

GAO

Report to the Chairman, Securities and  
Exchange Commission

March 2005

INFORMATION  
SECURITY

Securities and  
Exchange  
Commission Needs to  
Address Weak  
Controls over  
Financial and  
Sensitive Data



G A O

Accountability \* Integrity \* Reliability



Highlights of [GAO-05-262](#), a report to the Chairman, Securities and Exchange Commission

## Why GAO Did This Study

The Securities and Exchange Commission (SEC) relies extensively on computerized systems to support its financial and mission-related operations. As part of the audit of SEC's fiscal year 2004 financial statements, GAO assessed the effectiveness of the commission's information system controls in protecting the integrity, confidentiality, and availability of its financial and sensitive information.

## What GAO Recommends

GAO recommends that the SEC Chairman direct the Chief Information Officer to take several actions to fully develop and implement an effective agency-wide information security program. In commenting on a draft of this report, SEC agreed with our recommendations. SEC plans to address the identified weaknesses and indicated that significant progress is already being made to address them.

[www.gao.gov/cgi-bin/getrpt?GAO-05-262](http://www.gao.gov/cgi-bin/getrpt?GAO-05-262).

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-3317 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov).

## INFORMATION SECURITY

# Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data

## What GAO Found

SEC has not effectively implemented information system controls to protect the integrity, confidentiality, and availability of its financial and sensitive data. Specifically, the commission had not consistently implemented effective electronic access controls, including user accounts and passwords, access rights and permissions, network security, or audit and monitoring of security-relevant events to prevent, limit, and detect access to its critical financial and sensitive systems. In addition, weaknesses in other information system controls, including physical security, segregation of computer functions, application change controls, and service continuity, further increase risk to SEC's information systems. As a result, sensitive data—including payroll and financial transactions, personnel data, regulatory, and other mission critical information—were at increased risk of unauthorized disclosure, modification, or loss, possibly without detection.

A key reason for SEC's information system control weaknesses is that the commission has not fully developed and implemented a comprehensive agency information security program to provide reasonable assurance that effective controls are established and maintained and that information security receives sufficient management attention. Although SEC has taken some actions to improve security management, including establishing a central security management function and appointing a senior information security officer to manage the program, it had not clearly defined roles and responsibilities for security personnel. In addition SEC had not fully (1) assessed its risks, (2) established or implemented security policies, (3) promoted security awareness, and (4) tested and evaluated the effectiveness of its information system controls. As a result, SEC did not have a solid foundation for resolving existing information system control weaknesses and continuously managing information security risks.

---

# Contents

---

---

## Letter

Results in Brief	1
Background	2
Objective, Scope, and Methodology	4
SEC Information System Controls Were Not Effective	5
Comprehensive Information Security Program Is Not Fully Implemented	13
Conclusions	20
Recommendations for Executive Action	21
Agency Comments	21

---

## Appendixes

<b>Appendix I: Comments from the Securities and Exchange Commission</b>	23
<b>Appendix II: GAO Contact and Staff Acknowledgments</b>	25
GAO Contact	25
Staff Acknowledgments	25

---

### Abbreviations

CIO	Chief Information Officer
FISMA	Federal Information Security Management Act
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SEC	Securities and Exchange Commission

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, D.C. 20548

March 23, 2005

The Honorable William H. Donaldson  
Chairman, Securities and Exchange Commission

Dear Mr. Chairman:

As part of our fiscal year 2004 audit of the financial statements of the Securities and Exchange Commission (SEC), we assessed the effectiveness of the commission's information system general controls.<sup>1</sup> Effective information system controls are essential to ensuring that financial information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. These controls also affect the integrity, confidentiality, and availability of nonfinancial information maintained by SEC, such as personnel and regulatory information.

This report summarizes weaknesses in information system controls in SEC's computer systems. We are also issuing a report for "Limited Official Use Only," which describes in more detail the information security weaknesses identified, our specific recommendations for correcting them, and SEC's plan for implementing corrective actions.

We performed our review at SEC headquarters in Washington, D.C., and at its computer facility in Alexandria, Virginia, from April 2004 through November 2004. Our review was performed in accordance with generally accepted government auditing standards.

---

## Results in Brief

SEC did not effectively implement information system controls to protect the integrity, confidentiality, and availability of its financial and sensitive information. Specifically, the commission had not consistently implemented effective electronic access controls, including user accounts and passwords, access rights and permissions, network security, or audit

---

<sup>1</sup>Information system general controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. These controls include security management, operating procedures, software security features, and physical protection designed to ensure that access to data is appropriately restricted, computer security functions are segregated, only authorized changes to computer programs are made, and backup and recovery plans are adequate to ensure the continuity of essential operations.

---

and monitoring of security-relevant events to prevent, limit, and detect access to its critical financial and sensitive systems. In addition, weaknesses in other information system controls, including physical security, segregation of computer functions, application change controls, and service continuity, further increase the risk to SEC's information systems. As a result, sensitive data—including payroll and financial transactions, personnel data, regulatory, and other mission critical information—were at increased risk of unauthorized disclosure, modification, or loss, possibly without being detected.

A key reason for SEC's information system control weaknesses is that the commission has not fully developed and implemented a comprehensive agency information security program to provide reasonable assurance that effective controls are established and maintained and that information security receives sufficient management attention. Although SEC has taken some actions to improve security management, including establishing a central security management function and appointing a senior information security officer to manage the program, it had not clearly defined roles and responsibilities for security personnel. In addition, SEC had not fully (1) assessed its risks, (2) established or implemented security policies, (3) promoted security awareness, and (4) tested and evaluated the effectiveness of its information system controls. As a result, SEC did not have a solid foundation for resolving existing information system control weaknesses and continuously managing information security risks.

To assist SEC in implementing an effective agency-wide information security program, we are making recommendations to the SEC Chairman that address these issues.

In providing written comments on a draft of this report, SEC agreed with our recommendations. SEC plans to address the identified weaknesses and indicated that significant progress is already being made to address them.

---

## Background

Following the stock market crash of 1929, Congress passed the Securities Exchange Act of 1934,<sup>2</sup> which established the SEC to enforce securities laws, to regulate the securities markets, and to protect investors. In enforcing these laws, the SEC issues rules and regulations to provide

---

<sup>2</sup>15 U.S.C. § 78d.

---

protection for investors and to help ensure that the securities markets are fair and honest. This is accomplished primarily by promoting adequate and effective disclosure of information to the investing public. The SEC also oversees and requires the registration of other key participants in the securities industry, including stock exchanges, broker-dealers, clearing agencies, depositories, transfer agents, investment companies, and public utility holding companies. The SEC is an independent, quasi-judicial agency that operates under a bipartisan commission appointed by the President and confirmed by the Senate.

SEC had a budget of about \$800 million and staff of 4,100 to monitor and regulate the securities industry in fiscal year 2004. In 2003, the volume traded on U.S. exchanges and NASDAQ exceeded \$22 trillion and 850 billion shares. Each year the commission accepts, processes, and disseminates to the public more than 600,000 documents from companies and individuals that are filed with the SEC, including annual reports from more than 12,000 reporting companies.

SEC relies extensively on computerized systems to support its financial operations and store the sensitive information it collects. Its local and wide area networks interconnect these systems. To support the commission's financial management functions, it relies on several financial systems to process and track financial transactions that include filing fees paid by corporations and penalties from enforcement activities. In fiscal year 2004, the SEC collected \$389 million for filing fees and \$948 million in penalties and disgorgements. In addition, the commission uses other systems that maintain sensitive personnel information for its employees, filing data for corporations, and legal information on enforcement activities. The commission's Chief Information Officer (CIO) is SEC's key official for information security. The CIO is responsible for establishing, implementing, and overseeing the commission's information security program.

Information system controls are a critical consideration for any organization that depends on computerized systems and networks to carry out its mission or business. Without proper safeguards, there is risk that individuals and groups with malicious intent may intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

---

We have reported information security as a governmentwide high-risk area since February 1997.<sup>3</sup> Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations at risk of disruption, fraud, and inappropriate disclosure.

Congress and the executive branch have taken actions to address the risks associated with persistent information security weaknesses. In December 2002, the Federal Information Security Management Act (FISMA), which is intended to strengthen information security, was enacted as Title III of the E-Government Act of 2002.<sup>4</sup> In addition, the administration undertook important actions to improve security, such as integrating information security into the President's Management Agenda Scorecard. Moreover, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued security guidance to agencies.

---

## Objective, Scope, and Methodology

The objective of our review was to assess the effectiveness of SEC's information system controls in protecting its financial and sensitive information. Our evaluation was based on (1) our *Federal Information System Controls Audit Manual*,<sup>5</sup> which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data and (2) our May 1998 report on security management best practices<sup>6</sup> at leading organizations, which identifies key elements of an effective information security management program.

---

<sup>3</sup>See, for example, GAO, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructure*, [GAO-03-121](#) (Washington, D.C.: January 2003).

<sup>4</sup>Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec.17, 2002).

<sup>5</sup>GAO, *Federal Information System Controls Audit Manual, Volume I – Financial Statements Audits*, [GAO/AIMD-12.19.6](#) (Washington, D.C.: January 1999).

<sup>6</sup>GAO, *Information Security Management: Learning from Leading Organizations*, [GAO/AIMD-98-68](#) (Washington, D.C.: May 1998).

---

Specifically, we evaluated SEC's information system controls intended to

- prevent, limit, and detect electronic access to computer resources (data, programs, and systems), thereby protecting these resources against unauthorized disclosure, modification, and use;
- provide physical protection of computer facilities and resources from espionage, sabotage, damage, and theft;
- ensure that work responsibilities for computer functions are segregated so that one individual does not perform or control all key aspects of a computer-related operation and, thereby, have the ability to conduct unauthorized actions or gain unauthorized access to assets or records without detection by another individual performing assigned responsibilities;
- prevent the implementation of unauthorized changes to application or system software;
- ensure the recovery of computer processing operations and data in case of disaster or other unexpected interruption; and
- ensure an adequate information security program.

To evaluate these controls, we identified and reviewed pertinent SEC computer security policies, procedures, guidance, plans, and reports. We also discussed with key security representatives, system administrators, and management officials whether information system controls were in place, adequately designed, and operating effectively. In addition, we conducted tests and observations of controls in operation.

---

## SEC Information System Controls Were Not Effective

SEC did not effectively implement information system controls to protect the integrity, confidentiality, and availability of its financial and sensitive information. Specifically, the commission did not consistently implement effective electronic access controls, including user account and passwords, access rights and permissions, network security, and audit and monitoring of security-relevant events to prevent, limit, and detect access to its critical financial and sensitive systems. In addition, weaknesses in other information system controls, including physical security, segregation of computer functions, application change controls, and service continuity, further increase the risk to SEC's information systems. As a result, sensitive



---

data—including payroll and financial transactions, personnel data, regulatory, and other mission critical information—are at increased risk of unauthorized disclosure, modification, or loss, possibly without being detected.

---

## Electronic Access Controls Were Not Consistently Implemented

A basic management control objective for any organization is the protection of its information systems and critical data from unauthorized access. Organizations accomplish this objective by designing and implementing controls to prevent, limit, and detect electronic access to computing resources. These controls include user accounts and passwords, access rights and permissions, network security, and audit and monitoring of security-related events. Inadequate electronic access controls diminish the reliability of computerized data and increase the risk of unauthorized disclosure, modification, and use of data.

SEC did not consistently implement effective electronic access controls to prevent, limit, and detect access to financial and sensitive data. Numerous vulnerabilities existed in SEC's computing environment because of the cumulative effects of information system control weaknesses in the area of user accounts and passwords, access rights and permissions, network security, and audit and monitoring of security-relevant events. For example, our testers found a workstation located in an area of an SEC building readily accessible by the general public that was logged into the SEC computer network. With access from this workstation, a potential attacker would have direct access to the SEC's internal network and could have exploited other vulnerabilities, such as easy-to-guess passwords, vulnerable servers, and insecurely configured system servers to gain access to critical systems that maintain the commission's financial and regulatory information. Also, because of weaknesses in system audit logs and the lack of a fully implemented intrusion detection system, the likelihood of detection would have been remote. Prior to the completion of our review, SEC completed actions to remediate this access vulnerability. Weaknesses in the specific control areas are summarized here.

## User Accounts and Passwords

A computer system must be able to identify and differentiate among users so that activities on the system can be linked to specific individuals. Unique user accounts assigned to specific users allow systems to distinguish one user from another, a process called identification. The system must also establish the validity of a user's claimed identity through some means of authentication, such as a password, known only to its owner. The combination of identification and authentication, such as user

---

account/password combinations, provides the basis for establishing individual accountability and controlling access to the system. Accordingly, agencies should (1) implement procedures to control the creation, use, and removal of user accounts and (2) establish password parameters, such as length, life, and composition, to strengthen the effectiveness of account/password combinations for authenticating the identity of users.

SEC did not sufficiently control user accounts and passwords to ensure that only authorized individuals were granted access to its systems and data. For example, SEC operating personnel did not consistently configure password parameters securely, and users sometimes created easy-to-guess passwords. User accounts and passwords for privileged network and database administrator accounts were inappropriately stored in clear text, increasing the likelihood of their disclosure and unauthorized use to gain access to server resources. Moreover, SEC did not remove system access from certain separated employees, including one terminated employee who still had access to SEC's information systems 8 months after termination. These practices increase the risk that individuals might gain unauthorized access to SEC resources without attribution.

## Access Rights and Permissions

A basic underlying principle for securing computer systems and data is the concept of least privilege. This means that users are granted only those access rights and permissions needed to perform their official duties. Organizations establish access rights and permissions to restrict the access of legitimate users to the specific programs and files that they need to do their work. User rights are allowable actions that can be assigned to users or groups. File and directory permissions are rules associated with a file or directory that regulate which users can access them and in what manner. Assignment of rights and permissions must be carefully considered to avoid giving users unintentional and unnecessary access to sensitive files and directories.

SEC routinely permitted excessive access to the computer systems that support its critical financial and regulatory information and to certain key files and directories. For example, on certain network systems, users and administrators had access that would allow them to bypass security settings or change security parameters and audit logs. All 4,100 network users were inadvertently granted access that would allow them to circumvent the audit controls in the commission's main financial systems. Further, on certain systems, users had access to system files and directories that would allow them to gain unauthorized access to the system, thereby enabling them to compromise key servers or disrupt

---

operations. In addition, contractor staff did not follow SEC policy for obtaining remote access and instead granted themselves access to key financial systems without SEC approval. Inappropriate access to sensitive security files, audit logs, system directories, and key financial data provides opportunities for individuals to circumvent security controls and read, modify, or delete critical or sensitive information and computer programs.

## Network Security

Networks are a series of interconnected devices and software that allow individuals to share data and computer programs. Because sensitive programs and data are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their network, in part, by installing and configuring network devices that permit authorized network service requests and deny unauthorized requests and by limiting the services that are available on the network. Network devices include (1) firewalls designed to prevent unauthorized access into the network, (2) routers that filter and forward data along the network, (3) switches that forward information among parts of a network, and (4) servers that host applications and data. Network services consist of protocols for transmitting data between network devices. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as denial-of-service attacks. Since networks often provide the entry point for access to electronic information assets, failure to secure them increases the risk of unauthorized use of sensitive data and systems.

SEC enabled vulnerable, outdated, and/or misconfigured network services and devices. For example, key network devices were not securely configured to prevent unauthorized individuals from gaining access to detailed network system policy settings and listings of users or groups. The SEC also did not consistently secure its network against well-known software vulnerabilities or minimize the operational impact of potential failure in a critical network device. Moreover, the commission did not have procedures to ensure that its external contractor or business partner network connections to the internal SEC network were securely configured. Running vulnerable network services, not restricting access to configuration files of network devices, and not monitoring the security of external network connections increase the risk of system compromise, such as unauthorized access to and manipulation of sensitive system data, disruption of services, and denial of service.

---

## Audit and Monitoring of Security-Relevant Events

Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations. Organizations accomplish this by implementing system or security software that provides an audit trail for determining the source of a transaction or attempted transaction and monitoring users' activities. How organizations configure the system or security software determines the nature and extent of audit trail information that is provided. To be effective, organizations should (1) configure the software to collect and maintain a sufficient audit trail for security-relevant events; (2) generate reports that selectively identify unauthorized, unusual, and sensitive access activity; and (3) regularly monitor and take action on these reports. Without sufficient auditing and monitoring, organizations increase the risk that they may not detect unauthorized activities or policy violations.

The risks created by the serious electronic access control weaknesses discussed earlier were heightened because SEC had not fully established a comprehensive program to monitor user access. While SEC had several initiatives under way to monitor user access activity, it did not yet have a comprehensive program to routinely review, audit, or monitor system user access activities. For example, audit logging was not consistently implemented on all network services, and there was no capability to target unusual or suspicious network events for review as they occurred. In addition, SEC had not yet fully implemented a network intrusion detection system. As a result, there is an increased risk that unauthorized access to the servers and data may not be detected in a timely manner.

In response to identified weaknesses to electronic access controls, the CIO said that the commission has taken steps to improve access rights and permissions and has initiated efforts to restrict access to critical financial data and programs and related sensitive information. Further, the CIO stated that action is being taken to secure the network against known vulnerabilities, securely configure network devices, and monitor the security of external network connections. In addition, efforts were planned and, in some cases, completed, to enhance the commission's overall program for auditing and monitoring its systems for security-relevant events.

---

---

## Other Information System Controls Were Not Sufficient

In addition to the electronic access controls discussed, other important controls should be in place to ensure the integrity, confidentiality, and availability of an organization's data. These controls include policies, procedures, and control techniques to physically secure computer resources, provide appropriate segregation of computer functions, prevent unauthorized changes to application software, and ensure continuity of computer operations in the event of disaster. However, we found weaknesses in each of these areas. These weaknesses increase the risk of unauthorized access, disclosure, modification, or loss of SEC's information systems and data.

## Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and periodically reviewing access rights granted to ensure that access continues to be appropriate based on criteria established for granting it. At SEC, physical access control measures (such as guards, badges, and locks, used either alone or in combination) are vital to protecting its computing resources and the sensitive data it processes from external and internal threats.

Although SEC had taken certain actions to strengthen its physical security environment, certain weaknesses reduced its effectiveness in protecting and controlling physical access to sensitive work areas, as illustrated by the following examples:

- SEC did not always ensure that access to sensitive computing resources had been granted to only those who needed it to perform their jobs. At the time of our review, approximately 300 employees and contractors had access to SEC's data center, including an undetermined number of application programmers, budget analysts, administrative and customer support staff. Typically, individuals serving in these job functions do not require access to the data center. Although SEC had a policy with specific criteria for granting and retaining physical access to its data center, it did not routinely review its access list for compliance with its policy. At our request, the commission reviewed the list of staff with access to the computer center and subsequently reduced the number of authorized staff from approximately 300 to 150.

- 
- Sensitive computing resources were not always secured. For example, wiring closets containing telecommunication and data equipment were not in a physically restricted space. Although the doors could be locked, we identified six wiring closets in three facilities that were unlocked and unattended. In another facility, rooms that housed computers that were connected to the SEC network were left unlocked and unattended.

As a result, increased risk exists that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

## Segregation of Computer Functions

Segregation of computer functions refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and, thereby, gain unauthorized access to assets or records. Often segregation of computer functions is achieved by dividing responsibilities among two or more organizational groups. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the others. Inadequate segregation of computer functions increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed.

Although computer functions were generally properly segregated at SEC, we identified instances in which functions were not adequately segregated. For example, the commission did not sufficiently separate incompatible system administration and security administration functions of computer operating personnel on its key financial applications. To illustrate, the individuals responsible for performing system support were also responsible for setting security and audit parameters, reviewing user access privileges, and adding and deleting system users. Similarly, SEC assigned one individual to perform both security and software change management functions. Yet SEC did not provide supervisory oversight or establish other mitigating controls to ensure that this individual performed only authorized functions.

These conditions existed, in part, because SEC lacked implementing guidelines for separating incompatible functions among personnel administering its computer applications environment. As a consequence,

---

increased risk exists that these individuals could perform unauthorized system activities without being detected.

## Application Change Controls

It is important to ensure that only authorized and fully tested application programs are placed in operation. To ensure that changes to application programs are needed, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. In addition, as part of the application change control process, library management software should be used to control program versions, and test procedures should be established to ensure that only authorized changes are made to application program code.

SEC did not adequately document or control changes to application programs. Examples include the following instances:

- Although a change control board at SEC was responsible for authorizing all application changes, the authorization for these changes was not formally documented. For example, in a random sample of 32 application changes made during fiscal year 2004, none of the changes had documentation to show that the change control board had authorized these software modifications.
- For a key application, documentation was not always maintained to provide evidence that required reviews and approvals were performed. For 20 software changes reviewed, 13 lacked reviews of developer testing and 17 did not have the approval needed for implementing software changes.
- SEC did not use automated library management software to ensure that program versions were not accidentally misidentified and to prevent simultaneous changes to the same program.
- Procedures were not in place to periodically test application program code to ensure that only authorized changes had been made.

Without adequately documented or controlled application change control procedures, changes may be implemented that are not authorized, tested, reviewed, or approved. Further, the lack of adequate controls places SEC at greater risk that software supporting its operations will not produce reliable data or effectively meet operational needs.

---

---

## Service Continuity

Service continuity controls should be designed to ensure that, when unexpected events occur, key operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. These controls include environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions, along with a well-tested plan to recover critical operations should interruptions occur. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

SEC did not implement a service continuity plan to cover its major applications (including financial and related systems) and its general support systems. While the commission had developed draft plans, it did not include a list of alternate recovery team members, contractor service level agreements, or key components needed for processing at the backup site. Further, SEC had not developed plans for testing its service continuity plans for all critical systems. As a result, SEC has diminished assurance that it will be able to promptly recover essential processing operations if an unexpected interruption occurs.

In response to identified weaknesses in the area of other information system controls, the CIO stated that the commission had revised its computer center access procedures and will conduct additional reviews to determine the continued need for access by employees and contractors. Further, he said that actions had been taken to ensure appropriate segregation of computer functions and efforts were under way to improve the commission's application change control process. In addition, the CIO noted that the commission is finalizing its disaster recovery plans and has conducted limited tests in preparation for planned live tests of its disaster recovery plans.

---

## Comprehensive Information Security Program Is Not Fully Implemented

A key reason for SEC's weaknesses in information system controls is that it has not fully developed and implemented a comprehensive agency information security program to provide reasonable assurance that effective controls are established and maintained and that information security receives sufficient management attention. Our May 1998 study of



---

security management best practices<sup>7</sup> determined that a comprehensive information security program is essential to ensuring that information system controls work effectively on a continuing basis. Also, FISMA,<sup>8</sup> consistent with our study, requires an agency's information security program to include key elements. These elements include:

- a central information security management structure to provide overall information security policy and guidance along with oversight to ensure compliance with established policies and reviews of the effectiveness of the information security environment;
- periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- security awareness training to inform personnel, including contractors and other users of information systems, of information security risks and their responsibilities in complying with agency policies and procedures; and
- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls of every major information system identified in agencies' inventories.

SEC's information system control weaknesses were symptomatic of its weak security program. In its fiscal year 2004 report pursuant to FISMA, the SEC's Office of Inspector General (OIG) reported that the commission was not in substantial compliance with FISMA requirements that are intended to strengthen information security. Also, the SEC has recognized

---

<sup>7</sup>[GAO/AIMD-98-68](#).

<sup>8</sup>FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide information security for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management.

---

weaknesses in its information security program and since 2002 has reported information security as a material weakness in its annual accountability report.<sup>9</sup> Although SEC has initiated various actions to improve its information security program, including establishing a central security management function and appointing a senior information security officer to manage the program, the organization has not yet developed a comprehensive security program to ensure that its information security policies and practices were fully defined, consistent, and continuously effective across all systems. Such a program is critical to provide SEC with a solid foundation for resolving existing information security problems and continuously managing information security risks.

---

## Central Security Management

The first key element of an effective information security program is the establishment of a central security group with clearly defined roles and responsibilities. This group provides the overall security policy and guidance along with the oversight to ensure compliance with established policies and procedures; further, it reviews the effectiveness of the security environment. The central security group often is supplemented by individual security staff designated to assist in the implementation and management of the agency's information security program. To ensure the effectiveness of an agency's security program, clearly defined roles and responsibilities for all security staff should be established, and coordination of responsibilities between individual security staff and central security should be developed.

SEC has established a central security group and appointed a senior information security officer to manage its information security program. Nonetheless, the commission has not yet developed clearly defined roles and responsibilities for this group. In addition, the commission has not designated individual security staff to provide security oversight at its 11 field offices. Without a formally defined and commission-wide security focus, SEC is at increased risk that its security program will not be adequate to ensure the security of its highly interconnected computer environment.

---

<sup>9</sup>The Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. § 3512(d)) requires the head of each agency to annually prepare a statement that identifies material weaknesses in the agency's systems of internal accounting and administrative control and its plans and schedule for correcting them.

---

---

## Assessing Risks

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure that the policies and controls operate as intended. Our study of risk assessment best practices<sup>10</sup> found that a framework for performing these assessments should specify (1) when the assessments should be initiated and conducted, (2) who should participate, (3) how disagreements should be resolved, (4) what approvals are needed, and (5) how these assessments should be documented and maintained. Further, OMB Circular A-130, appendix III,<sup>11</sup> prescribes that risk be assessed when significant changes are made to computerized systems or at least every 3 years.

SEC has not yet fully implemented a risk assessment process. Although it has taken some action, including initiating risk assessments as part of the certification and accreditation process,<sup>12</sup> SEC had not yet developed a process for conducting these assessments. In addition, SEC had not developed a process for assessing risk when significant changes are made to its facility or its computer systems. During the past year, SEC upgraded its network hardware and software, including all workstations, network servers, routers, and switches. Each of these changes could have introduced new vulnerabilities into SEC's computer network, thus warranting a need for a risk assessment. However, SEC did not assess the risks associated with the network upgrade.

---

## Establishing and Implementing Policies

Another key element of an effective information security program is establishing and implementing appropriate policies, procedures, and technical standards to govern security over an agency's computing

---

<sup>10</sup>GAO, *Information Security Risk Assessment: Practices of Leading Organizations: A Supplement to GAO's May 1998 Executive Guide on Information Security Management*, GAO/AIMD-00-33 (Washington, D.C.: November 1999).

<sup>11</sup>Office of Management and Budget, Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (Washington, D.C.: Nov. 28, 2000).

<sup>12</sup>Certification is the comprehensive evaluation of the management, operational, and technical security controls in an information system to determine the effectiveness of these controls and identify existing vulnerabilities. Accreditation is the official management decision to authorize operation of an information system. This authorization explicitly accepts the risk remaining after the implementation of an agreed-upon set of security controls.

---

environment. Such policies and procedures should integrate all security aspects of an organization's interconnected environment, including local and wide area networks and interconnection, to contractor and other federal agencies that support critical mission operations. In addition, technical security standards are needed to provide consistent implementing guidance for each computing environment. Establishing and documenting security policies are important because they are the primary mechanism by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, agency systems and information will not receive the protection provided by the security policies and controls.

Although SEC had made progress in developing policies and procedures for specific security areas including certification and accreditation, password standards, and disaster recovery planning, it had not yet established comprehensive policies and procedures to govern a complete information security program. For example, SEC had not developed adequate policies that address security requirements for key control areas such as physical and electronic access control, segregation of duties, application change control, service continuity, and security management covering its computer network and interconnected environment. In addition, the commission had not developed policies and procedures for such areas as wireless networks and patch management.<sup>13</sup> As a result, SEC is at increased risk that its critical financial and sensitive data could be exposed to unauthorized access possibly without detection.

In addition, OMB Circular A-130 requires agencies to develop and implement information security plans for major applications and general support systems.<sup>14</sup> These plans should address policies and procedures for achieving management, operational, and technical controls. However, SEC had not yet developed security plans for its general support systems and

---

<sup>13</sup>Patch management is a process used to alleviate many of the challenges involved in securing computing systems from attack. It is a component of configuration management that includes acquiring, testing, and applying patches to a computer system.

<sup>14</sup>A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications.

---

had implemented security plans for only one of its seven major applications.

Further, FISMA requires each agency to develop and implement specific information security configuration standards for its computer network systems. In its 2004 FISMA report, the OIG reported that SEC does not have an agency-wide policy that requires specific security configuration standards. Such technical standards would not only help ensure that appropriate computer controls are established consistently, but would also facilitate periodic reviews of these controls.

---

## Promoting Security Awareness

Another FISMA requirement for an information security program involves promoting awareness and providing required training so that users understand the risks and their roles in implementing related policies and controls to mitigate those risks. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees who use computer resources in their day-to-day operations are made aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. FISMA mandates that all federal employees and contractors involved in the use of agency information systems be provided periodic training in information security awareness and accepted information security practices. Further, FISMA requires agency CIOs to ensure specialized training of personnel with significant information security requirements.

SEC established information security awareness programs for its employees and contractors. These programs included distributing security awareness bulletins and brochures and creating information security poster boards. In addition, SEC developed specialized security training for database, system, and network administrators. Nevertheless, SEC did not ensure that all employees, contractors, agency detailees, or staff working in specialized information technology (IT) positions completed security awareness training. SEC's goal that only 90 percent of employees and contractors complete security awareness training was not consistent with information security laws that mandate training for all employees and contractors. In addition, more than 100 staff and contractors serving in positions that provide network operation oversight and other services that provide access to system assets had not received specialized security training.

---

---

## Testing and Evaluating the Effectiveness of Controls

Another key element of an information security program is ongoing testing and evaluation to ensure that systems are in compliance with policies and that policies and controls are both appropriate and effective. This type of oversight is a fundamental element because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results improve the security program. Analyzing the results of monitoring efforts, as well as security reviews performed by external audit organizations, provides security specialists and business managers with a means of identifying new problem areas, reassessing the appropriateness of existing controls, and identifying the need for new controls.

SEC had not established a comprehensive program to test and evaluate the effectiveness of information system controls. SEC had efforts under way to test and evaluate controls, including limited ongoing tests of its computer network. Also, SEC had initiated a formal IT certification and accreditation program using contractor support to certify and accredit the commission's major systems. However, at the completion of our review, none of the commission's seven major applications and general support system had been certified and accredited. Further efforts are still needed to fully implement an ongoing program of tests and evaluation. Missing is an ongoing program that targets the key control areas of physical and electronic access, segregation of computer functions, application and system software, and service continuity. An effective program of ongoing tests and evaluations can be used to identify and correct information security weaknesses such as those discussed in this report.

Based on the results of tests and evaluations that have been conducted by agencies, including OIG and external audit groups, FISMA requires that agencies develop corrective action plans (e.g., plans of action and milestones). However, in its latest FISMA report, OIG stated that SEC does not have a comprehensive process that monitors and prioritizes all identified information security weaknesses. In addition, it noted that all information security weaknesses were not included in corrective action plans. Without adequate corrective action plans, the results of tests and evaluations may not be effectively used to improve the security program and correct identified weaknesses.

In response to identified weaknesses in SEC's information security program, the CIO said that the commission would develop policies and

---

procedures to define the roles and responsibilities of its central security group. These procedures would include coordination of responsibilities between security individuals and functions. In addition, the commission would develop a risk assessment framework to address the need to perform periodic risk assessments and to conduct these assessments when significant changes occur. SEC also intends to develop comprehensive security policies, including security plans for all major applications and general support systems. In addition, the commission plans to enhance its requirements for security awareness training and expects to develop and implement an ongoing security oversight program to include provisions for monitoring compliance with established procedures and testing the effectiveness of its controls.

---

## Conclusions

Information systems controls were not effective at SEC. We identified numerous weaknesses in electronic access controls and other information system controls. As a result, financial and sensitive information was at increased risk of unauthorized disclosure, modification, or loss, and operations at risk of disruption. A key reason for SEC's weaknesses in information system controls is that it has not yet fully developed and implemented a comprehensive agency information security program to ensure that effective controls are established and maintained and that information security receives sufficient attention. Effective implementation of such a program provides for an ongoing cycle of periodically assessing risks, establishing appropriate policies and procedures, promoting security awareness, and establishing an ongoing program of tests and evaluations of the effectiveness of policies and controls to ensure that they remain appropriate and accomplish their intended purpose. Such a program is critical to providing SEC with a solid foundation for resolving existing information security problems and continuously managing information security risks. SEC has taken some action to improve security management, including establishing a central security management function, appointing a senior information security officer to manage the program, and initiating actions to correct the specific weaknesses summarized in this report. However, until it fully implements an agency-wide information security program, SEC will have limited assurance that its financial and sensitive information are adequately protected.

---

---

## Recommendations for Executive Action

We recommend that the SEC chairman direct the CIO to take the following six actions to fully develop and implement an effective agency-wide information security program:

1. Clearly define the roles and responsibilities of the central security group.
2. Designate individual security staff to provide security oversight at SEC's 11 field offices.
3. Develop a process for assessing information security risks, including when significant changes are made to SEC facilities or computer systems.
4. Establish and implement comprehensive information security policies and procedures by addressing security requirements for key control areas and developing and implementing security plans for general support systems and major applications.
5. Provide security awareness training to each employee and contractor, and specialized security training to employees and contractors that require such training.
6. Institute an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective and that corrective action plans address identified weaknesses.

We are also making recommendations in a separate report designed for "Limited Official Use Only." These recommendations address actions needed to correct the specific information security weaknesses related to electronic access controls and other information system controls.

---

## Agency Comments

In providing written comments on a draft of this report, SEC's CIO, Managing Executive for Operations, and Executive Director agreed with our recommendations. SEC's comments are reprinted in appendix I of this report. Specifically, SEC plans to correct the information system control weaknesses identified and enhance its information security program by June 2006. Further, they indicated that significant progress is already being made to address our recommendation.



---

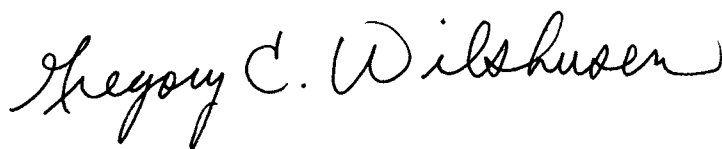
This report contains recommendations to you. As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Governmental Affairs and to the House Committee on Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report. Because agency personnel serve as the primary source of information on the status of recommendations, GAO requests that the agency also provide it with a copy of your agency's statement of action to serve as preliminary information on the status of open recommendations.

---

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Banking, Housing, and Urban Affairs; the Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia, Senate Committee on Homeland Security and Governmental Affairs; House Committee of Financial Services; the Subcommittee on Government Management, Finance, and Accountability, House Committee on Government Reform; and, SEC's Office of Managing Executive for Operations; Office of the Executive Director; Office of Financial Management; Office of Information Technology; and the SEC's Inspector General. We also will make copies available to others on request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions regarding this report, please contact me at (202) 512-3317 or David W. Irvin, Assistant Director, at (214) 777-5716. We can also be reached by e-mail at [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) and [irvind@gao.gov](mailto:irvind@gao.gov), respectively. Key contributors to this report are listed in appendix II.

Sincerely yours,



Gregory C. Wilshusen  
Director, Information Security Issues

# Comments from the Securities and Exchange Commission



UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
WASHINGTON, D.C. 20549

March 2, 2005

Mr. Gregory C. Wilshusen, Acting Director  
Information Security Issues  
Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to respond to the draft reports entitled *Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data*, dated March 2005. The Government Accountability Office (GAO) has identified a number of important information security issues at the SEC, which we are now moving to address. We also appreciate the GAO's acknowledgement that the SEC has made initial progress, by establishing a central information security management function and tasking it to implement the improvements the GAO has outlined.

GAO identified internal control issues resulting from our historical lack of a comprehensive agency program to manage information security. Specifically, the report has outlined the need for improvement in access control management, network security, audit and monitoring functions, and other areas. We appreciate the detailed information technology audit completed by the GAO team, and we intend to use the results to help the SEC improve its overall information security program.

Overall the SEC agrees with the results represented in the draft reports and recognizes the need to further enhance its existing programs. Over the past several months, we have been working internally as well as consulting with the GAO team to develop an action plan to remediate our information security issues. In response to the report's recommendations for executive action, by June 2006 the SEC will:

- Complete corrective action for the control weaknesses identified in the 2004 review;
- Continue to enhance the Commission's overall information security program by: (1) defining clear roles and responsibilities for enterprise information security, (2) developing security risk assessment processes, (3) implementing a comprehensive set of information security policies and procedures, (4) providing security awareness training to employees and contractors; and (5) systematically testing policies and procedures for their appropriateness and effectiveness.

---

**Appendix I**  
**Comments from the Securities and Exchange**  
**Commission**

---

Specific corrective action plans, including specific milestones and timing for each of the audit recommendations, were provided separately to the GAO Information Security audit team.

We believe that significant progress is being made to address the weaknesses identified in the draft reports. We also understand that the GAO is not advocating “quick fixes”, but rather a sustained effort that deeply embeds the principles of strong information security throughout our technical environment, our agencywide business processes, and our organizational culture. Given that, we have also recognized the need for resources and significant executive commitment towards resolving these issues.

The SEC is actively working to mitigate the GAO’s findings. We are committed to address high risk issues immediately, and to show substantial improvement throughout 2005. On a quarterly basis, we have directed the Chief Information Security Officer to formally update us on progress in remediating each of the security concerns raised by the audit. We look forward to continuing our productive dialogue with the GAO as we continue to enhance our security program.

If you have questions relating to our response or our information security program, please contact Corey Booth, Chief Information Officer, at (202) 551-8800.

Sincerely,



R. Corey Booth  
Chief Information Officer



Peter Derby  
Managing Executive for Operations



James M. McConnell  
Executive Director

# GAO Contact and Staff Acknowledgments

---

---

## GAO Contact

David W. Irvin, (214) 777-5716

---

## Staff Acknowledgments

In addition to the individual named above, Edward Alexander, Lon Chin, West Coile, Debra Conner, Anh Dang, Nancy Glover, Steve Gosewehr, Rosanna Guerrero, Harold Lewis, Leena Mathew, Duc Ngo, Eugene Stevens, Charles Vrabel, and Chris Warweg made key contributions to this report.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to Updates."

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office  
441 G Street NW, Room LM  
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000  
TDD: (202) 512-2537  
Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Gloria Jarmon, Managing Director, [JarmonG@gao.gov](mailto:JarmonG@gao.gov) (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, D.C. 20548

---

## Public Affairs

Paul Anderson, Managing Director, [AndersonP1@gao.gov](mailto:AndersonP1@gao.gov) (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548