

March 2009

# INFORMATION SECURITY

## Securities and Exchange Commission Needs to Consistently Implement Effective Controls

This is a revised version of a prior report that was issued on March 16, 2009 with an incorrect attachment.



GAO

Accountability \* Integrity \* Reliability



Highlights of [GAO-09-203](#), a report to the Chairman, Securities and Exchange Commission

## Why GAO Did This Study

In carrying out its mission to ensure that securities markets are fair, orderly, and efficiently maintained, the Securities and Exchange Commission (SEC) relies extensively on computerized systems. Effective information security controls are essential to ensure that SEC's financial and sensitive information is protected from inadvertent or deliberate misuse, disclosure, or destruction.

As part of its audit of SEC's financial statements, GAO assessed (1) the status of SEC's actions to correct previously reported information security weaknesses and (2) the effectiveness of SEC's controls for ensuring the confidentiality, integrity, and availability of its information systems and information. To do this, GAO examined security policies and artifacts, interviewed pertinent officials, and conducted tests and observations of controls in operation.

## What GAO Recommends

GAO recommends that SEC fully implement its information security program.

In commenting on a draft of this report, SEC agreed with GAO's recommendations and stated that it plans to address the identified weaknesses.

To view the full product, including the scope and methodology, click on [GAO-09-203](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or [wilshusen@gao.gov](mailto:wilshusen@gao.gov), or Dr. Nabajyoti Barkakati at (202) 512-4499 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov).

## INFORMATION SECURITY

### Securities and Exchange Commission Needs to Consistently Implement Effective Controls

#### What GAO Found

SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 18 of 34 weaknesses previously reported as unresolved at the time of our prior audit. For example, SEC has adequately validated electronic certificates from connections to its network, physically secured the perimeter of its operations center and put in place a process to monitor unusual and suspicious activities, and removed network system accounts and data center access rights from separating employees. In addition, the commission has made progress in improving its information security program. To illustrate, it has developed, documented, and implemented a policy on remedial action plans to ensure that deficiencies are mitigated in an effective and timely manner, and provided individuals with training for incident handling. Nevertheless, SEC has not completed actions to correct 16 previously reported weaknesses. For example, it did not adequately document access privileges granted to users of a key financial application, and did not always implement patches on vulnerable workstations and enterprise database servers.

In addition to the 16 previously reported weakness that remain uncorrected, GAO identified 23 new weaknesses in controls intended to restrict access to data and systems, as well as weaknesses in other information security controls, that continue to jeopardize the confidentiality, integrity, and availability of SEC's financial and sensitive information and information systems. The commission has not fully implemented effective controls to prevent, limit, or detect unauthorized access to computing resources. For example, it did not always (1) consistently enforce strong controls for identifying and authenticating users, (2) sufficiently restrict user access to systems (3) encrypt network services, (4) audit and monitor security-relevant events for its databases, and (5) physically protect its computer resources. SEC also did not consistently ensure appropriate segregation of incompatible duties or adequately manage the configuration of its financial information systems.

A key reason for these weaknesses is that the commission has not yet fully implemented its information security program to ensure that controls are appropriately designed and operating as intended. Specifically, SEC has not effectively or fully implemented key program activities. For example, it has not (1) filled the vacancy for a senior agency information security officer, (2) fully reported or assessed risks, (3) sufficiently tested and evaluated the effectiveness of its information system controls, and (4) certified and accredited a key intermediary subsystem. Although progress has been made, significant and preventable information security control deficiencies create continuing risks of the misuse of federal assets, unauthorized modification or destruction of financial information, inappropriate disclosure of other sensitive information, and disruption of critical operations.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Background	2
	Control Weaknesses Continue to Place Financial Information at Risk	6
	Conclusions	15
	Recommendations for Executive Action	16
	Agency Comments	16
<b>Appendix I</b>	<b>Objectives, Scope, and Methodology</b>	<b>18</b>
<b>Appendix II</b>	<b>Comments from the Securities and Exchange Commission</b>	<b>21</b>
<b>Appendix III</b>	<b>GAO Contacts and Staff Acknowledgments</b>	<b>23</b>

---

## Abbreviations

CIO	chief information officer
EDGAR	Electronic Data Gathering Analysis, and Retrieval
FISMA	Federal Information Security Management Act
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SEC	Securities and Exchange Commission
US-CERT	United States Computer Emergency Readiness Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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, DC 20548

March 16, 2009

The Honorable Mary L. Schapiro  
Chairman  
United States Securities and Exchange Commission

Dear Madam Chairman:

As you are aware, the Securities and Exchange Commission (SEC) is responsible for enforcing securities laws, issuing rules and regulations that provide protection for investors, and helping to ensure that the securities markets are fair and honest. To support its demanding financial and mission-related responsibilities, the commission relies extensively on computerized systems. In order to protect financial and sensitive information—including personnel and regulatory information maintained by SEC—from inadvertent or deliberate misuse, fraudulent use, improper disclosure or manipulation, or destruction, it is essential that SEC have effective information security controls in place.<sup>1</sup>

As part of our audit of SEC's fiscal year 2008 financial statements,<sup>2</sup> we assessed the effectiveness of the commission's information security controls over key financial systems, data, and networks. In our report on SEC's financial statements for fiscal years 2008 and 2007,<sup>3</sup> we concluded that weaknesses in information security controls constitute a significant

---

<sup>1</sup>Information security controls include security management, access controls, configuration management, segregation of duties, and contingency planning. These controls are designed to ensure that there is a continuous cycle of activity for assessing risk, logical and physical access to sensitive computing resources and information is appropriately restricted; only authorized changes to computer programs are made; one individual does not control all critical stages of a process; and backup and recovery plans are adequate to ensure the continuity of essential operations.

<sup>2</sup>GAO, *Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Years 2008 and 2007*, [GAO-09-173](#) (Washington, D.C.: Nov. 14, 2008).

<sup>3</sup>[GAO-09-173](#).

---

deficiency in internal controls over the information systems and data used for financial reporting.<sup>4</sup>

In this report, we provide additional details on SEC's information security controls. Our specific objectives were to assess (1) the status of the commission's actions to correct or mitigate previously reported information security weaknesses and (2) the effectiveness of its controls for ensuring the confidentiality, integrity, and availability of its financial information systems and information. We performed our audit at SEC headquarters in Washington, D.C., and at its computer facilities in Alexandria and Ashburn, Virginia, from July 2008 to March 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for additional details on our objectives, scope, and methodology.

---

## Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business and is especially important for government agencies, where maintaining the public's trust is essential. While the dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have enabled agencies such as SEC to better accomplish their missions and provide information to the public, the changes also expose federal networks and systems to various threats. For example, the Federal Bureau of Investigation has identified multiple sources of cyber threats, including foreign nation states engaged in information warfare, domestic criminals, hackers and virus writers, and disgruntled employees working within an organization. Concerns about these threats are well founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. For example, the number of incidents reported by federal

---

<sup>4</sup>A significant deficiency is a control deficiency or a combination of control deficiencies that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliability such that there is more than a remote likelihood that a more than inconsequential misstatement of SEC's financial statements will not be prevented or detected.

---

agencies to the United States Computer Emergency Readiness Team (US-CERT), has increased dramatically over the past 3 years, increasing from 3,634 incidents reported in fiscal year 2005 to 13,029 incidents in fiscal year 2007 (a 259 percent increase).<sup>5</sup> Without proper safeguards, systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain or manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Our previous reports and reports by federal inspectors general describe persistent information security weaknesses that place federal agencies at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997, a designation that remains in force today.<sup>6</sup> Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002 to strengthen the security of information and systems within federal agencies.<sup>7</sup> FISMA requires each agency to develop, document, and implement an agencywide 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.

---

## SEC's Role as Protector of Securities Investors

Following the stock market crash of 1929, Congress passed the Securities Exchange Act of 1934, establishing SEC to enforce securities laws, regulate the securities markets, and protect investors.<sup>8</sup> To carry out its responsibilities and help ensure that securities markets are fair and honest, SEC issues rules and regulations that promote adequate and effective disclosure of information to the investing public. The commission also oversees the registration of other key participants in the securities

---

<sup>5</sup>US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defenses against and responses to cyber attacks across the nation.

<sup>6</sup>GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

<sup>7</sup>FISMA was enacted as Title III, E-Government Act of 2002, Pub L. No 107-347, 116 Stat. 2946 (Dec. 17, 2002).

<sup>8</sup>15 U.S.C. § 78d.

---

industry, including stock exchanges, broker-dealers, clearing agencies, depositories, transfer agents, investment companies, and public utility holding companies. SEC is an independent, quasi-judicial agency that operates at the direction of five commissioners appointed by the President and confirmed by the Senate.

In fiscal year 2008, SEC received a budget authority of \$906 million and had a staff of 3,511 employees. In addition, the commission collected \$569,000 in filing fees and about \$434 million in penalties and disgorgements.<sup>9</sup>

To support its financial operations and store the sensitive information it collects, SEC relies extensively on computerized systems interconnected by local and wide-area networks. For example, to process and track financial transactions, such as filing fees paid by corporations, disgorgements and penalties from enforcement activities, and procurement activities, SEC relies on several enterprise database applications—Momentum; Phoenix; Electronic Data Gathering, Analysis, and Retrieval (EDGAR); and Fee Momentum—and a general support system network that allows users to communicate with the database applications. The database applications provide SEC with the following capabilities:

- Momentum is used to record the commission’s accounting transactions, to maintain its general ledger, and to maintain some of the information SEC uses to produce financial reports.
- Phoenix contains and processes sensitive data relating to penalties, disgorgements, and restitution on proven and alleged violations of securities and futures laws.
- EDGAR performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others that are required to file certain information with SEC. Its primary purpose is to increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency.

---

<sup>9</sup>A disgorgement is the repayment of illegally gained profits (or avoided losses) for distribution to harmed investors whenever feasible.

- 
- The general support system is an integrated client-server system composed of local- and wide-area networks and is organized into distinct subsystems based along SEC's organizational and functional lines. The general support system provides services to internal and external customers who use them for their business applications. It also provides the necessary security services to support these applications.

Under FISMA, the Chairman of SEC has responsibility for, among other things, (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information systems and information; (2) ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; and (3) delegating to the agency chief information officer (CIO) the authority to ensure compliance with the requirements imposed on the agency. FISMA requires the CIO to designate a senior agency information security officer who shall carry out the CIO's information security responsibilities.

---

### SEC Has Made Important Progress Correcting Previously Reported Weaknesses and Improving Security

SEC has corrected or mitigated 18 of the 34 security control weaknesses that we had reported as unresolved at the time of our prior audit report in 2008.<sup>10</sup> For example, it has

- adequately validated electronic certificates from connections to its network,
- physically secured the perimeter of the operations center,
- monitored unusual and suspicious activities at its operations center, and
- removed network system accounts and data center access rights from separating employees.

In addition, SEC has made progress in improving its information security program. For example, the commission has developed, documented, and implemented a policy on remedial action plans to help ensure that deficiencies are mitigated in an effective and timely manner, and provided individuals with training for incident handling. These efforts constitute an

---

<sup>10</sup>[GAO-08-280](#).



---

important step toward strengthening the agencywide information security program mandated by FISMA.

While SEC has made important progress in strengthening its information security controls, it has not completed actions to correct or mitigate 16 of the previously reported weaknesses. For example, SEC has not adequately documented access privileges for the EDGAR application, always implemented patches on vulnerable workstations and enterprise database servers, or always sufficiently protected passwords. Failure to resolve these issues could leave sensitive data vulnerable to unauthorized disclosure, modification, or destruction.

---

## Control Weaknesses Continue to Place Financial Information at Risk

In addition to the 16 previously reported weakness that remain uncorrected, we identified 23 new weaknesses in controls intended to restrict access to data and systems, as well as weaknesses in other information security controls, that continue to jeopardize the confidentiality, integrity, and availability of SEC's financial and sensitive information and information systems. Previously reported and newly identified weaknesses hinder the commission's ability to perform vital functions and increase the risk of unauthorized disclosure, modification, or destruction of financial information. A key reason for these weaknesses was that SEC did not fully implement key activities of its information security program.

---

## SEC Did Not Sufficiently Control Access to Information Resources

A basic management objective for any organization is to protect the resources that support its critical operations and assets from unauthorized access. Organizations accomplish this by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computer resources (e.g., data, programs, equipment, and facilities), thereby protecting them from unauthorized disclosure, modification, and loss. Specific access controls include identification and authentication, authorization, cryptography, audit and monitoring, and physical security. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally modify or delete data or execute changes that are outside of their span of authority.

---

Controls for Identifying and Authenticating Users Were Not Consistently Enforced

A computer system must be able to identify and authenticate the identities of users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system must also establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. Furthermore, SEC policy requires the implementation of automated identification and authentication mechanisms that enable the unique identification of individual users and systems.

SEC did not consistently enforce identification and authentication controls for its users and systems. For example, it did not always

- securely configure the snmp community string (similar to a password) used to monitor and manage network devices;<sup>11</sup>
- remove the default vendor account for a remote network service, which could allow access to the network service without the need to provide a password;
- restrict multiple database administrators from sharing the same log-on application ID to a powerful database account; and
- uniquely identify individual accounts on network switches for https login.<sup>12</sup>

As a result, increased risk exists that users will not be uniquely identified before they access the SEC network, and SEC will not be able to hold them accountable in the event of a security incident.

User Access to Systems Was Not Sufficiently Restricted

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying access rights is

---

<sup>11</sup>Simple Network Management Protocol (*snmp*) is a standard protocol for remote management and monitoring of network devices that uses a community string as a password for authentication.

<sup>12</sup>Hypertext Transfer Protocol Secure (*https*) is a separate protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.

---

the concept of “least privilege.” Least privilege is a basic principle for securing computer resources and data that means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users’ access to only those programs and files that they need in order to do their work, organizations establish access rights and permissions. “User rights” are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that are associated with a particular file or directory, regulating which users can access it—and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. In addition, SEC policy requires that each user or process be assigned only those privileges or functions needed to perform authorized tasks and that approval of such privileges be documented. Furthermore, SEC policy states that only services that are absolutely necessary are allowed to have a remote connection.

SEC did not always sufficiently restrict system access and privileges to only those users that needed access to perform their assigned duties. For example, SEC did not always

- remove excessive user privileges on its financial systems,
- properly document or maintain approval of user access privileges to the Momentum system,
- restrict unnecessary remote access to database servers, and
- limit users’ privileges so that users do not monopolize database system resources during critical times of the day.

As a result, increased risk exists that users could gain inappropriate access to computer resources, circumvent security controls, and deliberately or inadvertently read, modify, or delete critical financial information. In addition, SEC’s financial information may not be available when it is needed.

## Network Services Were Not Always Encrypted

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity by transforming plaintext into ciphertext using a special value known as a key and a mathematical process known as an algorithm. The National Security Agency

---

recommends encrypting network services. If encryption is not used, user ID and password combinations are susceptible to electronic eavesdropping by devices on the network when they are transmitted.

Although SEC has implemented a network topology that employs extensive switching and limits eavesdropping to only the network segment accessible by the potential eavesdropper, it did not always ensure that information transmitted over the network was adequately encrypted. While the eavesdropping risk on the SEC network is reduced by its topology, nonetheless, increased risk exists that individuals could capture user IDs and passwords and use them to gain unauthorized access to network devices.

#### Audit and Monitoring of Security-Relevant Events on Databases Was Inadequate

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. 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. 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. SEC also requires the enforcement of auditing and accountability by configuring information systems to produce, store, and retain audit records of system, application, network, and user activity.

SEC did not adequately configure several database systems to enable auditing and monitoring of security-relevant events. For example, it did not configure one database to record successful log-ons or security violations for unauthorized modification of data, and three databases to safeguard log data against loss. As a result, there is increased likelihood that unauthorized activities or policy violations would not be detected.

#### Weaknesses in Physical Security Controls Reduced Their Effectiveness

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 has strengthened its physical security controls, certain weaknesses reduced its effectiveness in protecting and controlling physical access to sensitive work areas. For example, on multiple occasions SEC employees entered electronically secured interior spaces by following another employee through an open door instead of using their badges to obtain access. In addition, physical security standards have been drafted but have not been approved by management. 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.

---

## Weaknesses in Other Information System Controls Increase Risk

### Incompatible Duties and Functions Were Not Adequately Segregated

In addition to having access controls, an organization should have policies, procedures, and control techniques in place to appropriately segregate computer-related duties. Segregation of duties 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 incompatible duties 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 another. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. In addition, SEC policy requires that each user or process be assigned only those privileges or functions needed to perform authorized tasks.

SEC did not adequately segregate incompatible computer-related duties and functions. For example, a financial services branch chief could perform multiple incompatible duties such as creating, modifying, and deleting security organizations, roles, and security categories. At the same time, he could perform financial operations such as creating, approving, and changing invoices. These conditions existed, in part, because SEC

---

lacked implementation guidelines for assigning incompatible duties among personnel administering its computer applications environment. In addition, although SEC has logically separated many of its networked devices, it did not always adequately separate network management traffic from general network traffic. As a result, general users could gain inappropriate access and intentionally or inadvertently disrupt network operations. As a consequence, increased risk exists that users could perform unauthorized system activities without detection.

### Configuration Management Controls Were Not Adequately Implemented

Configuration management is another important control that involves the identification and management of security features for all hardware and software components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. An effective configuration management process includes procedures for (1) identifying, documenting, and assigning unique identifiers (for example, serial number and name) to a system's hardware and software parts and subparts, generally referred to as configuration items; (2) evaluating and deciding whether to approve changes to a system's baseline configuration; (3) documenting and reporting on the status of configuration items as a system evolves; (4) determining alignment between the actual system and the documentation describing it; and (5) developing and implementing a configuration management plan for each system. In addition, establishing controls over the modification of information system components and related documentation helps to prevent unauthorized changes and ensure that only authorized systems and related program modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all hardware, software, and firmware programs and program modifications are properly authorized, tested, and approved.

SEC has implemented several elements of a configuration management process. Specifically, it has documented policies and procedures for assigning unique identifiers and naming configuration items so that they can be distinguished from one another and for requesting changes to configuration items. SEC has also developed a change request process and an enterprise-level change control board to review changes.

However, SEC has not adequately implemented key configuration management controls over the information system components associated with the upgrade to Momentum. Specifically, it did not always document, evaluate, or approve changes to a system's baseline. For example, it did not consistently document test plans; adequately document or approve changes to the requirements, design, and scripts; establish or maintain

---

configuration baselines; or apply up-to-date patches on its database servers that support processing of financial data. In addition, SEC did not document and report on the status of configuration items as Momentum evolved, nor did it conduct configuration audits to determine the alignment between the actual system and the documentation describing it.

Furthermore, SEC did not (1) develop a configuration management plan for Momentum, (2) assign a manager or team to conduct these activities, and (3) use adequate tools to implement the process. As a result, increased risk exists that authorized changes will not be made and unauthorized changes will be made to the Momentum system.

---

### SEC Has Not Fully Implemented Its Information Security Program

SEC has made important progress in implementing its information security program. For example, SEC has provided individuals with training for incident handling and developed, documented, and implemented a policy on remedial action plans to ensure that deficiencies are mitigated in an effective and timely manner. However, a key reason for the information security weaknesses is that it has not effectively or fully implemented key program activities. Until all key elements of its information security program are fully and consistently implemented, SEC will not have sufficient assurance that new weaknesses will not emerge and that financial information and financial assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

### SEC Has Not Filled the Senior Agency Information Security Officer Position

FISMA requires the CIO to designate a senior agency information security officer who shall have information security duties as that official's primary duty and head an office with the mission and resources to assist in ensuring agency compliance with the provisions of the act. This officer will be responsible for carrying out the CIO's information security responsibilities, including developing and maintaining a departmentwide information security program, developing and maintaining information security policies and procedures, and providing training and oversight to security personnel.

However, although SEC appointed an acting senior agency information security officer from April to July 2008, the position has been vacant for the past 8 months. According to an SEC official, a vacancy announcement has not yet been posted for this position. Without a senior security officer to provide direction for an agencywide 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.

---

SEC Did Not Fully Report Risks to Management

FISMA and its implementing policies require agencies to develop, document, and implement periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. The National Institute of Standards and Technology (NIST) also states that a risk assessment report should be presented as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. SEC policy states that security risk assessment involves the identification and evaluation of IT security risks. This process identifies IT security-related risks to information and information systems, considers the probability of occurrence, and measures their potential impact. The SEC Office of IT Security Group is responsible for periodically reviewing the risk assessments to ensure that all aspects of risk and applicable IT security requirements have been adequately addressed.

SEC did not provide full information for management oversight of risks associated with the Momentum application. For example, the SEC security testing and evaluation for Momentum identified numerous configuration management vulnerabilities that affect other areas such as access controls, separation of duties, and inappropriate administrative roles assigned to individuals. Several of these vulnerabilities in the security testing and evaluation were not reported in the risk assessment summary for the Momentum application for management attention. As a result, SEC management may not be fully aware of all risks or the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support their operations and assets.

System Security Tests Were Not Always Sufficient

FISMA and its implementing policies require periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices performed with a frequency depending on risk, but no less than annually; this should include testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems. This type of oversight is a fundamental element of a security program because it demonstrates management's commitment to the program, reminds employees of their roles and responsibilities, and identifies areas of noncompliance and ineffectiveness. Analyzing the results of security reviews 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. FISMA



---

requires that the frequency of tests and evaluations be based on risks and occur no less than annually.<sup>13</sup>

However, SEC did not sufficiently conduct periodic testing and evaluation of controls. For example, SEC did not test and evaluate the effectiveness of security controls for the general support system supporting Momentum and EDGAR in fiscal year 2008. In addition, the scope and depth of security testing and evaluation that were performed were not comprehensive and often did not identify control weaknesses. To illustrate, SEC did not test or assess the effectiveness of a key subsystem used to develop financial statements, and an independent contractor tested only 4 of 65 security roles in Momentum, severely limiting the scope of the testing.<sup>14</sup> In addition, control tests conducted by SEC on Momentum did not identify vulnerabilities in the following controls: (1) configuration management, (2) separation of duties, (3) audit and monitoring, and (4) access controls; in contrast our tests identified vulnerabilities in these controls. As a result, there is heightened risk that SEC cannot be assured that Momentum and EDGAR meet requirements and perform as intended.

#### A Key Intermediary Subsystem Was Not Certified and Accredited

According to NIST, security certification and accreditation of information systems and subsystems are important activities that support a risk management process and are an integral part of an agency's information security program.<sup>15</sup> Security certification consists of conducting a security control assessment and developing the security documents. Security accreditation is the official management decision given by a senior agency official to authorize the operation of an information system and to explicitly accept the risk it may present to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Required by Office of Management and Budget (OMB) Circular A-130, appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible on an information system, given mission requirements and technical, operational, and

---

<sup>13</sup>44 U.S.C. § 3544(b) (5).

<sup>14</sup>Role-based security is used to restrict access to resources to only those users who have been granted a particular security role.

<sup>15</sup>An information system includes information resources organized for the collection, processing, maintenance, use, sharing, dissemination, and disposition of information. A subsystem is a major component of an information system consisting of information, information technology, and personnel that perform one or more specific functions.

---

cost/schedule constraints. After certification, a security accreditation package with security documents is provided to the authorizing official with the essential information for the official to make a credible, risk-based decision on whether to authorize operation of the information system. The security accreditation package includes the security plan, risk assessment, contingency plan, security assessment report, and plan of action and milestones.

SEC did not certify and accredit a key intermediary subsystem that supports the production of its financial statements. In preparing its financial statements, SEC regularly used this intermediary subsystem to process transactions before loading the financial data into the Momentum application. The subsystem encompassed (1) an application tool to handle transactions of disgorgement data between the Phoenix and Momentum applications; (2) spreadsheets to record, calculate, maintain, and report financial transactions from various accounts; and (3) a third-party tool used for manipulating, sorting, and merging financial data. SEC did not certify or accredit the subsystem or include it as part of the security certification and accreditation process for Phoenix and Momentum. For example, the subsystem was not described in a security plan, risk assessment, contingency plan, security assessment report, or plan of action and milestone. Without certification and accreditation of the intermediate subsystem, possible security weaknesses may go undetected and management may not be alerted to potential vulnerabilities.

---

## Conclusions

SEC has made progress in correcting or mitigating previously reported weaknesses. However, information security weaknesses—both old and new—continue to impair the agency’s ability to ensure the confidentiality, integrity, and availability of financial and sensitive information. These weaknesses represent a significant deficiency in internal controls over the information systems and data used for financial reporting.

A key reason for these weaknesses is that the agency has not yet fully implemented critical elements of its agencywide information security program. Until SEC (1) mitigates known information security weaknesses in access controls and other information system controls and (2) fully implements a comprehensive agencywide information security program that includes filling the security officer position, adequately reporting risks, conducting effective system security tests, and certifying and accrediting an intermediary subsystem, its financial information will remain at increased risk of unauthorized disclosure, modification, or

---

destruction, and its management decisions may be based on unreliable or inaccurate information.

---

## Recommendations for Executive Action

To assist the commission in improving the implementation of its agencywide information security program, we recommend that the SEC Chairman direct the CIO to take the following four actions:

- designate a senior agency information security officer who will be responsible for managing SEC's information security program,
- provide full information for management oversight of information security risks,
- conduct comprehensive periodic testing and evaluation of the effectiveness of security controls for the general support system and key financial applications, and
- certify and accredit subsystems that support the production of SEC's financial statements.

In a separate report with limited distribution, we are also making 32 recommendations to enhance SEC's access controls and configuration management practices.

---

## Agency Comments

In providing written comments on a draft of this report, the SEC Chairman agreed with our recommendations and reported that the agency is on track to address our new findings and to complete remediation of prior year findings. She stated that strong internal controls are one of SEC's highest priorities and that it is committed to proper stewardship of the information entrusted to it by the public. The Chairman's written comments are reprinted in appendix II.

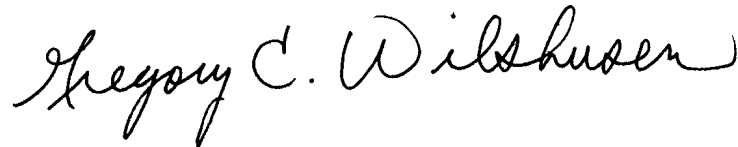
---

We are sending copies of this report to the Chairmen and Ranking Members of the Senate Committee on Banking, Housing, and Urban Affairs; the Senate Committee on Homeland Security and Governmental Affairs; the House Committee on Financial Services; and the House Committee on Oversight and Government Reform. We are also sending copies to the Secretary of the Treasury, the Director of the Office of Management and Budget, and other interested parties. In addition, this report will be available at no charge on our Web site at <http://www.gao.gov>.

---

If you have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) or [barkakatin@gao.gov](mailto:barkakatin@gao.gov). Contacts for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. Individuals who made key contributions to this report are listed in appendix III.

Sincerely yours,



Gregory C. Wilshusen  
Director, Information Security Issues



Dr. Nabajyoti Barkakati  
Director, Center for Technology and Engineering

---

# Appendix I: Objectives, Scope, and Methodology

---

The objectives of our review were (1) to determine the status of the Securities and Exchange Commission's (SEC) actions to correct or mitigate previously reported information security weaknesses and (2) to determine whether controls over key financial systems were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive information. This review was performed for the purpose of supporting the opinion developed during our audit of SEC's internal controls over the preparation of its 2008 financial statements.

To determine the status of SEC's actions to correct or mitigate previously reported information security weaknesses, we identified and reviewed its information security policies, procedures, practices, and guidance. We reviewed prior GAO reports to identify previously reported weaknesses and examined the commission's corrective action plans to determine which weaknesses it had reported were corrected. For those instances where SEC reported that it had completed corrective actions, we assessed the effectiveness of those actions by reviewing the appropriate documents and interviewing the appropriate officials.

To determine whether controls over key financial systems were effective, we tested the effectiveness of selected information security controls. We concentrated our evaluation primarily on the controls for financial applications, enterprise database applications, and network infrastructure—Momentum; Phoenix; Electronic Data Gathering, Analysis, and Retrieval (EDGAR); Fee Momentum; and the general support system—that directly or indirectly support the processing of material transactions reflected in the agency's financial statements. Our evaluation was based on our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information.

Using National Institute of Standards and Technology (NIST) standards and guidance and SEC's policies, procedures, practices, and standards, we evaluated controls by

- testing the complexity and expiration of password settings on selected servers to determine if strong password management was enforced;
- analyzing users' system authorizations to determine whether users had more permissions than necessary to perform their assigned functions;

- observing methods for providing secure data transmissions across the network to determine whether sensitive data were being encrypted;
- observing whether system security software was logging successful system changes;
- testing and observing physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- inspecting key servers and workstations to determine whether critical patches had been installed or were up to date;
- examining access privileges to determine whether incompatible functions were segregated among different individuals; and
- observing end user activity pertaining to the process of preparing SEC financial statements.

Using the requirements identified by the Federal Information Security Management Act (FISMA), the Office of Management and Budget (OMB), and NIST, we evaluated SEC's implementation of its security program by

- reviewing SEC's risk assessment process and risk assessments for three key systems that support the preparation of financial statements to determine whether risks and threats were documented consistent with federal guidance;
- analyzing SEC's policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- analyzing security plans to determine if management, operational, and technical controls were in place or planned and that security plans were updated;
- examining training records for personnel with significant security responsibilities to determine if they received training commensurate with those responsibilities;
- analyzing security testing and evaluation results for three key systems to determine whether management, operational, and technical controls were tested at least annually and based on risk;

- examining remedial action plans to determine whether they addressed vulnerabilities identified in security testing and evaluations; and
- examining contingency plans for three key systems to determine whether those plans had been tested or updated.

We also discussed, with key security representatives and management officials, whether information security controls were in place, adequately designed, and operating effectively. We conducted this audit from July 2008 to March 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Comments from the Securities and Exchange Commission



THE CHAIRMAN

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

March 11, 2009

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

Dear Mr. Wilshusen:

Thank you for the opportunity to respond to the draft report entitled *Information Security: Securities and Exchange Commission Needs To Consistently Implement Effective Controls*, dated March 2009. As required by the Accountability of Tax Dollars Act of 2002, this audit was conducted to ensure that the SEC's financial statements for fiscal 2008 were reliable and to verify that SEC management maintained internal controls over financial reporting. Since the mission of the SEC involves ensuring strong internal controls within the companies the agency monitors, it is imperative that we hold ourselves to high standards in this area. Improving our internal controls has been, and continues to be, one of our highest priorities.

The report demonstrates our commitment to this effort, by documenting the SEC's continued progress in addressing GAO findings from previous audits, as well as our prompt remediation of many specific issues discovered during the course of this year's work. Because in previous years the SEC had addressed many of the more common information security weaknesses, auditors have increasingly focused their reviews on a narrower set of relatively lower-level controls. Since the conclusion of the audit in November 2008, we have made additional progress in resolving outstanding issues and further strengthening our information security program. In particular, we have:

- Implemented additional processes, tools, and techniques to continuously monitor for vulnerabilities in our general support system and critical applications;
- Improved user access reporting by monitoring user accounts and ensuring that separated employees do not have access to systems and applications;
- Attained, for the third year, over 99 percent completion rate for yearly security awareness training;
- Implemented a monitoring and notification system to track entry and exit from designated high security areas.

Overall, we agree with GAO's recommendations, are on track to address new findings, and to complete remediation of prior year findings. Specifically, we will:



---

**Appendix II: Comments from the Securities  
and Exchange Commission**

---

Mr. Gregory C. Wilshusen  
Page 2

- Improve authentication, authorization, and configuration management processes, bringing these critical functions closer to full compliance with existing policies;
- Encrypt, to the maximum extent practical, data and services;
- Better capture critical information needed for auditing and monitoring of security-related events;
- Improve documentation of our physical security procedures, many of which were still in draft form during the audit.

Enclosure (1) contains our response to specific audit findings highlighted in the draft report. Information security continues to be a critical priority for this agency and we will allocate our resources on a risk-weighted basis to address the GAO recommendations. The SEC is committed to providing proper stewardship over the information the public routinely entrusts to us. We appreciate GAO's ongoing support in helping us achieve these goals.

If you have any questions relating to the SEC Management Response, please feel free to contact me at (202) 551-2100, or contact our Chief Information Officer, Charles Boucher, at (202) 551-8802.

Sincerely,



Mary L. Schapiro  
Chairman

Charles Boucher - Chief Information Officer

Enclosure (1): SEC Response to GAO 2009 Audit Findings 3-5-09

Enclosure (1) is  
reprinted in a separate  
report with limited  
distribution.

---

# Appendix III: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov)  
Dr. Nabajyoti Barkakati, (202) 512-4499 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov)

---

## Staff Acknowledgments

In addition to the contacts named above, David B. Hayes and William F. Wadsworth (Assistant Directors), Angela M. Bell, Mark J. Canter, Kirk J. Daubenspeck, Patrick R. Dugan, Mickie E. Gray, Sharon S. Kitrell, Lee A. McCracken, Stephanie Santoso, Duc M. Ngo, Tammi L. Nguyen, Henry I. Sutanto, Edward R. Tekeley and Jayne L. Wilson 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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## 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

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548