United States Government Accountability Office

GAO

Report to the Chairman, Securities and Exchange Commission

March 2007

INFORMATION SECURITY

Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission

GAO
Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-07-256, a report to the Chairman, Securities and Exchange Commission

March 2007

INFORMATION SECURITY

Sustained Progress Needed to Strengthen Controls at the 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. Integrating effective information security controls into a layered control strategy is 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) SEC's actions to correct previously reported information security weaknesses and (2) the effectiveness of controls for ensuring the confidentiality, integrity, and availability of SEC's 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 the SEC Chairman improve the implementation of its policies and procedures, control tests and evaluations, and remedial action plans as part of its agencywide information security program.

In commenting on a draft of this report, SEC stated that it will actively work to implement GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-256.

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

What GAO Found

SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 58 of the 71 weaknesses previously reported as unresolved at the conclusion of GAO's 2005 audit. The commission resolved all of the previously reported weaknesses in security related activities and contingency planning, and made significant progress in resolving access control weaknesses. A key reason for its progress was that SEC's senior management was actively engaged in implementing information security related activities.

Despite this progress, SEC has not consistently implemented certain key controls to effectively safeguard the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to 13 previously identified weaknesses that remain unresolved, 15 new information security weaknesses were identified. By the conclusion of GAO's review, SEC took action to address 11 of the 15 new weaknesses. A primary reason for these control weaknesses is that SEC had not consistently implemented elements of its information security program. This included inconsistent implementation of agency policies and procedures, not sufficiently testing and evaluating the effectiveness of controls for a major system as required by its certification and accreditation process, and not consistently taking effective and timely action to correct deficiencies identified in remedial action plans. Until SEC does, it will have limited assurance that it will be able to manage risks and protect sensitive information on an ongoing basis.

Contents

Abbreviations

CATS	Case Activity Tracking System 2000
CIO	chief information officer
CISO	chief information security officer
EDGAR	Electronic Data Gathering, Analysis, and Retrieval system
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
SEC	Securities and Exchange Commission

G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

March 27, 2007

The Honorable Christopher Cox
Chairman, Securities and Exchange Commission

Dear Mr. 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 maintain fair, orderly, and efficient securities markets. To support its demanding financial and mission-related responsibilities, the commission relies extensively on computerized systems.

Integrating effective information security controls[1] into a layered control strategy is essential to ensure that financial and sensitive information—such as personnel and regulatory information maintained by SEC—is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of our audit of SEC's fiscal year 2006 financial statements,[2] we assessed the effectiveness of the commission'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 information security weaknesses and (2) the effectiveness of the commission's information system controls for ensuring the confidentiality, integrity, and availability of its information systems and information.

In our report on SEC's financial statements for fiscal years 2006 and 2005,[3] we reported that the new information security deficiencies we identified in

[1] Information security controls include access controls, configuration management, segregation of duties, and contingency planning. These controls are designed to ensure that access to data is appropriately restricted, only authorized changes to computer programs are made, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations.

[2] GAO, *Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Years 2006 and 2005*, GAO-07-134 (Washington, D.C.: Nov. 15, 2006).

[3] GAO-07-134.

fiscal year 2006 and the unresolved deficiencies from prior audits represented a reportable condition[4] in internal controls over the commission's information systems.

We performed our work at SEC headquarters in Washington, D.C., and at its computer facility in Alexandria, Virginia, from May 2006 through November 2006 in accordance with generally accepted government auditing standards.

Results in Brief

SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 58 of the 71 weaknesses previously reported as unresolved at the conclusion of our 2005 audit. The commission resolved all of the previously reported weaknesses in security related activities and contingency planning, and it made significant progress in resolving access controls weaknesses. A key reason for its progress was that SEC's senior management was actively engaged in implementing information security related activities, including establishing policies and procedures for risk management, ensuring that all users complete security training, and developing an incident response program.

Despite this progress, SEC has not consistently implemented key controls to effectively safeguard the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to 13 previously identified weaknesses that remain unresolved, we identified 15 new information security weaknesses pertaining to SEC's access controls and configuration management. For example, SEC did not have current documentation on the privileges granted to users of a major application, did not securely configure certain system settings, or has not consistently installed all patches to its systems. As a result, the commission's financial and sensitive data are at increased risk of unauthorized disclosure, modification, or destruction.

A primary reason for these control weaknesses is that SEC had not consistently implemented elements of its information security program. Agency policies and procedures were not consistently implemented across the agency. In addition, the commission did not sufficiently test and

[4] A reportable condition represents a significant design or operational deficiency that could adversely affect an agency's ability to meet its internal control objectives.

evaluate the effectiveness of controls for a major system as required by its certification and accreditation process. The commission also did not take effective and timely action to correct deficiencies identified in remedial action plans. If SEC does not continue to sustain the progress it has made to improve its information security program, it will not have sufficient assurance that its processes can mitigate known weaknesses and protect sensitive information on an ongoing basis.

We are making recommendations to the SEC Chairman to assist the commission in improving the implementation of its policies and procedures, control tests and evaluations, and remedial action plans as part of its agencywide information security program.

In a separate report designated “Limited Official Use Only”,[5] we are also making 18 recommendations to address actions needed to correct 15 information security weaknesses. By the conclusion of our review, SEC took action to address 11 of the 15 new information security weaknesses.

In providing written comments on a draft of this report, the SEC Chairman and Chief Information Officer agreed that the agency needs to maintain momentum addressing the remaining gaps in its information security program and stated that it is actively working to complete corrective actions for findings that remain open and enhance its information security program by implementing our recommendations.

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 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,

[5] GAO, *Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission*, GAO-07-257SU (Washington, D.C.: Mar. 27, 2007).

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 reports by several agencies' inspectors general describe persistent information security weaknesses that place a variety of federal operations at risk of inappropriate disclosure, fraud, and disruption. We have designated information security as a governmentwide high-risk area since 1997.[6]

Recognizing the importance of securing the information systems of federal agencies, Congress enacted the Federal Information Security Management Act (FISMA)[7] in December 2002. FISMA requires each agency to develop, document, and implement an agencywide information security program for the data and systems that support the operations and assets of the agency, using a risk-based approach to information security management. Information security program requirements to be implemented include 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.

SEC's Role as Protector of Securities Investors

Following the stock market crash of 1929, Congress passed the Securities Exchange Act of 1934,[8] establishing SEC to enforce securities laws, regulate the securities markets, and protect investors. To carry out its responsibilities and help ensure that fair, orderly, and efficient securities markets are maintained, the commission issues rules and regulations that promote 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

[6] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997); GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

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

[8] 15 U.S.C. § 78d.

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 2006, SEC had a budget of about $888 million and staff of 3,590. Each year the commission accepts, processes, and publicly disseminates more than 600,000 documents from companies and individuals, including annual reports from more than 12,000 reporting companies. In fiscal year 2006, the commission collected $499 million in filing fees and $1.8 billion in penalties and disgorgements.[9] To support its financial operations and store the sensitive information it collects, the commission relies extensively on computerized systems interconnected by local and wide area networks. To process and track financial transactions such as filing fees paid by corporations and penalties from enforcement activities, SEC relies on several applications—Momentum, Electronic Data Gathering, Analysis, and Retrieval system (EDGAR), and Case Activity Tracking System 2000 (CATS). Momentum, a commercial off-the-shelf accounting software product, is used to record the commission's accounting transactions, to maintain its general ledger, and to maintain the information SEC uses to produce financial reports. EDGAR is an Internet-based system used to collect, validate, index, and accept the submissions of forms filed by SEC-registered companies. EDGAR transfers this information to the general ledger nightly. The commission's Division of Enforcement uses CATS, a modified commercial off-the-shelf database application, to record enforcement data and create management reports. CATS tracks enforcement-related data, including SEC-imposed fines and penalties. In addition, the commission uses these systems to maintain sensitive information, including filing data for corporations, and legal information on enforcement activities.

According to FISMA, the Chairman of the SEC has responsibility for 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. The Chairman of the SEC delegated authority to the chief information officer (CIO) to be responsible for establishing and maintaining a comprehensive information security

[9] A disgorgement is the repayment of illegally gained profits (or avoided losses) for distribution to harmed investors whenever feasible.

program and governance framework. As part of its program, the CIO is to (1) ensure that policies, procedures, and control techniques to address all applicable information security requirements are effectively implemented and maintained; (2) work closely with designated authorizing officials to ensure that the SEC-wide program is effectively implemented and managed; and (3) delegate authority to the agency chief information security officer (CISO) to carry out information security responsibilities and to ensure compliance with applicable federal laws, regulations, and standards. The CISO serves as the CIO's liaison with system owners and authorizing officials to ensure the agency security program is effectively implemented. The CISO also ensures certifications and accreditations are accomplished in a timely and cost-effective manner and that there is centralized reporting of all information security related activities.

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 weaknesses and (2) the effectiveness of the commission's information system controls for ensuring the confidentiality, integrity, and availability of its information systems and information. As part of our assessment of the effectiveness of SEC's information system controls, we also evaluated the commission's progress toward meeting the requirements for an agencywide security program mandated by FISMA.

We conducted our review using our Federal Information System Controls Audit Manual (FISCAM),[10] a methodology for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized data. Specifically, we evaluated information security controls in the following areas:

- *security management*, which provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the agency's computer-related controls;

- *access controls*, which limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure;

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

- *configuration management*, which prevents unauthorized changes to information system resources (for example, software programs and hardware configurations);

- *segregation of duties*, which includes policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations; and

- *contingency planning*, so that when unexpected events occur, critical operations continue without disruption or are promptly resumed, and critical and sensitive data are protected.

For our first objective, we examined supporting documentation and conducted tests and evaluations of corrective actions taken by the commission to correct weaknesses previously reported as unresolved at the conclusion of our 2005 audit.[11]

To evaluate the effectiveness of the commission's information security controls and program, we identified and examined its pertinent security policies, procedures, guidance, security plans, and relevant reports. Where federal requirements, laws, and other guidelines, including National Institute of Standards and Technology guidance, were applicable, we used these to assess the extent to which the commission had complied with specific requirements. We held discussions with key security representatives, system administrators, and management officials to determine whether information system controls were in place, adequately designed, and operating effectively. In addition, we conducted tests and observations of controls in operation using federal guidance, checklists and vendor best practices.

[11] GAO, *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); GAO, *Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, GAO-06-407SU (Washington, D.C.: Mar. 31, 2006); GAO, *Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program*, GAO-06-408 (Washington, D.C.: Mar. 31, 2006).

SEC Has Made Important Progress Correcting Previously Reported Weaknesses

SEC has corrected or mitigated 58 of the 71 security control weaknesses previously reported as unresolved at the conclusion of our 2005 audit. Specifically, the commission resolved all of the previously reported weaknesses in security related activities and contingency planning, and it has made significant progress in resolving access control weaknesses. A key reason for SEC's progress was that its senior management was actively engaged in implementing information security related activities and mitigating the previously reported weaknesses.

The commission has addressed 34 of the previously identified access control weaknesses. For example, SEC has

- implemented controls to enforce strong passwords, and removed excessive rights granted to certain users on their Microsoft Windows servers and workstations;
- established audit trails on its critical financial systems;
- reconfigured its internal network infrastructure to be configured securely;
- implemented virus protection on all of its Microsoft Windows servers;
- developed and implemented procedures to review employee and contractor access to the data center based on SEC-established criteria;
- assessed the physical security of each of its 11 field office locations and developed a plan to review each of the offices biannually; and
- developed an incident response program that includes policies and procedures for handling and analyzing incidents.

SEC has also corrected or mitigated all 18 security related activity weaknesses previously reported as unresolved at the conclusion of our 2005 audit. For example, the commission has

- implemented a risk assessment process;
- established a process to ensure that effective information system controls exist to safeguard its payroll/personnel system;
- had 99 percent of employees and contractors complete security awareness training;

- developed and documented a process to ensure background investigations were conducted for employees and contractors; and
- established a process to identify and remove computer access rights accounts granted to separated contractors or nonpaid users of SEC systems.

In addition, SEC has developed and updated its disaster recovery plans covering major applications. Moreover, the commission has tested its plans throughout the year through a series of disaster recovery exercises covering major applications and various scenarios.

A key reason for its progress was that SEC's senior management was actively engaged in implementing information security related activities and mitigating the previously reported weaknesses. The Chairman has received regular briefings on agency progress in resolving the previously reported weaknesses, and the CIO has coordinated efforts with other offices involved in implementing information security policies and controls at the commission. An executive-level committee with oversight responsibility for the commission's internal controls was also established and has responsibility for approving programs and policies for internal control assessment and testing as well as developing policies to resolve internal control weaknesses.

While SEC has made important progress in strengthening its information security controls and program, it has not completed actions to correct or mitigate 13 previously reported weaknesses. For example, the commission has not mitigated weaknesses in user account and password management, periodically reviewed software changes, or adequately controlled access to sensitive information. Failure to resolve these issues will leave the commission's sensitive data vulnerable to unauthorized disclosure, modification, or destruction.

Key Controls Were Not Consistently Implemented

SEC has not consistently implemented certain key controls to effectively safeguard the confidentiality, integrity, and availability of its financial and sensitive information and information systems. In addition to 13 previously identified weaknesses that remain unresolved, we identified 15 new information security weaknesses in access controls and configuration management. By the conclusion of our review, SEC had taken action to address 11 of the 15 new weaknesses. A primary reason for these control weaknesses is that SEC had not consistently implemented elements of its information security program. As a result, the commission cannot be assured that its controls are appropriate and working as intended and that its financial and sensitive data and systems are not at increased risk of unauthorized disclosure, modification, or destruction.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized disclosure, modification, and loss. Specific access controls include boundary protection, identification and authentication, authorization, 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 their span of authority.

Boundary Protection

Boundary protection pertains to the protection of a logical or physical boundary around a set of information resources and implementing measures to prevent unauthorized information exchange across the boundary in either direction. Organizations physically allocate publicly accessible information system components to separate subnetworks with separate physical network interfaces, and they prevent public access into their internal networks. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but the risk of unauthorized access in a shared environment. SEC policy requires that certain automated boundary protection mechanisms be established to control and monitor communications at the external boundary of the information system and at key internal boundaries within the system. Additionally, SEC policy requires that if remote access technology is used to connect to the network, it must be configured securely.

The commission did not configure a remote access application to include required boundary protection mechanisms. For example, the application was configured to allow simultaneous access to the Internet and the internal network. This could allow an attacker who compromised a remote user's computer to remotely control the user's secure session from the Internet. In addition, SEC did not securely configure the systems used for remote administration of its key information technology resources. Consequently, a remote attacker could exploit these vulnerabilities to launch attacks against other sensitive information systems within the commission.

Identification and Authentication

A computer system must be able to identify and authenticate different 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. SEC policy requires the implementation of automated identification and authentication mechanisms that enable the unique identification of individual users.

The commission did not securely enforce identification and authentication controls on all of its information systems. For example, SEC did not remove default database accounts with known or weak passwords or ensure that these accounts had been locked. In addition, the commission was still unable to enforce strong password management on all of its systems and continued to have weak key-management practices for some of its secure connections. This increases the risk that unauthorized users could gain access to SEC systems and sensitive information.

Authorization

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 the concept of "least privilege." Least privilege is a basic principle for securing computer resources and data. It 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. SEC policy requires that each user or process be assigned only those privileges needed to perform authorized tasks.

SEC system administrators did not ensure that their systems sufficiently restricted system and database access and privileges to only those users and processes requiring them to perform authorized tasks. For example, administrators had not properly restricted access rights to sensitive files on some servers. Nor did the commission adequately restrict privileges to a system database. In addition, new requests or modifications for user access to the EDGAR system were not reviewed by its system owner; nor was current documentation maintained on user privileges granted to individuals based on their roles and divisions. The commission also continued to experience difficulty implementing a process to effectively remove network system accounts from separated employees and adequately controlling access to sensitive information. These conditions provide more opportunities for unauthorized individuals to escalate their privileges and make unauthorized changes to files.

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 policy requires that specific procedures be followed to protect and control physical access to sensitive work areas in its facilities.

SEC procedures for protecting and controlling physical access to sensitive work areas were not always followed. Specifically, the commission had not properly implemented perimeter security at a key location. Guards at the location did not inspect photo identification and expiration dates. In addition, the commission did not adequately restrict physical access to its network in public locations. 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.

Configuration Management

To protect an organization's information, it is important to ensure that only authorized applications and programs are placed in operation and that the applications are securely configured. This process, known as configuration management, consists of instituting policies, procedures, and techniques to help ensure that all programs and program modifications are properly authorized, tested, and approved. Specific controls for configuration management include policies and procedures over change control and patch management. Configuration management policies and procedures should be developed, documented, and implemented at the agency, system, and application levels to ensure an effective configuration management process. Patch management, including up-to-date patch installation, helps to mitigate vulnerabilities associated with flaws in software code, which could be exploited to cause significant damage. SEC policy requires vulnerability management of system hardware and software on all of its information systems.

SEC continues to have difficulty implementing effective control over changes to software and other applications. For example, the commission lacked procedures to periodically review application code to ensure that only authorized changes were made to the production environment, did not document authorizations for software modifications, and did not always follow its policy of assigning risk classifications to application changes. As a result, unapproved changes to SEC production systems could be made.

In addition, the commission did not ensure the application of timely and comprehensive patches and fixes to system software. For example, the commission did not consistently install critical patches for the operating system and third-party applications on its servers and end-user workstations. Failure to keep system patches up-to-date could allow unauthorized individuals to gain access to network resources or launch denial-of-service attacks against those resources. A malicious user can exploit these vulnerabilities to gain unauthorized access to network resources or disrupt network operations. As a result, there is increased risk that the integrity of these network devices and administrator workstations could be compromised.

Information Security Program Not Yet Consistently Implemented

A primary reason for these control weaknesses is that SEC had not consistently implemented elements of its information security program. The effective implementation of an information security program includes implementing the key elements required under FISMA and the establishment of a continuing cycle of activity—which includes assessing risk, developing and implementing security procedures, and monitoring the effectiveness of these procedures—to ensure that the elements implemented under the program are effective. FISMA requires agencies to develop, document, and implement an information security program, which includes the following:

- developing and implementing policies and procedures;
- testing and evaluating the effectiveness of controls; and

- planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies.

Policies and Procedures

A 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 document and implement them.

Although SEC has developed and documented information security related policies and procedures, it has not consistently implemented them across all systems. According to SEC policy, heads of office and system owners are responsible for implementing policies and procedures as well as reviewing and enforcing security for their systems. However, our analysis showed that 13 of the 15 newly identified weaknesses were due to the inconsistent implementation of policies and procedures by the system owners and offices. Until the commission can verify that all system owners and offices implement agency policies and procedures, it will not have assurance that requirements are being followed and controls will work as intended.

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 the 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 risk, but occur no less than annually.

SEC did not sufficiently test and evaluate the effectiveness of controls for a major system as required by its certification and accreditation process. When the general ledger system underwent a significant change, agency policy required that the system undergo recertification and reaccreditation, which included system testing and evaluation of controls. However, SEC did not complete recertification and reaccreditation testing of controls for the system. We identified three control weaknesses associated with the change to the general ledger system that SEC had not detected. Since the commission has not completed sufficient testing and evaluation for the general ledger system after it underwent a significant change, it cannot be assured that its security policies and controls are appropriate and working as intended.

Remedial Actions

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

Although SEC developed remedial action plans to mitigate identified weaknesses in its systems and developed a mechanism to track the progress of actions to correct deficiencies, it did not consistently take effective and timely action to do so. Our analysis showed that 7 of the 15 new weaknesses had been previously identified in remedial action plans. Of the 7 weaknesses, 4 were not effectively mitigated, although SEC noted that they had been closed in prior year remedial action plans. Another known weakness had been listed in a remedial action plan since April 2004. This existed in part because until recently, system remedial action plans did not have completion dates for all deficiencies. These inconsistencies exist because the commission did not develop, document, and implement a policy on remedial action plans to ensure deficiencies were mitigated in an effective and timely manner. As a result, SEC will have limited assurance that all known information security weaknesses are mitigated or corrected in an effective and timely manner.

Conclusions

Public trust is vital to the proper functioning of the securities markets. Because SEC relies heavily on computerized systems to maintain fair, orderly, and efficient securities markets, the security of its financial and sensitive data is paramount. While the commission has made important progress in addressing our previous information security recommendations and strengthening its information security program, both outstanding and newly identified weaknesses continue to impair SEC's ability to ensure the confidentiality, integrity, and availability of financial and other sensitive data. Accordingly, these deficiencies represent a reportable condition in internal controls over SEC's information systems.

Sustained senior management involvement and oversight are vital for SEC's newly developed security program to undergo the continuous cycle of activity required for the effective development, implementation, and monitoring of policies and procedures. If the commission continues to have senior management actively engaged and continues to implement a framework and continuous cycle of activity, it will help ensure that outstanding weaknesses are mitigated or resolved and that key controls are consistently implemented. If progress is not sustained, SEC will not have sufficient assurance that its processes can mitigate current weaknesses and detect new weakness, and its financial and sensitive data will remain at risk of unauthorized disclosure, modification, or destruction.

Recommendations for Executive Action

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

1. verify that all system owners and offices implement agency security policies and procedures;

2. complete recertification and reaccreditation testing and evaluation on the general ledger system;

3. develop, document, and implement a policy on remedial action plans to ensure deficiencies are mitigated in an effective and timely manner.

In a separate report designated "Limited Official Use Only",[12] we also made 18 recommendations to the SEC Chairman to address actions needed to correct 15 information security weaknesses.

[12] GAO-07-257SU.

Agency Comments

In providing written comments on a draft of this report, the SEC Chairman and Chief Information Officer agreed that the agency needs to maintain momentum addressing the remaining gaps in its information security program and stated that it is actively working to complete corrective actions for findings that remain open and enhance its information security program by implementing our recommendations.

They also identified several actions the agency has completed to resolve known weaknesses and stated that going forward the commission's primary focus will be on making its information security program more aggressive in identifying and resolving issues as or before they arise, to ensure high levels of security compliance across the agency. Their written comments are reprinted in appendix I.

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 Oversight and 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 recommendation.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Banking, Housing, and Urban Affairs; Senate Committee on Homeland Security and Governmental Affairs; House Committee on Financial Services; House Committee on Oversight and 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.

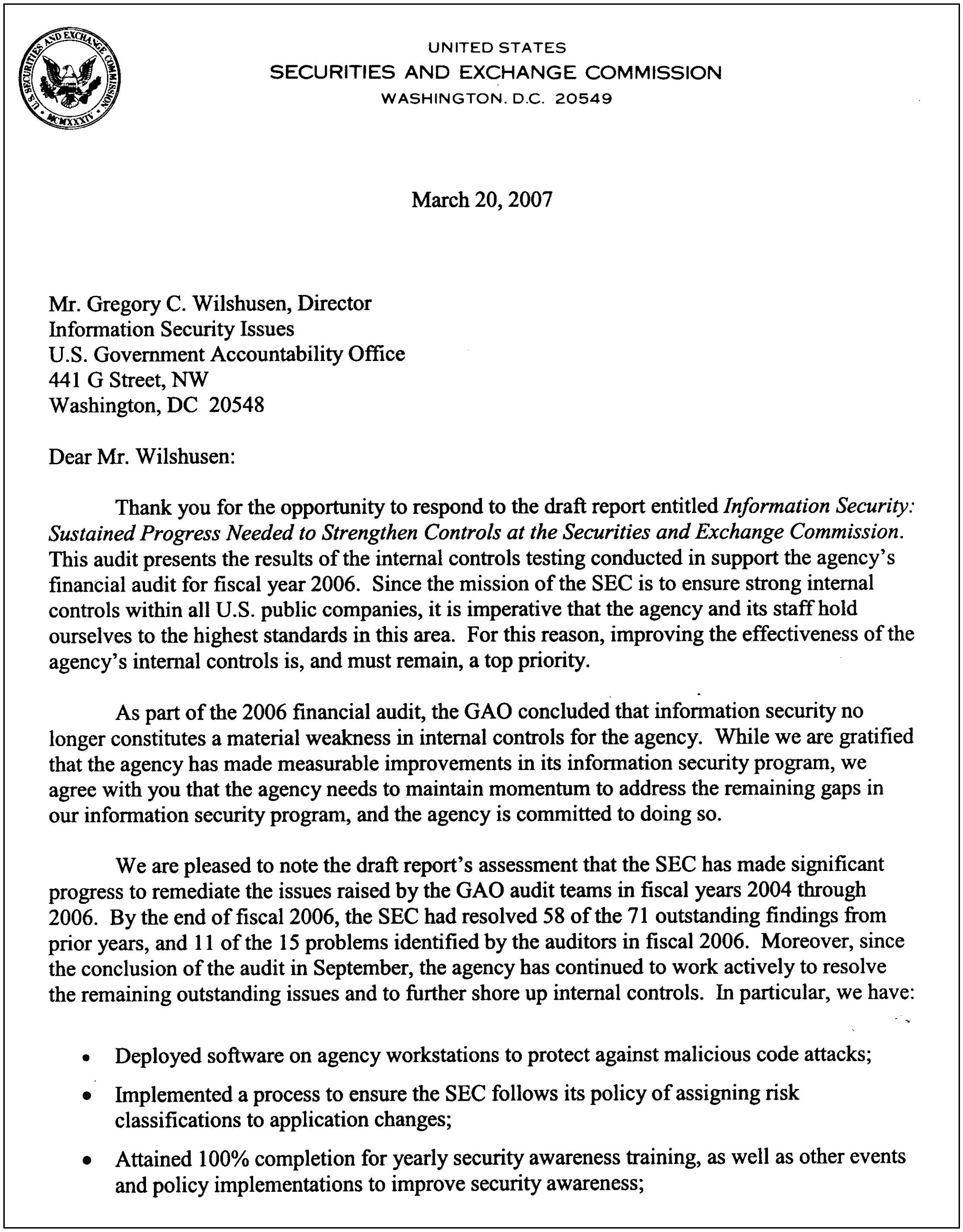
If you have any questions regarding this report, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Comments from the Securities and Exchange Commission



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

March 20, 2007

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

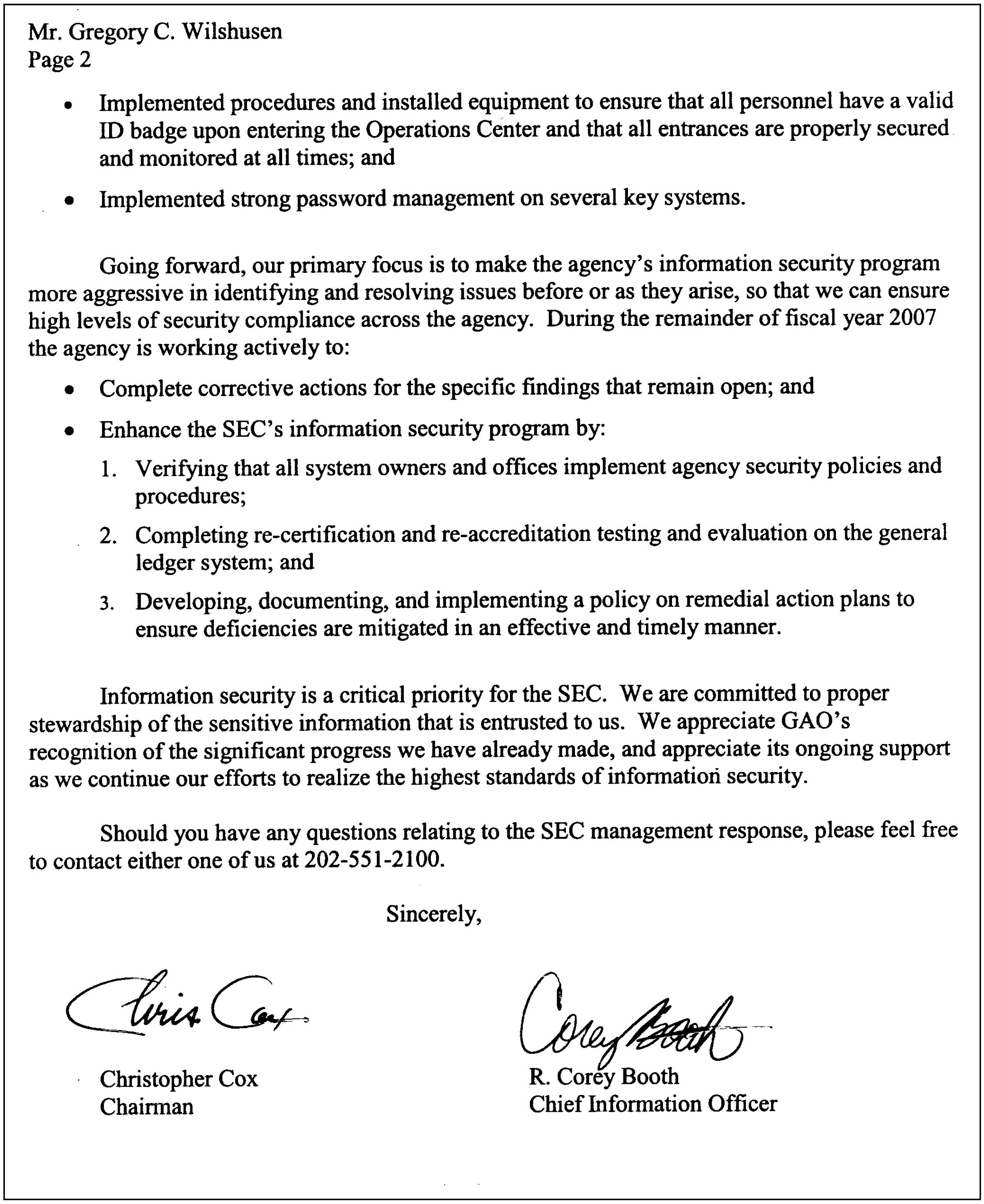
Dear Mr. Wilshusen:

Thank you for the opportunity to respond to the draft report entitled *Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission*. This audit presents the results of the internal controls testing conducted in support the agency's financial audit for fiscal year 2006. Since the mission of the SEC is to ensure strong internal controls within all U.S. public companies, it is imperative that the agency and its staff hold ourselves to the highest standards in this area. For this reason, improving the effectiveness of the agency's internal controls is, and must remain, a top priority.

As part of the 2006 financial audit, the GAO concluded that information security no longer constitutes a material weakness in internal controls for the agency. While we are gratified that the agency has made measurable improvements in its information security program, we agree with you that the agency needs to maintain momentum to address the remaining gaps in our information security program, and the agency is committed to doing so.

We are pleased to note the draft report's assessment that the SEC has made significant progress to remediate the issues raised by the GAO audit teams in fiscal years 2004 through 2006. By the end of fiscal 2006, the SEC had resolved 58 of the 71 outstanding findings from prior years, and 11 of the 15 problems identified by the auditors in fiscal 2006. Moreover, since the conclusion of the audit in September, the agency has continued to work actively to resolve the remaining outstanding issues and to further shore up internal controls. In particular, we have:

- Deployed software on agency workstations to protect against malicious code attacks;
- Implemented a process to ensure the SEC follows its policy of assigning risk classifications to application changes;
- Attained 100% completion for yearly security awareness training, as well as other events and policy implementations to improve security awareness;



Mr. Gregory C. Wilshusen
Page 2

- Implemented procedures and installed equipment to ensure that all personnel have a valid ID badge upon entering the Operations Center and that all entrances are properly secured and monitored at all times; and
- Implemented strong password management on several key systems.

Going forward, our primary focus is to make the agency's information security program more aggressive in identifying and resolving issues before or as they arise, so that we can ensure high levels of security compliance across the agency. During the remainder of fiscal year 2007 the agency is working actively to:

- Complete corrective actions for the specific findings that remain open; and
- Enhance the SEC's information security program by:
  1. Verifying that all system owners and offices implement agency security policies and procedures;
  2. Completing re-certification and re-accreditation testing and evaluation on the general ledger system; and
  3. Developing, documenting, and implementing a policy on remedial action plans to ensure deficiencies are mitigated in an effective and timely manner.

Information security is a critical priority for the SEC. We are committed to proper stewardship of the sensitive information that is entrusted to us. We appreciate GAO's recognition of the significant progress we have already made, and appreciate its ongoing support as we continue our efforts to realize the highest standards of information security.

Should you have any questions relating to the SEC management response, please feel free to contact either one of us at 202-551-2100.

Sincerely,

Chris Cox

Christopher Cox
Chairman

Corey Booth

R. Corey Booth
Chief Information Officer

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244

Staff Acknowledgments

In addition to the individual named above, Charles Vrabel and Lon Chin, Assistant Directors; Angela Bell, Jason Carroll, Daniel Castro, West Coile, William Cook, Anh Dang, Kirk Daubenspeck, Valerie Hopkins, Henry Sutanto, Amos Tevelow, and Chris Warweg made key contributions to this report.

(310584)

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). 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."

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
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

PRINTED ON RECYCLED PAPER