

March 2006

INFORMATION SECURITY

Securities and Exchange Commission Needs to Continue to Improve Its Program



Highlights of [GAO-06-408](#), a report to the Chairman, Securities and Exchange Commission

Why GAO Did This Study

The Securities and Exchange Commission (SEC) has a demanding responsibility enforcing securities laws, regulating the securities markets, and protecting investors. In enforcing these laws, SEC issues rules and regulations to provide protection for investors and to help ensure that the securities markets are fair and honest. It relies extensively on computerized systems to support its financial and mission-related operations. Information security controls affect the integrity, confidentiality, and availability of sensitive information maintained by SEC.

As part of the audit of SEC's fiscal year 2005 financial statements, GAO assessed (1) the status of SEC's actions to correct or mitigate previously reported information security weaknesses and (2) the effectiveness of the commission's information system controls in protecting the confidentiality, integrity, and availability of its financial and sensitive information.

What GAO Recommends

GAO recommends that SEC Chairman direct the Chief Information Officer to fully implement an agencywide information security program. In providing written comments on a draft of this report, SEC said that GAO's recommendations are appropriate and actionable, and that it is focusing on fully implementing the recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-408.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

March 2006

INFORMATION SECURITY

Securities and Exchange Commission Needs to Continue to Improve Its Program

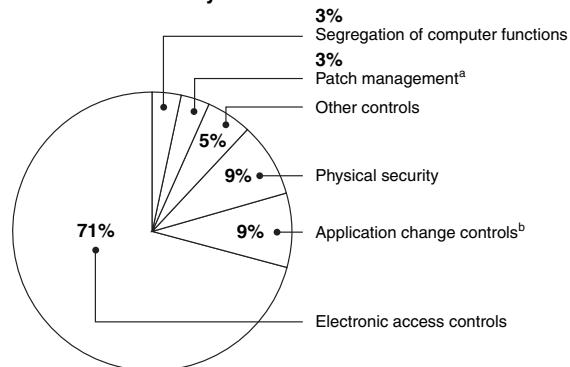
What GAO Found

Although SEC has taken steps to strengthen its information security program, most of the previously reported information security controls and program weaknesses persist. Specifically, the commission has corrected or mitigated 8 of the 51 weaknesses that GAO reported as unresolved in last year's report. Among the corrective actions SEC has taken include replacing a vulnerable, publicly accessible workstation and developing and implementing change control procedures for a major application. However, the commission has not yet effectively controlled remote access to its servers, established controls over passwords, managed access to its systems and data, securely configured network devices and servers, or implemented auditing and monitoring mechanisms to detect and track security incidents.

Overall, SEC has not effectively implemented information security controls to properly protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to the 43 previously reported weaknesses that remain uncorrected, GAO identified 15 new information security weaknesses. As illustrated in the figure below, most identified weaknesses pertained to electronic access controls such as user accounts and passwords, access rights and permissions, and network devices and services. These weaknesses increase the risk that financial and sensitive information will be inadequately protected against disclosure, modification, or loss, possibly without detection, and place SEC operations at risk of disruption.

A key reason for SEC's information security controls weaknesses is that the commission has not fully developed, implemented, or documented key elements of an information security program to ensure that effective controls are established and maintained. Until SEC implements such a program, its facilities and computing resources and the information that is processed, stored, and transmitted on its systems will remain vulnerable.

Information Security Weaknesses at SEC



Source: GAO.

^aPatch management helps mitigate software vulnerabilities

^bApplication change controls help ensure only authorized programs and modifications are implemented.

Contents

Letter

Results in Brief	1
Background	2
Objectives, Scope, and Methodology	4
SEC Has Made Limited Progress Correcting Previously Reported Weaknesses	6
Ineffective Controls Place Financial and Sensitive Data at Risk	7
Information Security Program Not Yet Fully Implemented at SEC	8
Conclusions	14
Recommendations for Executive Action	20
Agency Comments	21

Appendices

Appendix I: Comments from the Securities and Exchange Commission	23
Appendix II: GAO Contact and Staff Acknowledgments	26

Figure

Figure 1: Information Security Weaknesses at SEC	9
--	---

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
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 31, 2006

The Honorable Christopher Cox
Chairman, Securities and Exchange Commission

Dear Mr. Chairman:

The Securities and Exchange Commission (SEC) has a demanding responsibility enforcing securities laws, regulating the securities markets, and protecting investors. In enforcing these laws, SEC issues rules and regulations to provide protection for investors and to help ensure that the securities markets are fair and honest. The commission relies extensively on computerized systems to support its financial and mission-related operations.

Effective controls¹ over information security affect the integrity, confidentiality, and availability of sensitive information—such as personnel and regulatory information—maintained by SEC. These controls are essential to ensure that financial information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of our audit of SEC's fiscal year 2005 financial statements,² we assessed the effectiveness of SEC's information security controls over key financial systems, data, and networks. Our specific objectives were to assess (1) the status of SEC's actions to correct or mitigate previously reported weaknesses and (2) whether controls over key financial systems and data have been effective in ensuring the confidentiality, integrity, and availability of financial systems and data. We are also issuing a report³ for "Limited Official Use Only," which describes in more detail the information

¹Information security controls include electronic access controls, software change control, physical security, segregation of duties, and service continuity. These controls are designed to ensure that access to data is appropriately restricted, that only authorized changes to computer programs are made, that physical access to sensitive computing resources and facilities is protected, that computer security duties are segregated, and that backup and recovery plans are adequate to ensure the continuity of essential operations.

²GAO, *Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Years 2005 and 2004*, [GAO-06-239](#) (Washington, D.C.: Nov. 15, 2005).

³GAO, *Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, [GAO-06-407SU](#) (Washington, D.C.: Mar. 31, 2006).

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 June 2005 through October 2005. Our review was performed in accordance with generally accepted government auditing standards.

Results in Brief

Although SEC has taken steps to strengthen its information security program, most of the previously reported information security control weaknesses persist. Specifically, the commission has corrected or mitigated 8 of the 51 weaknesses that we previously reported as unresolved.⁴ Among actions SEC has taken include replacing a vulnerable, publicly accessible workstation and developing and implementing change control procedures for a major application. However, SEC did not effectively control remote access to its servers, establish controls over password composition and storage, or manage access to its systems and data. Further, the commission did not securely configure all its network devices and servers, nor did it implement auditing and monitoring mechanisms to detect and track security-relevant incidents.

Overall, SEC has not effectively implemented information security controls to properly protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to the remaining 43 previously reported weaknesses for which SEC has not completed corrective actions, we have identified 15 new information security weaknesses. For example, SEC has not consistently implemented effective electronic access controls over user accounts and passwords; access rights and permissions; network services and devices; and audit and monitoring of security-related events to prevent, limit, or detect access to its critical financial and sensitive systems and information. In addition, the commission has not effectively implemented certain other information

⁴GAO, *Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data*, GAO-05-263SU (Washington, D.C.: Mar. 23, 2005). GAO, *Information Security: Securities and Exchange Commission Needs to Address Weak Controls over Financial and Sensitive Data*, GAO-05-262 (Washington, D.C.: Mar. 23, 2005).

security controls relating to physical security, patch management,⁵ segregation of computer functions, and application change controls.⁶ Information security weaknesses—both old and new—continue to impair its ability to ensure the confidentiality, integrity, and availability of financial and other sensitive data.

A key reason for these information security weaknesses is that the commission had not fully developed, documented, and implemented elements for a comprehensive information security program. Although it has improved aspects of its program, such as increasing the number of security personnel, completing certification and accreditation of several major applications, and establishing a backup data center, it has not fully implemented other key elements. For example, SEC has not fully developed or documented policies and procedures related to (1) assessing risks, (2) testing and evaluating the effectiveness of controls, (3) reporting and tracking remedial actions, and (4) analyzing security incidents. Further, it could not ensure that all system users complied with training requirements. A fully implemented program is critical to providing SEC with a solid foundation for resolving existing information security problems and continuously managing information security risks.

To assist SEC in implementing an effective agencywide information security program, we are making recommendations to the SEC Chairman to direct the Chief Information Officer (CIO) to develop, document, and implement the commission's agencywide information security program.

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

In providing written comments on a draft of this report, the SEC Chairman stated that our recommendations are appropriate and actionable and that the Commission’s current efforts are focused on fully implementing them.

⁵Patch management is a critical process to help mitigate software vulnerabilities by using a work-around or patch to alleviate vulnerabilities.

⁶Application change controls help ensure only authorized programs and modifications are implemented.

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. It is especially important for government agencies, where the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, systems are unprotected from individuals and groups with malicious intent to intrude and use the access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. These concerns 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, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come.

Computer-supported federal operations are likewise at risk. 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. We have designated information security as a governmentwide high-risk area since 1997⁷—a designation that remains today.⁸

Recognizing the importance of securing federal information systems, in December 2002, Congress enacted the Federal Information Security Management Act (FISMA) to strengthen the security of information and systems within federal agencies.⁹ 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.

⁷GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

⁸GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

⁹FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002).

SEC Is a Key Protector of Securities Investors

Following the stock market crash of 1929, Congress passed the Securities Exchange Act of 1934,¹⁰ which established SEC to enforce securities laws, to regulate the securities markets, and to protect investors. In enforcing these laws, SEC issues rules and regulations to provide 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 commission 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. 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 \$888 million and staff of 3,865 to monitor and regulate the securities industry in fiscal year 2005. In 2003, the volume traded on U.S. exchanges and NASDAQ¹¹ 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, including annual reports from more than 12,000 reporting companies. In fiscal year 2005, SEC collected \$595 million for filing fees and \$1.6 billion 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.

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 such as filing fees paid by corporations and penalties from enforcement activities.

According to FISMA, the Chairman of SEC has responsibility for, among other things, (1) providing information security protections commensurate

¹⁰15 U.S.C. § 78d.

¹¹The National Association of Securities Dealers Automated Quotation System (NASDAQ) is an electronic stock market that uses a computerized system to provide brokers and dealers with price quotes.

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 CIO the authority to ensure compliance with the requirements imposed on the agency under FISMA. SEC's CIO is responsible for developing and maintaining a departmentwide information security program and for developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements.

Objectives, Scope, and Methodology

The objectives of our review were to assess (1) the status of SEC's actions to correct or mitigate previously reported information security and (2) the effectiveness of the commission's information system controls for ensuring the confidentiality, integrity, and availability of its information systems and information. Our evaluation was based on our Federal Information System Controls Audit Manual,¹² which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized data.

Specifically, we evaluated information security controls that are 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;
- prevent the exploitation of vulnerabilities;
- prevent the introduction of unauthorized changes to application or system software; and

¹²GAO, *Federal Information System Controls Audit Manual, Volume I-Financial Statements Audits*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

-
- ensure that work responsibilities for computer functions are segregated so that one individual does not perform or control all key aspects of computer-related operations and, thereby, have the ability to conduct unauthorized actions or gain unauthorized access to assets or records without detection.

In addition, we evaluated SEC's information security program. Such a program includes assessing risk; developing and implementing policies, procedures, and security plans; providing security awareness and training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; detecting, reporting, and responding to security incidents; and ensuring continuity of operations.

To evaluate SEC's information security controls and program, we identified and examined pertinent SEC security policies, procedures, guidance, security plans, and relevant reports. In addition, we conducted tests and observations of controls in operation and reviewed corrective actions taken by the commission to address vulnerabilities identified during our previous review.¹³ We also discussed whether information system controls were in place, adequately designed, and operating effectively with key security representatives, system administrators, and management officials.

SEC Has Made Limited Progress Correcting Previously Reported Weaknesses

Although SEC has taken steps to address its information security controls weaknesses, most of the weaknesses persist. Specifically, the commission has corrected or mitigated 8 of the 51 weaknesses that we previously reported as unresolved. For example, SEC has

- replaced a vulnerable, publicly accessible workstation with a terminal that provides the minimum capabilities needed to accomplish its purpose and a more secure configuration;
- developed and implemented procedures to ensure that changes made to a major financial system are reviewed, tested, and approved prior to implementation; and

¹³ GAO-05-263SU.

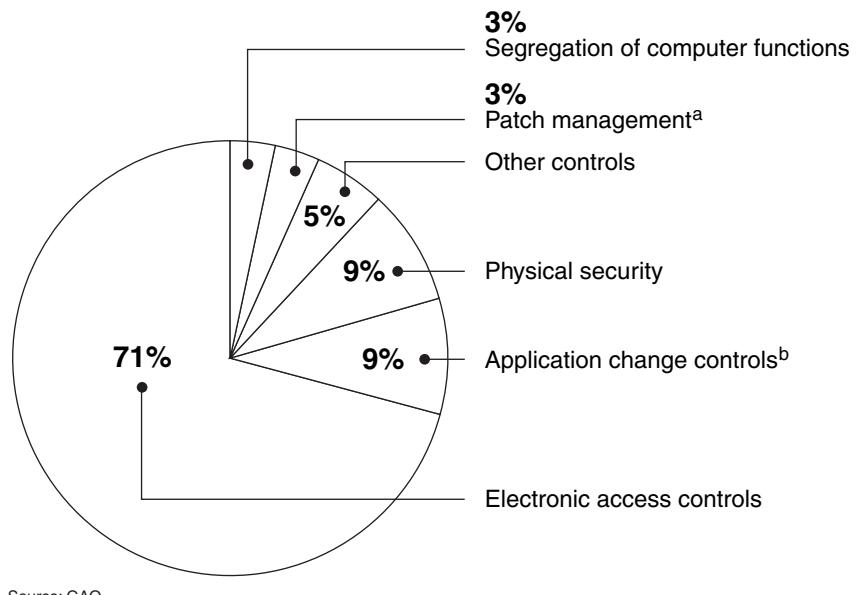
-
- hired contractors to appropriately segregate change management and security management functions for a major financial system.

While SEC has made some progress in strengthening its information security controls, it has not completed actions to correct or mitigate the remaining 43 of the 51 previously reported weaknesses. These weaknesses include allowing remote access to production servers via unauthorized accounts; permitting inadequate and insecure password storage and configuration; allowing excessive access rights to Windows servers, network system accounts, and sensitive information; and failing to adequately secure access to sensitive computing environments. Failure to resolve these issues will leave SEC's sensitive data and facilities vulnerable to unauthorized access, manipulation, and destruction.

Ineffective Controls Place Financial and Sensitive Data at Risk

SEC has not effectively implemented information security controls to properly protect the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to the 43 previously reported weaknesses that remain uncorrected, we identified 15 new information security weaknesses during this review. Most of the 58 identified weaknesses pertained to electronic access controls, as illustrated in figure 1. A primary reason for these weaknesses is that SEC has not yet fully implemented its information security program. As a result, weaknesses in controls over its financial and sensitive data increase the risk of unauthorized disclosure, modification, or destruction of data.

Figure 1: Information Security Weaknesses at SEC



Source: GAO.

^aPatch management helps mitigate software vulnerabilities.

^bApplication change controls help ensure only authorized programs and modifications are implemented.

Electronic Access Controls Were Not Always Effective

Protecting the resources that support critical operations from unauthorized access is a basic management objective for any organization. Organizations accomplish this objective by designing and implementing electronic controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information. Electronic access controls include user accounts and passwords, access rights and permissions, network services and devices, and audit and monitoring of security-related events. Inadequate electronic access controls diminish the reliability of computerized information, and they increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and of disruption of service.

User Accounts and Passwords

A computer system must be able to identify and differentiate 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 distinguishes 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, that is 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 for controlling access to the system.

Accordingly, agencies (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 has not adequately controlled user accounts and passwords to ensure that only authorized individuals are granted access to its systems and data. For example, SEC has not finalized policies and procedures to enforce strong password management or ensure the most appropriate and secure password settings are used. Similarly, it did not complete efforts to develop and implement a policy and process to prevent unauthorized remote access to security accounts. As a result, there is increased risk that unauthorized users could gain authorized user identification and password combinations to claim a user identity and then use that identity to gain access to SEC systems.

Access Rights and Permissions

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

SEC routinely permitted excessive access to the computer systems that support its critical financial and regulatory information. For example, SEC permitted users to modify sensitive information or critical system files and directories, although the users did not need such permissions to perform their job-related duties. Further, the commission did not implement a methodology to ensure that user rights were assigned on the basis of job function on all its servers. As a result, there is increased risk that SEC's financial and sensitive data and applications may be compromised.

Network Services and Devices	<p>Networks are collections of interconnected computer systems and devices that allow individuals to share resources such as computer programs and information. Because sensitive programs and information 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 networks, in part, by installing and configuring network devices that permit authorized network service requests, deny unauthorized requests, and limit the services that are available on the network. Devices used to secure networks include (1) firewalls that prevent unauthorized access to the network, (2) routers that filter and forward data along the network, (3) switches that forward information among segments 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. Because networks often include both external and internal access points for electronic information assets, failure to secure these assets increases the risk of unauthorized modification of sensitive information and systems, or of disruption of service.</p>
Audit and Monitoring of Security-Related Events	<p>SEC did not securely control network services to prevent unauthorized access to, and ensure the integrity of, SEC's computer networks, systems, and sensitive information. For example, SEC's network infrastructure was not securely configured, access to sensitive files on its network devices was not adequately controlled, and SEC workstations were not adequately configured. Further, SEC did not establish procedures for securing external connections to its network or provide guidance for implementing secure wireless networks. The commission's network security weaknesses could result in unauthorized and inappropriate access to SEC systems and sensitive information.</p> <p>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 are taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security events.</p>

SEC did not adequately audit and monitor security events. For example, SEC has not enabled audit trails for two of its financial applications; it has not deployed an effective intrusion detection system; and it does not have a process to analyze security incidents. In addition, at least two of the servers under our review lacked virus protection software. As a result, if a system were modified or disrupted, the commission's capability to trace or recreate events would be diminished.

Other Information System Controls Were Not Always Effective

In addition to electronic access controls, other important controls should be in place to ensure the security and reliability of an organization's data. These controls include policies, procedures, and control techniques to physically secure computer resources, prevent exploitation of vulnerabilities, appropriately segregate incompatible duties, and prevent unauthorized changes to application software. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of SEC's financial systems and sensitive information.

Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted in order to ensure that access continues to be appropriate. At SEC, physical access control measures (such as guards, badges, and locks—used alone or in combination) are vital to protecting the agency's sensitive computing resources from both external and internal threats.

SEC has taken steps to improve its physical security, such as relocating its headquarters operations to a newly constructed building that employs various technologies to control physical access. Further, SEC has recognized the need for physical security enhancements and has included a gated entry and an updated card access system in its future plans. However, SEC did not always effectively protect and control physical access to sensitive work areas in its facilities. For example, we found that many personnel at an SEC facility had unneeded access to the on-site computer room. Further, SEC did not always lock wiring closets and permitted individuals unnecessary access to the data center. Until SEC fully addresses its physical security vulnerabilities, there is increased risk that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

Patch Management

Patch management is a critical process that can help to alleviate many of the challenges of securing computing systems. As vulnerabilities in a system are discovered, attackers may attempt to exploit them, possibly causing significant damage. Malicious acts can range from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. When a software vulnerability is discovered, the software vendor may develop and make a patch or work-around to mitigate the vulnerability.

SEC does not have an effective patch management program. For example, SEC has not installed patches for critical vulnerabilities on two audit log servers and a network device. Because SEC has not installed and maintained the latest patches, its computing systems are more vulnerable to attackers taking advantage of outdated, less secure software.

Segregation of Computer Functions

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. This division of responsibilities 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 other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and computer resources could be damaged or destroyed.

Although SEC has taken action to enhance the segregation of incompatible security and change management functions for one of its financial applications, we identified instances in which duties were not adequately segregated to ensure that no individual had complete authority or system access. For example, SEC did not adequately segregate incompatible security and administrative functions within one of its financial applications. Specifically, financial management staff have been assigned roles that allow them to perform both security and systems administration duties for the application. Without adequate segregation of duties or appropriate mitigating controls, SEC is at increased risk that fraudulent activities could occur without detection.

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 necessary, 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, test procedures should be established to ensure that only authorized changes are made to the application's program code.

SEC did not establish and implement effective application change controls. For example, SEC did not finalize procedures to ensure that only authorized changes were made to the production version of application code for all applications. Further, SEC did not appropriately document the authorizations for software modifications, conduct independent reviews of software changes, or adequately control its software libraries. As a result, the risk of unauthorized, untested, or inaccurate application modifications is increased.

Information Security Program Not Yet Fully Implemented at SEC

SEC has made limited progress in developing and implementing the elements of FISMA's mandated information security program. In response to our prior recommendations, the commission has established a central security management group; appointed a senior information security officer to manage the program; increased the number of security personnel; certified and accredited several major applications; and established a backup data center for service continuity. However, other key elements of an information security program have not been fully or consistently developed, documented, or implemented for SEC's information systems. A key reason for SEC's information security controls weaknesses is that the commission has not fully developed or implemented an information security program to ensure that effective controls are established and maintained. Without a strong information security program, SEC cannot protect its information and its information systems.

FISMA¹⁴ requires agencies to develop, document, and implement an information security program that includes the following:

¹⁴FISMA 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, including those operated or maintained by contractors or others on behalf of the agency, using a risk-based approach to information security management.

-
- periodic assessments of the risk and the magnitude of 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;
 - 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 that is identified in the agencies' inventories;
 - a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in their information security policies, procedures, or practices;
 - procedures for detecting, reporting, and responding to security incidents; and
 - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Risk Assessments

Identifying and assessing information security risks are essential steps in determining what controls are required. Moreover, by increasing awareness of the risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. Further, Office of Management and Budget (OMB) Circular A-130, appendix III, prescribes that risk be reassessed when significant changes are made to computerized systems—or at least every 3 years.

Although SEC had risk assessments for the systems we reviewed, it did not follow a documented process for risk assessments. Specifically, SEC did not have policies and procedures on how to perform risk assessments. Until the commission's risk assessment process is completed and

institutionalized, risks may not be adequately assessed and countermeasures may not be properly identified. As a result, inadequate or inappropriate security controls may be implemented that do not address the system's true risk and efforts to implement effective controls later on may be more costly.

Policies and Procedures

Another key task in developing, documenting, and implementing an effective information security program is to establish and implement risk-based policies, procedures, and technical standards that cover security over an agency's computing environment. If properly implemented, policies and procedures can help to reduce the risk that could come from unauthorized access or disruption of services. Because security policies are the primary mechanism by which management communicates its views and requirements, it is important to establish and implement them.

SEC had no finalized policies governing its information security program. Since the completion of our review, SEC has finalized SEC Regulation 24-04, the first level of its policy framework that provides high-level policy, requirements, and governance for security over its information systems. However, policies and procedures for password management, remote access to security accounts, external connections to networks, application change controls, and patch management remain in draft. As a result, SEC has less assurance that its systems and information are sufficiently protected.

Security Awareness Training

Another FISMA requirement for an information security program is that it promote awareness and provide required training for users so that they can understand the system security risks and their role 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 and contractors who use computer resources in their day-to-day operations be 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 who use agency information systems be provided with periodic training in information security awareness and accepted information security practice. SEC policy requires that employees and contractors take annual security awareness training.

SEC could not ensure that all system users complied with the annual security awareness training requirement. The training contractor who

provided information security awareness training supplied SEC with training reports that contained reporting inaccuracies, making it difficult for SEC to determine if its users had complied with the training requirement. After the completion of our review, SEC contracted with a new vendor for security awareness training and is striving to meet its goal of 100 percent compliance for all employees, contractors, and agency detailees. Until SEC can ensure that each employee, contractor, and agency detailee receives annual security awareness training, security lapses due to user activity are more likely to occur.

Tests and Evaluations of Control Effectiveness

Testing and evaluating systems is a key element of an information security program that ensures that an agency is 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 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, but occur no less than annually.

SEC lacks a program to test and evaluate the effectiveness of information system controls. SEC conducts security tests and evaluations as part of its certification and accreditation process,¹⁵ which is required every 3 years or when significant changes occur to the system. However, SEC had not

¹⁵Certification 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.

completed testing of its security controls in its general support system.¹⁶ SEC's Inspector General noted in its latest FISMA report¹⁷ that the general support system is a critical security component for all of SEC's major applications. The effectiveness of the general support system controls is a significant factor in the effectiveness of security controls for its major applications. Since the commission has not tested the security controls in the general support system, it cannot be assured that tests and evaluations are sufficient to assess whether its security policies and controls are appropriate and working as intended.

Remedial Actions

Remedial action plans are a key component described in FISMA. They assist agencies in identifying, assessing, prioritizing, and monitoring the progress in correcting security weaknesses that are found in information systems. According to OMB Circular A-123, agencies should take timely and effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, remedial action plans should be developed for each deficiency and progress should be tracked for each.

SEC has not developed a reporting and tracking mechanism for its remedial action plans. Further, our review of remedial action plans for five of the applications certified and accredited during fiscal year 2005 noted that some of the control deficiencies had been labeled "waiver granted" and therefore had been exempted from remedial actions. The waivers had been granted based on future plans to replace the application or other cost-based reasons. However, the remedial plans lacked complete justifications, risk mitigation, and cost-benefit analysis for the deficiencies that had been waived. Nevertheless, these applications had been certified and accredited and granted full authority to operate. As a result, SEC did not have assurance that all known information security weaknesses had been mitigated or corrected.

Incident Handling

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they

¹⁶A 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.

¹⁷SEC OIG, *2005 FISMA Executive Summary Report* (Washington, D.C.: Sept. 23, 2005).

promptly take steps to detect and respond to them before significant damage is done. In addition, accounting for and analyzing security problems and incidents are effective ways for organizations to gain a better understanding of the threats to their information and the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. Problem and incident reports can provide valuable input for risk assessments, can help in prioritizing security improvement efforts, and can be used to illustrate risks and related trends for senior management.

SEC does not have a program to handle security incidents. The commission has drafted an incident response program plan that provides general guidance on handling security incidents; however, it lacks a comprehensive program to collect, document, and analyze incident information to determine if trends exist that could be mitigated through user awareness, training, or the addition of technical security controls. As previously reported, SEC has acknowledged the importance of security incident reporting and analysis, however, it does not perform trend analysis of its security incidents. Until SEC formalizes its process for handling security incidents, it remains at risk of not being able to detect or respond quickly to them.

Continuity of Operations

Continuity of operations 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 accomplished some elements of disaster recovery planning, but it did not complete all the tasks necessary to establish and maintain an effective continuity of operations program. To its credit, SEC set up a backup data center in a separate contractor facility to replicate its operations center functionality and has drafted contingency plans for many of its major applications, so that recovery steps are documented in the event of a disaster. SEC also conducted a partially successful test to validate the sufficiency of the plans and assess SEC's ability to recover operations. However, SEC successfully tested the recovery of only 12 of 20 of its major

applications. Despite SEC's accomplishments in the disaster recovery area, SEC must test its service continuity plans to ensure its ability to continue and/or recover operations in the event of a disaster.

Conclusions

Information security weaknesses—both old and new—continue to impair SEC's ability to ensure the confidentiality, integrity, and availability of financial and other sensitive data. While the commission has made some progress in addressing our previous recommendations, the many outstanding weaknesses place its systems at risk. Until SEC fully develops, documents, and implements a comprehensive agencywide information security program that includes enhanced policies, procedures, plans, training, and continuity of operations, its facilities and computing resources and the information that is processed, stored, and transmitted on its systems will remain vulnerable to unauthorized access, modification, or destruction.

Recommendations for Executive Action

To help establish effective information security over key financial systems, data, and networks, we recommend that the SEC Chairman direct the Chief Information Officer to take the following seven actions to fully develop, document, and implement an effective agencywide information security program:

- Fully document and implement a process for assessing risks for its information systems.
- Finalize comprehensive information security policies and procedures.
- Ensure that all system users comply with annual security awareness training requirements.
- Institute a testing and evaluation program that includes testing the controls within the general support system.
- Develop a mechanism to track remedial action plans that incorporates all identified weaknesses and related risks.
- Establish a program for handling security incidents with detection, response, analysis, and reporting capabilities.

-
- Maintain a continuity of operations program that includes fully tested plans for restoring operations.

We are also making additional recommendations in a separate report designated for “Limited Official Use Only.” These recommendations address actions needed to correct 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, the SEC Chairman agreed with our recommendations. Specifically, he stated that our recommended actions are appropriate and actionable and that SEC’s current efforts are focused on fully implementing them. The Chairman’s comments are reprinted in appendix I of this report.

The Chairman’s comments also addressed several achievements in advancing SEC’s information security program, including certifying and accrediting 16 of 20 major applications, implementing a new automated system for tracking plans of action and milestones, and successfully testing continuity of operations planning efforts for 12 major applications. He also highlighted SEC’s annual security awareness training compliance rate exceeding 90 percent and a new computer security incident response team in place to implement and test SEC’s incident response program.

The Chairman stated that he has identified information security as the commission’s highest information technology priority and will continue to implement corrective actions. SEC plans to complete the corrective actions for specific weaknesses we identified, as well as implement recommended information security program enhancements to address the agency’s program deficiencies.

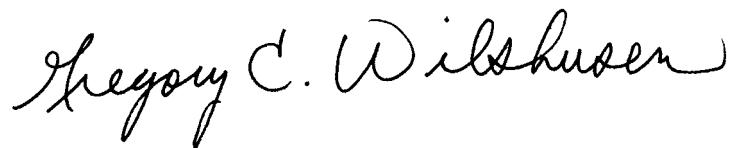
This report contains recommendations to you. As you know, 31 U.S.C. 720 requires that the head of a federal agency submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Government Reform 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 us 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 on 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 will also 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) 512-6244 or by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Sincerely yours,

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is fluid and cursive, with "Gregory" on top, "C." in the middle, and "Wilshusen" on the bottom line.

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 24, 2006

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

Dear Mr. Wilshusen:

Thank you for the opportunity to respond to the draft report entitled, *Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, dated March 2006. This audit was conducted in conjunction with the Government Accountability Office (GAO) audit of the SEC's fiscal year 2005 financial statements and reflects the state of our information security program as of September 30, 2005. The GAO has identified a number of information security issues at the SEC which we are now moving to address. We appreciate the GAO's acknowledgement that the SEC has made progress in addressing a number of issues. We are also glad to see that, in most cases, this year's issues are ones to which we have already committed significant effort and which are well-positioned to be resolved in the coming months.

In the audit, the GAO identified internal control issues resulting from our having not fully developed and implemented a comprehensive program to manage information security. Thus, despite significant effort in the preceding year to fix known weaknesses, gaps in our overall security management processes, policies, and procedures allowed for problems to recur. We appreciate the detailed set of recommendations developed by the GAO team, and we intend to use the results to continue to guide improvements to the SEC's information security program and other program areas.

During the several months since the conclusion of the GAO audit, the SEC has taken significant strides in advancing its information security program. Our achievements include:

- Completing certification and accreditation for the general support systems; this brings the number of major applications certified and accredited to sixteen. The remaining four major applications are on track to be accredited during the spring;

Appendix I
Comments from the Securities and Exchange
Commission

Mr. Gregory C. Wilshusen
Page 2

- Maintaining and tracking our “plans of action and milestones” via a new automated system;
- Completing successful disaster recovery testing for twelve major applications and numerous other applications utilizing the SEC alternate data center to ensure continuity of operations for our information systems;
- Attaining over 90 percent completion for yearly security awareness training, as well as conducting events and implementing policies to improve security awareness; and
- Implementing and testing an incident response program under our newly established computer security incident response team.

We believe the GAO’s recommendations are appropriate and actionable, and we are focusing our current efforts on implementing them fully. 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. During the remainder of fiscal year 2006, we will:

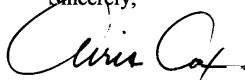
- Complete corrective actions for the specific weaknesses identified in the 2004 and 2005 reviews; and
- Continue to enhance the SEC’s information security program by:
 - Directing the SEC’s Chief Information Officer to fully implement the agency-wide information security program;
 - Fully documenting and implementing a process for assessing information systems risk;
 - Implementing a comprehensive set of information security policies and procedures;
 - Achieving full compliance with annual security awareness training for users;
 - Commencing a test and evaluation program for our security controls, including those in the general support systems (the overall SEC IT infrastructure);
 - Systematically tracking our remedial action plans to mitigate risk;
 - Instituting a comprehensive process for security incident handling; and
 - Refining and testing a continuity of operations program.

Appendix I
Comments from the Securities and Exchange
Commission

Mr. Gregory C. Wilshusen
Page 3

Overall, we continue to rate information security as our highest information technology priority and are grateful for extremely strong levels of support and frequent involvement from the entire Commission in our efforts. We look forward to working with the GAO on an ongoing basis as we continue to enhance our security program.

If you have questions relating to the SEC management response, please contact me at 202-551-2100.

Sincerely,

Christopher Cox
Chairman

GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244

Staff Acknowledgments

In addition to the individual named above, Suzanne Lightman, Assistant Director; Jason Carroll; Lon Chin; West Coile; Anh Dang; Kristi Dorsey; Nancy Glover; Kenneth Johnson; Stephanie Lee; 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

Order by Mail or Phone

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (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 and select "Subscribe to Updates."

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

E-mail: fraudnet@gao.gov

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

Congressional Relations

Gloria Jarmon, Managing Director, 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 (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548
