Senate offices.

Specifically, we evaluated controls intended to

- protect data, files, and programs from unauthorized access;
- prevent unauthorized changes to systems and applications software;
- provide segregation of duties among applications and systems programmers, computer operators, security administrators, and other data center personnel;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure adequate computer security administration.

To evaluate these controls, we identified and reviewed SCC's information system general control policies and procedures. Through this review and discussions with SCC staff, including programming, operations, and security personnel, we determined how the general controls should work and the extent to which data center personnel considered them to be in place. We also reviewed the installation and implementation of SCC's systems and security software.

Further, we tested and observed the operation of general controls over SCC information systems to determine whether they were in place, adequately designed, and operating effectively. Our tests included attempts to obtain access to sensitive data and programs, which were performed with the knowledge and cooperation of SCC officials.

To assist in our evaluation and testing of general controls, we contracted with the public accounting firm of Deloitte & Touche LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported.

We performed our work at the Senate Computer Center in Washington, D.C., from April 1995 through July 1995 in accordance with generally accepted government auditing standards.

During the course of our work, we met with SCC officials to discuss our work and they informed us of the steps they planned to take or had taken to address our findings. At the conclusion of our work, we provided a draft of this report to Senate officials who said that they concurred with our findings, conclusions, and recommendations.

Access to Computer Resources Not Adequately Controlled

Two basic internal control objectives for any information system are to protect data from unauthorized changes and to prevent unauthorized disclosures of sensitive data. Without effective access controls, the reliability of a computer system's data cannot be maintained, sensitive data can be accessed and changed, and information can be inappropriately disclosed.

SCC had computer security weaknesses that could result in unauthorized access to the system's data, files, and programs. These weaknesses included ineffective (1) implementation of SCC's access control software and (2) practices to authorize, monitor, and review user access. During the course of our work, SCC officials advised of actions they had taken or planned to take to address some of the weaknesses we identified.

Ineffective Implementation of Access Control Software

SCC has implemented CA-ACF2, a commercially available access control software package, to control its primary financial management system and certain batch processing.[2] However, ACF2 was not implemented to control access to other mainframe programs, including parts of the payroll system, LEGIS, the Capitol Police system, and other administrative systems. While many programs have built-in security features, such features typically are not as comprehensive or stringent as those provided by ACF2. Common deficiencies in such programs include a lack of audit trails for user activity

[2] In computer operations, batch processing is the processing of a group of related transactions or other items at periodic intervals.

and few, if any, password management controls (for example, forced password changes and minimum character length passwords).

By not implementing ACF2 over all its systems and programs, SCC has forfeited many of the control benefits provided by the software, and must maintain expertise in the security administration for each of these systems and programs. For example, at least one system not under ACF2 requires the use of a single shared password for access. Since all users share the same password, the system cannot provide an audit trail of a particular user's activity, thereby limiting user accountability.

SCC officials advised us that they did not plan to implement ACF2 over other mainframe applications due to (1) indications that, for some programs, less rigorous security measures are preferred by user management to provide easier accessibility, (2) resource constraints, and (3) intentions to transition from the mainframe to a decentralized network environment. However, as the transition may not be completed for up to 5 years, we believe that it is important for SCC management to assess its ongoing risks of not implementing ACF2 completely and take appropriate actions.

In addition, the implementation of ACF2 over the financial management system and batch processing is not fully effective. The technical options that SCC has implemented to control access to the information on its mainframe negate many of the control benefits that the software offers. For example, ACF2 was implemented to allow up to 20 security violations, such as attempts to access data for which the user is not authorized, to occur in a single job or session before it is canceled. Similarly, a user was permitted up to 500 invalid password attempts daily before ACF2 denied access. By allowing such a high number of violations and invalid password attempts to occur, SCC increased the risk of unauthorized access and improper use or disclosure of sensitive Senate data. SCC officials advised us that they have begun changes to these ACF2 control settings, such as reducing the limits on the number of security violations and invalid password attempts.

Other password controls were weakened due to ineffective ACF2 implementation. While a user's identification (ID) typically follows a standard format that makes it easily deduced, passwords are used to authenticate the user and thus should be difficult to deduce, kept secret, and frequently changed. Most SCC users were only required to change their passwords every 180 days; some users were not required to change their passwords at all. In addition, SCC had not implemented a shorter password expiration period for users having special system or security privileges.

Moreover, SCC's current security policies did not prevent users from reusing the same password indefinitely. The longer a user is allowed to use the same password, the greater the risk that an unauthorized user may discover and use another user's ID/password combination. SCC management advised us that it was reviewing password policies and had reduced the password change requirement to 90 days for some users and to 30 days for some special privileges and was investigating ways to restrict others.

Improved Controls Needed Over Authorization, Monitoring, and Review of User Access

Organizations can reduce the risk that unauthorized changes or disclosures occur by (1) granting employees authority to read or modify only those programs and data that are necessary to perform their duties and (2) periodically reviewing this authority and modifying it to reflect changes in job responsibilities and terminations in employment.

Having unused or unneeded user accounts increases the risk that an unauthorized user will discover and use such an account without prompt detection. In a sample of 38 SCC accounts, we found 3 assigned to individuals who had separated from Senate employment from 5 to 15 months earlier. We also found that 159, or over one quarter of the accounts, had not been used in more than 6 months. We noted that another 79 had never been used, of which 64 had existed for more than 120 days. Because initial passwords[3] may be easily guessed, these inactive accounts present an increased risk that passwords will be compromised and unauthorized access allowed.

We also identified 30 user IDs and passwords that were shared by staff in certain departments, even though these staff members have individual accounts. The use of shared IDs and passwords undermines the effectiveness of monitoring because individual accountability is lost and increases the risk of password compromise.

In addition, SCC's implementation of ACF2 allowed for unnecessary access to sensitive data and programs. Both operations and programming personnel in SCC's Central Services Division had a level of access that was not necessary for performance of their regular job duties and could

[3] The initial password for a new user is assigned by the security administrator and must by changed the first time the user logs on.

increase the risk of unauthorized disclosure or modification of sensitive data. For example, 11 applications programmers had the ability to change on-line payroll data, 11 could alter vendor information, and 2 could change financial data. Moreover, this level of access could not be monitored because no record, or log, of the access was created.

We identified another area in which SCC could improve its access monitoring controls. Specifically, SCC did not implement session timeouts, which automatically log off a user's terminal after a specified period of inactivity, over all of its programs. Lack of session timeouts increases the risk of unauthorized access to unattended terminals.

SCC management was reviewing its access authorization and monitoring procedures at the time of our review and had taken or planned to take several corrective actions. Specifically, SCC management indicated that the security administrator had begun to log and monitor user access to determine what programs and files are being used. This information will be used as a basis for removing access privileges where they are not used or needed. However, where unrestricted access is deemed necessary, management plans to log and monitor it. Also, SCC management advised us that inactive user IDs were being removed from the system. Finally, SCC management was reviewing shared user IDs and passwords and planned to reduce or eliminate them.

Other General Controls Not Effective

In addition to access controls, a computer system typically has other important general controls to ensure the integrity and reliability of data. These general controls include policies, procedures, and control techniques to (1) prevent unauthorized changes to system software, (2) provide appropriate segregation of duties among computer personnel, and (3) ensure continuation of computer processing operations in case of an unexpected interruption. SCC had weaknesses in the general controls over each of these areas, although its management had made or planned to make improvements in several areas.

Strengthened Controls Needed Over Software Changes and Maintenance

The integrity of an information system depends upon management's clear understanding and documentation of the system. Formal processes for developing and maintaining software are important tools to assist management in ensuring that all changes to software meet user specifications, are appropriately reviewed and authorized, and include adequate security measures.

SCC did not have a formal change control process to document management's authorization and approval of routine and emergency changes to systems software. Change control procedures for the major financial programs have not been formalized to ensure that only authorized changes are made to programs and data. Inadequate management of system software changes and maintenance, including the lack of documentation, also increased the risk that back-up and recovery procedures could not be effectively performed.

Also, we found instances of (1) the unintended creation of access paths to computer resources and (2) situations in which SCC staff were unsure of the purpose of undocumented systems software functions. Both of these weaknesses increased the risk of security or reliability breaches. For example, the operating system contained the names of five programs that no longer existed, introducing the risk that an unauthorized program could be run under one of those program names to gain unauthorized access to programs and data files.

SCC officials were reviewing software change and maintenance procedures and planned to formalize them. Also, SCC management advised us that unused program names have been eliminated.

Inadequate Segregation of Computer Duties

One fundamental technique for safeguarding programs and data is the appropriate segregation of duties and responsibilities of computer personnel to reduce the risk that errors or fraud will go undetected. At SCC, we found inadequate segregation of duties, particularly in the granting of powerful security privileges.

SCC has explicitly assigned two systems programmers to assist in the security administration of the access control software. Under normal circumstances, back-up security staff should report to the security administrator and have no programming, operations, or librarian duties. Because these individuals have both systems and security administrator privileges associated with their user accounts, they can eliminate any audit trail of their activity in the system. SCC officials indicated that they were reviewing this issue and considering several steps to mitigate the risks of assigning dual responsibilities.

In addition, SCC has assigned powerful ACF2 security functions to many user accounts for which these privileges represent a significant security exposure. For example, 49 accounts could bypass all ACF2 controls (including the creation of audit trails, known as logging), allowing the user full and virtually undetectable access to all files, programs, and other system resources. This level of authority should generally be limited to emergency IDs, which are activated with management approval on a temporary, as-needed basis to handle problems or emergencies. SCC officials advised us that they are assessing the granting of full access to such a large number of individuals and have begun to reduce or eliminate such access. In the interim, to mitigate the risks associated with unlogged access to sensitive files, they have changed their procedures to ensure that all updates to order entry and payroll files are logged.

Further, controls over security administration could be improved if the data security administrator reported directly to the SCC Director to provide adequate authority and independence in security matters. Currently, the data security administrator reports to the assistant director of the Educational Services and Support Division. The data security administrator, therefore, had customer service responsibilities, which may not be compatible with the duties associated with systems security. SCC management was considering the role and organizational placement of the data security administrator at the conclusion of our work.

Disaster Recovery and Contingency Planning Needed

An agency must ensure that it is adequately prepared to cope with a loss of operational capability due to an earthquake, fire, accident, sabotage, or any other operational disruption. A detailed, current, and tested disaster recovery plan is essential to ensure that the SCC information system can promptly restore operations and data, such as payroll processing and records, in the event of a disaster.

Prior to its move to its current location in 1992, SCC had an arrangement with the Library of Congress to provide back-up operations on its mainframe in the event of an emergency. However, the two mainframes are no longer compatible, so the Library of Congress back-up site cannot be used. SCC has developed a back-up capability on its mainframe in the event a portion of the machine goes down. However, in the event that the entire SCC was incapacitated, back-up processing would not be readily available.

SCC has advised us that the Sergeant at Arms has since contracted with a commercial vendor to provide off-site back-up processing facilities in the event of an emergency. Further, SCC management has advised us that it has begun to develop a disaster recovery plan. Once developed, it will be important that SCC implement and periodically test the plan at the back-up facility, identifying the objectives and expected results for use in evaluating test results.

Comprehensive Strategic Computer Security Plan Needed

The Senate's lack of a comprehensive strategic plan for computer security administration contributed to the general control weaknesses in SCC operations. Such a plan would consider all Senate computer resources, and include SCC, the Office of Telecommunications, and users in a comprehensive policy for security awareness and administration.

Development and implementation of a comprehensive strategic plan will become more important as SCC and its customers continue moving from an environment in which all major applications are processed on a mainframe to a decentralized network environment distributed throughout the Senate. In a distributed processing environment, an integrated security plan is crucial for coordinating control over multiple locations, numerous hardware and software installations, and numerous paths of communication. For example, given the large number of possible access sites throughout the Senate, external access is a significant area of exposure and should be considered in any overall security plan. Without a comprehensive strategy, duplication of some controls and omission of others are likely to occur, adversely affecting both efficiency and effectiveness.

Weaknesses Did Not Affect Financial Statements of Receipts and Disbursements

As part of our audits of receipts and disbursements, we evaluated assertions made by the Secretary of the Senate and the Sergeant at Arms and Doorkeeper that internal controls in place on September 30, 1994, were effective in safeguarding assets from material loss, assuring material compliance with relevant laws and regulations, and assuring that there were no material misstatements in the financial statements.[4] We considered the effect of general computer control weaknesses and determined that other management controls mitigated their effect on the statements of disbursements, receipts, and financing sources for the two audited entities.

Both of these offices use SCC resources to process financial information that is essential to their operations. The Senate Disbursing Office, a part of the Office of the Secretary, uses SCC to process payroll and personnel

[4] See GAO/AIMD-95-185 and GAO/AIMD-95-186 for a detailed discussion of our testing of receipts and disbursements.

information and to maintain vendor information. The Senate Disbursing Office maintains its own accounting system, which is used to process other disbursements and report all Senate financial transactions. The Sergeant at Arms and Doorkeeper uses SCC to process its accounting and equipment inventory systems.

The Senate Disbursing Office performs various control procedures to ensure that data are properly authorized and entered into the system, including comparison of system reports with supporting documents at various stages of processing. Also, the Senate Disbursing Office distributes monthly reports to the Secretary of the Senate and the Sergeant at Arms and Doorkeeper that list payroll and other disbursements made on their behalf. The offices then review the monthly reports for accuracy. Both the Secretary of the Senate and the Sergeant at Arms and Doorkeeper reconcile the nonpayroll information to their own independent records to ensure that disbursements are consistent with the approved requests for payment that they submitted. Any differences discovered by reviews or reconciliations are discussed with the Senate Disbursing Office and resolved. Finally, the Secretary of the Senate publishes a semiannual public report that summarizes payroll information by employee and details the individual disbursements of the entire Senate.

Conclusions

The Senate's general computer control weaknesses could result in serious breaches in the security of its sensitive data and programs, such as those related to payroll and personnel. A comprehensive strategic plan that integrates and controls access and processing for all Senate files, programs, and data is crucial to ensuring that Senate computer resources are adequately safeguarded. As the Senate moves to a distributed processing environment, development and implementation of a comprehensive computer security plan will become even more important.

Recommendations

To correct the existing weaknesses at the Senate Computer Center, we recommend that you direct the Sergeant at Arms and Doorkeeper to take the following actions.

- Develop and implement policies and procedures to limit access for the system's users to only those computer programs and data needed to perform their duties. Access controls should be improved by (1) effectively utilizing SCC's access control software, including assessing ongoing risks of incomplete implementation and taking appropriate control measures, (2) strengthening procedures to authorize, monitor, and review user access, and (3) implementing session timeout procedures.

- Develop and implement policies and procedures for controlling software changes, including requiring documentation for the purpose of the change, management review and approval, and independent testing.
- Provide for appropriate segregation of computer duties, including upgrading the position of data security administrator to allow for appropriate independence and authority.
- Develop, implement, and test a disaster recovery plan for all critical SCC operations.

In addition, to improve Senatewide computer security, we recommend that you direct that the Senate develop and implement a comprehensive strategic plan that integrates and controls access and processing for all Senate files, programs, and data.

We are sending copies of this report to the Sergeant at Arms and Doorkeeper of the U.S. Senate and to the Secretary of the Senate. Copies will be made available to others upon request.

Please contact me at (202) 512-9489 if you or your staffs have any questions. Major contributors to this report are listed in appendix I.

David L Clark

David L. Clark
Director, Audit Oversight
and Liaison

Major Contributors to This Report

Accounting and Information Management Division

Shannon Cross
Robert Dacey
Francine Delvecchio
Sharon Kittrell
Crawford Thompson

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001