United States Government Accountability Office

GAO

Report to the Chairman, Securities and Exchange Commission

February 2008

INFORMATION SECURITY

Securities and Exchange Commission Needs to Continue to Improve Its Program

GAO
Accountability * Integrity * Reliability

GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-280, a report to the Chairman, Securities and Exchange Commission

February 2008

INFORMATION SECURITY

Securities and Exchange Commission Needs to Continue to Improve Its Program

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 are protected from inadvertent or deliberate misuse, disclosure, or destruction.

As part of its audit of SEC's fiscal year 2007 financial statements, GAO assessed (1) the status of SEC's actions to correct previously reported information security weaknesses and (2) the effectiveness of SEC's controls for ensuring the confidentiality, integrity, and availability of its information systems and information. To do this, GAO examined security plans, policies, and practices; interviewed pertinent officials; and conducted tests and observations of controls in operation.

What GAO Recommends

GAO recommends that the SEC Chairman take several actions to fully implement an agencywide information security program.

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

To view the full product, including the scope and methodology, click on GAO-08-280. For more information, contact Greg Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 8 of 20 weaknesses previously reported as unresolved at the time of our prior audit. For example, SEC has documented authorizations for software modifications, developed a comprehensive program for monitoring access activities to its computer network environment, and tested and evaluated the effectiveness of controls for the general ledger system. In addition, the commission has made progress in improving its information security program. To illustrate, it has developed remedial action plans to mitigate identified weaknesses in its systems and developed a mechanism to track the progress of actions to correct deficiencies. A key reason for its progress is that SEC senior management has been actively engaged in implementing information security activities. Nevertheless, SEC has not completed actions to correct 12 previously reported weaknesses. For example, SEC workstations are susceptible to malicious code attacks and perimeter security is not properly implemented at its Operations Center.

Significant control weaknesses intended to restrict access to data and systems, as well as other information security controls, continue to threaten the confidentiality, integrity, and availability of SEC's financial and sensitive information and information systems. SEC has not consistently implemented effective controls to prevent, limit, or detect unauthorized access to computing resources. For example, it did not always (1) consistently enforce strong controls for identifying and authenticating users, (2) limit user access to only those individuals who need such access to perform their job functions, (3) encrypt sensitive data, (4) log and monitor security related events, (5) physically protect its computer resources, and (6) fully implement certain configuration management controls. A key reason for these weaknesses is that SEC has not yet fully implemented its information security program to ensure that controls are appropriately designed and operating effectively. Specifically, SEC has not effectively or fully implemented key program activities. For example, security plans for certain enterprise database applications were incomplete, information security training for certain key personnel was not sufficiently documented and monitored, security tests and evaluations of enterprise database applications were not comprehensive, and continuity of operations plans were not always complete. As a result, SEC is at increased risk of unauthorized access to and disclosure, modification, or destruction of its financial information, as well as inadvertent or deliberate disruption of its financial systems, operations, and services.

Contents

Abbreviations

CIO	Chief Information Officer
CERT	Computer Emergency Readiness Team
EDGAR	Electronic Data Gathering Analysis and Retrieval
FISMA	Federal Information Security Management Act
GSS	general support system
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PKI	public key infrastructure
SAM	Strategic Acquisition Manager
SEC	Securities and Exchange Commission
US-CERT	United States Computer Emergency Readiness Team

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

February 29, 2008

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 ensure that the securities markets are fair and honest. To support its demanding financial and mission-related responsibilities, the commission relies extensively on computerized systems. In order to protect financial and sensitive information—including personnel and regulatory information maintained by SEC—from inadvertent or deliberate misuse, fraudulent use, improper disclosure or manipulation, or destruction, it is essential that SEC integrate effective information security controls[1] into a layered control strategy.

As part of our audit of SEC's fiscal year 2007 financial statements,[2] we assessed the effectiveness of the commission's information security controls over key financial systems, data, and networks. In our report on SEC's financial statements for fiscal years 2007 and 2006,[3] we concluded that weaknesses in SEC's information security controls constitute a

[1] Information security controls include security management, access controls, configuration management, segregation of duties, and contingency planning. Among other things, these controls are designed to ensure that logical and physical access to sensitive computing resources and information is appropriately restricted, that only authorized changes to computer programs are made, and that 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 2007 and 2006*, GAO-08-167 (Washington, D.C.: Nov. 16, 2007).

[3] GAO-08-167.

significant deficiency[4] in internal controls over the commission's financial and information systems.

In this report, we provide additional details on SEC's information security controls. 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 controls for ensuring the confidentiality, integrity, and availability of its financial information and information systems. We performed our work at SEC headquarters in Washington, D.C., and at its computer facility in Alexandria, Virginia, from July 2007 to November 2007 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for additional details on our objectives, scope, and methodology.

Results in Brief

SEC has made important progress toward correcting previously reported information security control weaknesses. Specifically, it has corrected or mitigated 8 of 20 weaknesses previously reported as unresolved at the time of our prior audit. For example, SEC has documented authorizations for software modifications, developed a comprehensive program for monitoring access activities to its computer network environment, and tested and evaluated the effectiveness of controls for the general ledger system. In addition, the commission has made progress in improving its information security program. To illustrate, it has developed remedial action plans to mitigate identified weaknesses in its systems and developed a mechanism to track the progress of actions to correct deficiencies. A key reason for progress in these areas is that SEC senior management has been actively engaged in implementing information security activities. Nevertheless, SEC has not completed actions to correct 12 previously reported weaknesses. For example, SEC workstations are

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

susceptible to malicious code attacks and perimeter security is not properly implemented at its Operations Center.

Significant deficiencies in controls intended to restrict access to data and systems, as well as weaknesses in other information security controls, continue to threaten the confidentiality, integrity, and availability of SEC's financial and sensitive information and information systems. SEC has not consistently implemented effective controls to prevent, limit, or detect unauthorized access to computing resources. For example, it did not always (1) consistently enforce strong controls for identifying and authenticating users, (2) limit user access to only those individuals who need such access to perform their job functions, (3) encrypt sensitive data, (4) log and monitor security related events, (5) physically protect its computer resources, and (6) fully implement certain configuration management controls. A key reason for these weaknesses is that SEC has not yet fully implemented its information security program to ensure that controls are appropriately designed and operating effectively. Specifically, SEC has not effectively or fully implemented key program activities. For example, security plans for certain enterprise database applications were incomplete, information security training for certain key personnel was not sufficiently documented and monitored, security tests and evaluations of enterprise database applications were not comprehensive, and continuity of operations plans were not always complete. As a result, SEC is at increased risk of unauthorized access to and disclosure, modification, or destruction of its financial information, as well as the inadvertent or deliberate disruption of its financial systems, operations, and services.

We are making recommendations to the SEC Chairman to take several actions to fully implement a comprehensive, agencywide information security program. We are also making recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the information security weaknesses related to access controls and configuration management practices.

In providing written comments on a draft of this report, the SEC Chairman welcomed our findings as an opportunity for further improvement, fully agreed with GAO's recommendations, and stated that SEC is on track to address them in the current fiscal year.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business and is especially important for government agencies, where maintaining the public's trust is essential. While the dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have enabled agencies such as SEC to better achieve their mission and provide information to the public, the changes also expose federal networks and systems to various threats. For example, the Federal Bureau of Investigation has identified multiple sources of cyber threats, including foreign nation states engaged in information warfare, domestic criminals, hackers, and virus writers, and disgruntled employees working within an organization. Similarly, the U.S. Secret Service and the Computer Emergency Readiness Team (CERT) Coordination Center[5] conducted a study on insider threats and stated in a May 2005 report that "insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases." 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, and steady advances in the sophistication and effectiveness of attack technology. For example, for fiscal year 2006, the Office of Management and Budget (OMB) cited[6] a total of 5,146 incidents reported by federal agencies to the United States Computer Emergency Readiness Team (US-CERT),[7] an increase of 44 percent from the previous fiscal year. Without proper safeguards, systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain or manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Our previous reports and reports by inspectors general describe persistent information security weaknesses that place federal agencies at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,[8] a designation that remains in

[5] The CERT Coordination Center is a research center that specializes in Internet security. It is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[6] OMB, *FY 2006 Report to Congress on Implementation of The Federal Information Security Management Act of 2002* (Washington, D.C., March, 2007).

[7] US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

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

force today. Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002[9] to strengthen the security of information and systems within federal agencies. FISMA requires each agency to develop, document, and implement an agencywide information security program to provide information security for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management.

SEC's Role as Protector of Securities Investors

Following the stock market crash of 1929, Congress passed the Securities Exchange Act of 1934,[10] establishing the SEC to enforce securities laws, regulate the securities markets, and protect investors. To carry out its responsibilities and help ensure that securities markets are fair and honest, SEC issues rules and regulations that promote adequate and effective disclosure of information to the investing public. The commission also oversees 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 at the direction of five commissioners appointed by the President and confirmed by the Senate.

In fiscal year 2007, SEC had a budget of about $882 million and a staff of 3,470. In fiscal year 2007, the commission collected $258 million in filing fees and $496 million in penalties and disgorgements.[11]

To support its financial operations and store the sensitive information it collects, SEC relies extensively on computerized systems interconnected by local-and wide-area networks. For example, to process and track financial transactions, such as filing fees paid by corporations, disgorgements and penalties from enforcement activities, and procurement activities, SEC relies on several enterprise database applications—Momentum; CATS/Phoenix; Electronic Data Gathering, Analysis, and Retrieval (EDGAR); Strategic Acquisition Manager (SAM)—

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

[10] 15 U.S.C. § 78d.

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

and a general support system (GSS) network that allows users to communicate with the database applications. The database applications provide SEC with the following capabilities:

- Momentum is used to record some of the commission's accounting transactions, to maintain its general ledger, and to maintain some of the information SEC uses to produce financial reports.

- CATS/Phoenix contains and processes sensitive data relating to penalties, disgorgements, and restitution on proven and alleged violations of the securities and futures laws.

- EDGAR performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required to file certain information with SEC. Its primary purpose is to increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency.

- SAM is intended to automate procurement processes for the SEC Procurement and Contracting office.

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

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

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

SEC has corrected or mitigated 8 of the 20 security control weaknesses that we had reported as unresolved at the time of our previous audit. For example, SEC has

- documented authorizations for software modifications,
- developed a comprehensive program for monitoring access activities to its computer network environment, and
- tested and evaluated the effectiveness of controls for the general ledger system.

In addition, SEC has made progress in improving its information security program. For example, the commission has developed and documented information security related policies, including those responding to information security incidents, such as unauthorized access. SEC has also developed remedial action plans to mitigate identified weaknesses in its systems and developed a mechanism to track the progress of the actions taken to correct deficiencies. The commission also has tested disaster recovery plans two times a year through a series of disaster recovery exercises covering major applications and various scenarios. These efforts constitute an important step towards strengthening the agencywide information security program mandated by FISMA.

A key reason for its progress in these areas is that SEC senior management has been actively engaged in mitigating the previously reported weaknesses. For example, the Chairman has received regular briefings on SEC's progress in resolving the previously reported weaknesses, and the CIO has coordinated efforts with other offices involved in implementing information security controls and practices at the commission.

While SEC has made important progress in strengthening its information security controls, it has not completed actions to correct or mitigate 12 previously reported weaknesses. For example, SEC has not mitigated weaknesses that could lead to malicious code attacks on SEC's workstations, has not adequately documented access privileges for the EDGAR application, and has not implemented an effective intrusion detection system. In addition, SEC has not adequately controlled access to its facility. Failure to resolve these issues could leave SEC's sensitive data vulnerable to unauthorized disclosure, modification, or destruction.

Significant Control Deficiencies Place SEC's Internal Financial Information at Risk

Controls intended to restrict access to data and systems, as well as in other information security controls, insufficiently protect the confidentiality, integrity, and availability of SEC financial systems and information. The unresolved, previously reported weaknesses and newly identified weaknesses could hinder SEC's ability to perform vital functions and increase the risk of unauthorized disclosure, modification, or destruction of financial information. A key reason for these weaknesses was that SEC did not always effectively implement key program activities of its information security program.

SEC Did Not Sufficiently Control Access to Information Resources

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

Controls for Identifying and Authenticating Users Were Not Consistently Enforced

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

However, SEC did not consistently identify and authenticate the identity of users before granting them access to its enterprise database applications, as the following examples illustrate:

- SEC did not always enforce strong password settings on its enterprise database servers, which increased the likelihood that passwords could be compromised.

- Multiple individuals shared a single-user account to enter system information on a key SEC enterprise database application, which diminished SEC's capability to attribute system activity to specific individuals.

- Plaintext passwords may have been accessible to unauthorized users, who could have used them to gain access to a key financial application.

As a result, there was an increased risk that a malicious individual could gain inappropriate access to SEC database applications and data.

Users Were Routinely Authorized More System Access Than Needed to Perform Their Job Functions

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 determining 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.

However, SEC did not always have appropriate authorization settings in place on its enterprise database applications to ensure proper access to data. Specifically, SEC did not adequately restrict user privileges to the minimum access employees needed to perform their job-related duties on several of its enterprise databases. For example, users could escalate their access privileges to run a powerful database system account. In addition, SEC also allowed unnecessary links among databases that could be used to bypass security controls through remote connectivity to other databases. As a result, the unnecessary level of access granted to SEC computer resources provided opportunities for individuals to circumvent security controls and deliberately or inadvertently read, modify, or delete critical information relating to financial statements.

Sensitive Data Were Not Always Encrypted

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity by transforming plaintext into ciphertext using a special value known as a key and a mathematical process known as an algorithm. A public key infrastructure (PKI) is a system of hardware, software, and policies that uses cryptographic techniques to generate and manage electronic certificates, which links an individual or entity to a given public key. These certificates are then used to verify digital signatures (providing authentication and data integrity) and facilitate data encryption (providing confidentiality). A properly designed and implemented PKI can also be used to ensure that a given digital signature is still properly linked to the individual or entity associated with it (providing nonrepudiation). Commonly available commercial Web browsers (such as Microsoft's Internet Explorer and America Online's Netscape Communicator) make use of the technical features of PKI to provide security for Web-enabled transactions. They invoke a standardized information exchange protocol known as secure sockets layer, which uses PKI-like features to provide authentication between a user application, such as a Web browser, and a server. The National Security Agency also recommends disabling protocols that do not encrypt information, such as user ID and password combinations, transmitted across the network.

SEC did not always ensure that sensitive data was protected by encryption. For example, it did not adequately validate electronic certificates for certain connections, thereby diminishing their effectiveness. SEC also did not enable secure sockets layer communications between certain client computers and a key financial application's database servers. In addition, users authenticating to a key enterprise database application sent unencrypted passwords across the network, thereby increasing the likelihood that the passwords would be compromised. As a result, an attacker could view unencrypted data, such as passwords, and use them to gain unauthorized access to SEC network resources and view or modify messages transmitted across the network.

Logging Procedures Did Not Provide Sufficient Audit Trails to Monitor Access Activity

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail of needed information in the desired formats and locations in order 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 the audit trails can provide. SEC policy requires the enforcement of auditing and accountability by configuring information systems to produce, store, and retain audit records of system, application, network, and user activity. SEC also requires that audit records contain sufficient information to establish what events occurred, when the events occurred, the source of the events, and the event's outcomes. In addition, SEC policy states that conducting a baseline assessment of the network is part of the detection and analysis phase of its incident response process. Network baselining enables the organization to detect unusual traffic patterns, monitor bandwidth usage, and understand normal network behavior.

However, SEC did not always provide adequate auditing and monitoring of enterprise databases. For example, it did not maintain complete audit trails of activity by users and applications in the database applications that were relevant to security. Key security-related events, such as unsuccessful log-in attempts and the use of important system privileges, were not logged. In addition, SEC did not conduct a baseline assessment of its network to enable the organization to detect unusual traffic patterns, monitor bandwidth usage, and understand normal network behavior. The lack of effective database logging and network baselining increased the risk that anomalous activity in SEC would not be effectively detected or investigated.

Weaknesses in Physical Security Controls Reduced Their Effectiveness

Physical access control measures, such as guards, badges, and locks, are vital to protecting the agency's sensitive computing resources from both external and internal threats. SEC policy requires that managers periodically review the list of employees and contractors who have physical access to restricted facilities and remove the access privileges of individuals who no longer require access.

However, SEC did not keep updated lists of personnel who had authorized access to the Operations Center current and did not promptly remove personnel who no longer required access. For example, the list of individuals authorized to enter the SEC Operations Center was not current and included 48 individuals who no longer worked for the commission. A SEC physical security official confirmed that the list was inaccurate and that the electronic badges for 21 of the individuals were still active and would permit access to the Operations Center. As a result, increased risk exists that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

Other Weaknesses in Information System Controls Increased Risk

Configuration Management Policies Were Not Fully Implemented

To protect an organization's information, it is important to ensure that only authorized applications and programs are placed in operation. 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. Patch management, including up-to-date patch installation, helps to mitigate vulnerabilities associated with flaws in software code that could be exploited to cause significant damage.

SEC continues to have difficulty implementing certain configuration management controls. For example, SEC lacks procedures to periodically review application code to ensure that only authorized changes were made to production. In addition, it has not implemented an effective patch management program. A malicious user can exploit vulnerabilities associated with unpatched applications to gain unauthorized access to network resources or disrupt network operations. Consequently, major enterprise database applications were vulnerable to code exploit attacks, and individuals internal to SEC could gain unauthorized access to sensitive information and systems, thereby increasing the risk that the integrity of certain network devices and administrator workstations could be compromised.

SEC Has Not Fully Implemented Its Information Security Program

Although SEC has made important progress in implementing its information security program, a key reason for these weaknesses is that SEC has not effectively or fully implemented key program activities. The commission requires its components to implement information security program activities in accordance with FISMA requirements, OMB policies, and applicable National Institute of Standards and Technology (NIST) guidance. Among other things, FISMA requires agencies to develop, document, and implement

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;

- plans for providing adequate information security for networks, facilities, and systems;

- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices performed with a frequency depending on risk, but no less than annually, that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices of the agency;[12]

- 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.

SEC has taken several actions to implement elements of its information security program. For example, SEC has

- implemented a risk assessment process that identified possible threats and vulnerabilities to its systems and information, and the controls needed to mitigate potential vulnerabilities;

[12] OMB requires agencies to address remedial actions through plans of action and milestones for all programs and systems where an information technology security weakness has been found. The plan lists the weaknesses and shows estimated resource needs, challenges to resolving the weaknesses, key milestones and completion dates, and the status of corrective actions.

- implemented a test and evaluation process to assess the effectiveness of information security policies, procedures, and practices;

- ensured that vulnerabilities identified during its tests and evaluations are addressed in its remedial action plans and risk assessments;

- developed an incident response policy and has deployed personnel, procedures, and tools for managing its audit logs and incident response process; and

- subjected its GSS network and major applications to disaster recovery testing twice a year.

However, SEC has not yet fully or consistently implemented key elements of its information security program. For example, security plans for certain enterprise database applications were incomplete, information security training for key personnel was not sufficiently documented and monitored, security tests and evaluations of enterprise database applications were not comprehensive, and continuity of operations plans were not always complete. Until all key elements of its information security program are fully and consistently implemented, SEC will not have sufficient assurance that new weaknesses will not emerge and that financial information and financial assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

Security Plans Did Not Adequately Document System Interconnections and Other Key Information

The purpose of an information system security plan is to provide an overview of the security requirements of the system and to describe the controls that are in place or planned for meeting those requirements. According to NIST guidance, security plans should document all interconnected systems and describe the interaction among systems with regard to the authorization for the connection to other systems or the sharing of information. System interconnections, if not appropriately protected, may compromise connected systems and the data they store, process, or transmit. SEC policy states that security protections for interconnected systems should include documented agreement of all interconnected information systems between SEC's systems and systems owned or operated by other government agencies or contractors. The owners and managers for both of the interconnected systems approve and sign the agreement. In addition, system security plans should also cover the security categories, objectives, and impact levels, which drive requirements for the system's security controls.

However, the Momentum and GSS security plans were incomplete because they did not document system interconnection and information sharing agreements with other systems. The Momentum security plan also did not define system boundaries, identify common security controls, and provide up-to-date information that reflects changes and vulnerabilities discovered based on the application's risk assessment and security evaluations. Without complete security plans, SEC cannot ensure that appropriate controls are in place to protect its systems and critical information. Moreover, without current and complete documentation on the interconnection of systems supporting SEC, unintended access may be granted to connecting parties, and the heightened risk of compromise increases for connected systems and the data they store, process, or transmit.

Training for Employees with Significant Security Responsibilities Was Not Adequately Documented and Monitored

Another important element of an information security program involves promoting awareness and providing required training so that users understand the system security risks and their role in implementing related policies and controls to mitigate those risks. FISMA mandates that all federal employees and contractors who use agency information systems be provided with information security awareness training. Further, FISMA requires agency chief information officers to ensure that personnel with significant information security responsibilities receive specialized training.[13] In addition, NIST Special Publication 800-53 states that organizations must document and monitor individual information system security training activities, including basic security awareness training and specific information system security training.

SEC established an information security awareness program for its employees and contractors. This program includes distributing security awareness bulletins and brochures and creating information security poster boards. In addition, SEC developed specialized security training for database, system, and network administrators. However, SEC did not document and monitor specific information system security training activities for its incident handling team. Specifically, SEC did not document and monitor required specialized training that incident handling personnel received. While SEC maintained some records of employee training certifications, SEC officials stated that they did not monitor whether personnel required to take the specific training sessions actually completed that training. As a result, SEC has limited assurance that

[13] 44 U.S.C. § 3544(a)(3)(D).

incident responders are receiving the instruction they need in order to respond more effectively to security incidents.

Although Controls Were Tested and Evaluated, Tests Were Not Always Comprehensive

A key element of an information security program is the periodic testing and evaluation of controls to ensure that they are in compliance with security policies, are effective, and are operating as intended. 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 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, and occur no less than annually.[14] Furthermore, SEC requires all systems to undergo an annual self-assessment by testing controls identified in NIST guidance.

However, SEC had not completed the annual testing of security controls for its general ledger application and GSS. Without comprehensive tests and evaluations, the commission cannot be assured that employees and contractors are complying with established policies or that policies and controls are appropriate and working as intended.

Continuity of Operations Planning Was Not Always Complete

Continuity of operations planning, which includes developing and testing contingency plans and disaster recovery plans, should be performed to ensure that when unexpected events occur, essential operations continue without interruption or can be promptly resumed, and critical and sensitive data are protected. NIST guidance states that organizations should develop and implement a contingency plan that addresses contingency roles and responsibilities and describes activities associated with backing up and restoring the system after a disruption or failure.

Although SEC tested the contingency plan for its GSS and its major applications, it did not adequately back up critical accounting data files on key workstations. For example, agency personnel performed substantial workstation-based accounting procedures during closing processes and

[14] 44 U.S.C. § 3544(b)(5).

financial statement preparation on spreadsheets maintained on local drives that were not backed up. In addition, the disaster recovery plan for a mission-critical application did not contain key information. For example, essential personnel contact information, recovery time objectives, and test scripts were missing from the Phoenix disaster recovery plan. Without measures to back up important data stored on workstation drives and to maintain up-to-date information in the application's disaster recovery plan, there is an increased risk that SEC will not be able to effectively recover and continue operations when an emergency occurs.

Conclusions

SEC has made progress in correcting or mitigating previously reported weaknesses, implementing controls over key financial systems, and developing and documenting a framework for its agencywide information security program. However, information security weaknesses—both old and new—continue to impair the commission's ability to ensure the confidentiality, integrity, and availability of financial and sensitive information. A key reason for these weaknesses is that the agency has not yet fully implemented critical elements of its agencywide information security program. Until SEC (1) mitigates known information security weaknesses in access controls and other information system controls and (2) fully implements a comprehensive agencywide information security program that includes complete security plans, appropriate specialized training, comprehensive tests and evaluations, and a complete continuity of operations process, its financial information will remain at increased risk of unauthorized disclosure, modification, or destruction, and its management decisions may be based on unreliable or inaccurate information.

Recommendations for Executive Action

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

1. Ensure that security plans are complete and that the plans (a) document system interconnection and information sharing agreements with other systems, (b) define system boundaries, (c) identify common security controls, and (d) provide up-to-date information that reflects changes and vulnerabilities discovered based on the applications' risk assessment and security evaluations.

2. Document and monitor individual specific information system security training activities for the incident handling team.

3. Complete the annual testing of security controls for the general ledger application and general support system.

4. Adequately back up critical data files on key workstations used for storing large accounting data files and ensure that mission-critical application contingency plans contain key information.

In a separate report designated “Limited Official Use Only,” we are also making 26 recommendations to enhance SEC’s access controls and configuration management practices.

Agency Comments

In providing written comments on a draft of this report, the SEC Chairman welcomed our findings as an opportunity for further improvement, fully agreed with GAO’s recommendations, and stated that SEC is on track to address them in the current fiscal year. The SEC Chairman also reported several actions that the agency has completed in resolving outstanding issues and stated that information security continues to be a critical priority for the agency, as it is committed to proper stewardship of the sensitive information entrusted by the public. The Chairman’s written comments are reprinted in appendix II.

We are sending copies of this report to the Chairmen and Ranking Members of the Senate Committee on Banking, Housing, and Urban Affairs; the Senate Committee on Homeland Security and Governmental Affairs; the House Committee on Financial Services; and the House Committee on Oversight and Government Reform. We are also sending this report to other interested congressional committees, the Director of the Office of Management and Budget, and other interested parties. We will also make copies available to others upon 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 about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Sincerely yours,

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati

Dr. Nabajyoti Barkakati
Acting Chief Technologist

Appendix I: Objectives, Scope, and Methodology

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

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

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

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

- testing the complexity and expiration of password settings on servers to determine if strong password management was enforced;
- analyzing users' system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- observing methods for providing secure data transmissions across the network to determine whether sensitive data was being encrypted;

- observing whether system security software was logging successful system changes;

- testing and observing physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;

- inspecting key servers and workstations to determine whether critical patches had been installed or were up-to-date;

- examining access responsibilities to determine whether incompatible functions were segregated among different individuals; and

- observing end-user activity pertaining to the process of preparing SEC financial statements.

Using the requirements identified by the Federal Information Security Management Act (FISMA), which establishes key elements for an effective agencywide information security program, we evaluated SEC's implementation of its security program by

- reviewing SEC's risk assessment process and risk assessments for three key SEC systems that support the preparation of financial statements to determine whether risks and threats were documented consistent with federal guidance;

- analyzing SEC's policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;

- analyzing security plans to determine if management, operational, and technical controls were in place or planned and that security plans were updated;

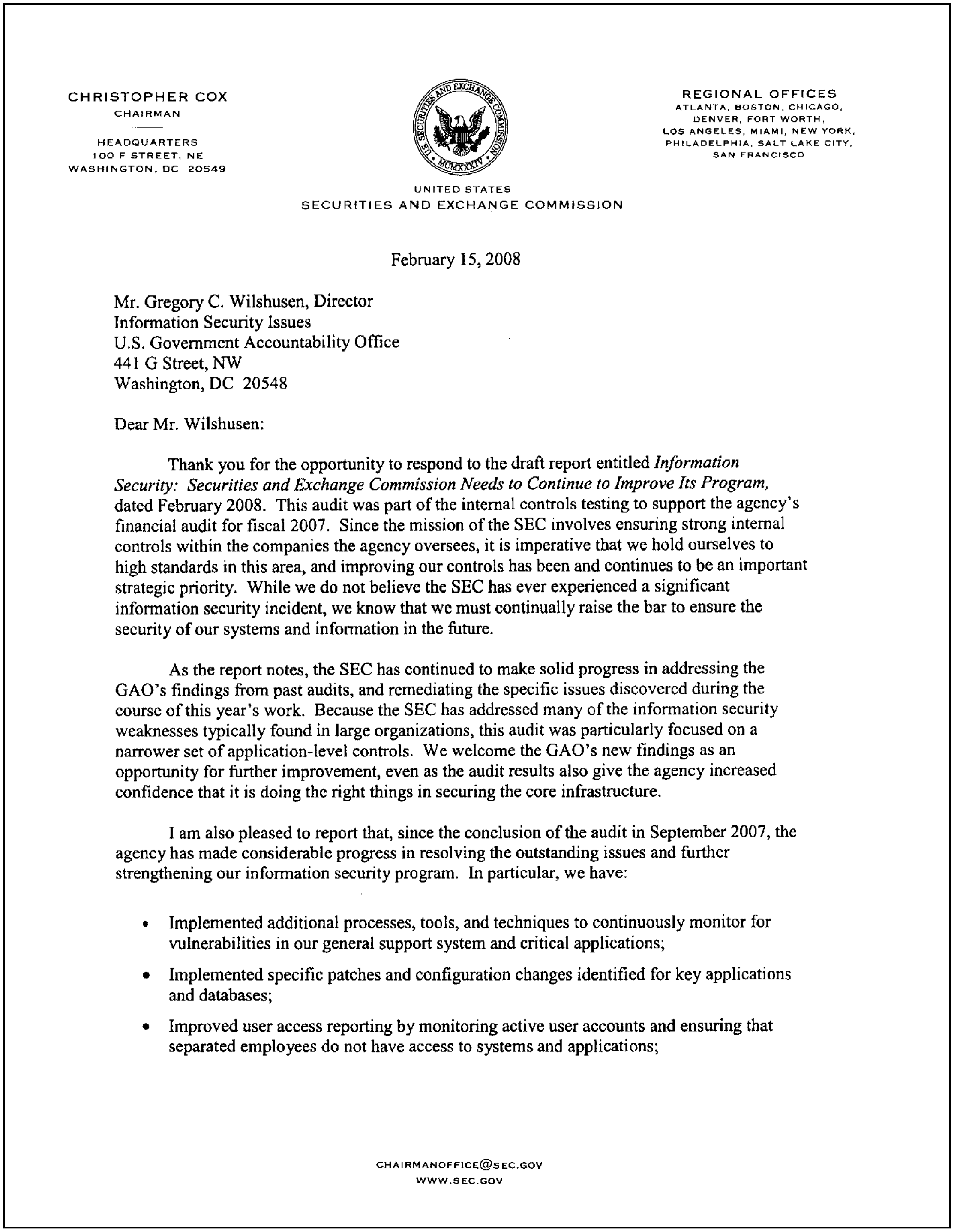
- examining training records for personnel with significant security responsibilities to determine if they received training commensurate with those responsibilities;

- analyzing security testing and evaluation results for three key SEC systems to determine whether management, operational, and technical controls were tested at least annually and based on risk;

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

We also discussed, with key security representatives and management officials, whether information security controls were in place, adequately designed, and operating effectively. We conducted this performance audit from July 2007 to November 2007 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Securities and Exchange Commission



CHRISTOPHER COX
CHAIRMAN

HEADQUARTERS
100 F STREET, NE
WASHINGTON, DC 20549

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

REGIONAL OFFICES
ATLANTA, BOSTON, CHICAGO,
DENVER, FORT WORTH,
LOS ANGELES, MIAMI, NEW YORK,
PHILADELPHIA, SALT LAKE CITY,
SAN FRANCISCO

February 15, 2008

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

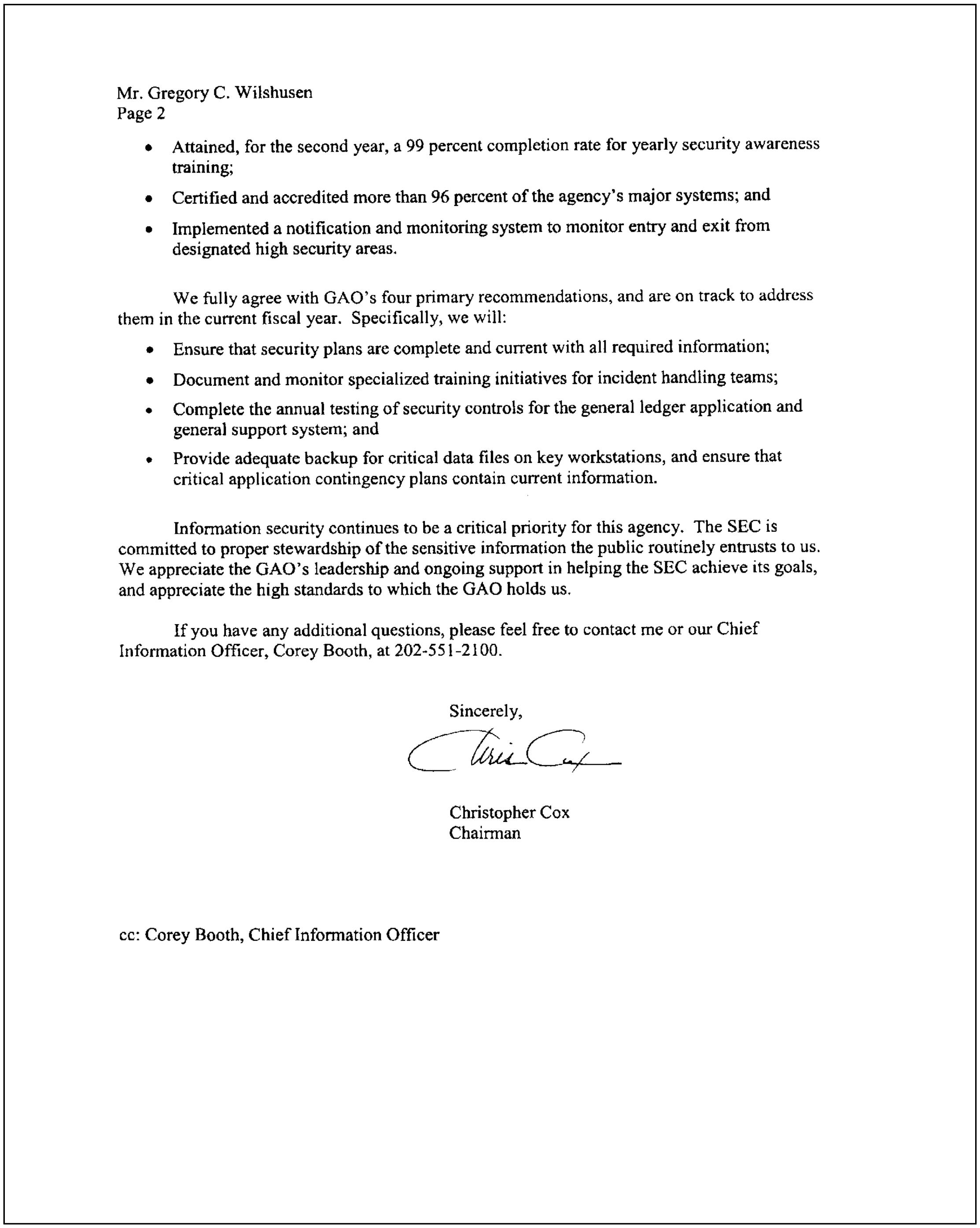
Dear Mr. Wilshusen:

Thank you for the opportunity to respond to the draft report entitled *Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program,* dated February 2008. This audit was part of the internal controls testing to support the agency's financial audit for fiscal 2007. Since the mission of the SEC involves ensuring strong internal controls within the companies the agency oversees, it is imperative that we hold ourselves to high standards in this area, and improving our controls has been and continues to be an important strategic priority. While we do not believe the SEC has ever experienced a significant information security incident, we know that we must continually raise the bar to ensure the security of our systems and information in the future.

As the report notes, the SEC has continued to make solid progress in addressing the GAO's findings from past audits, and remediating the specific issues discovered during the course of this year's work. Because the SEC has addressed many of the information security weaknesses typically found in large organizations, this audit was particularly focused on a narrower set of application-level controls. We welcome the GAO's new findings as an opportunity for further improvement, even as the audit results also give the agency increased confidence that it is doing the right things in securing the core infrastructure.

I am also pleased to report that, since the conclusion of the audit in September 2007, the agency has made considerable progress in resolving the outstanding issues and further strengthening our information security program. In particular, we have:

- Implemented additional processes, tools, and techniques to continuously monitor for vulnerabilities in our general support system and critical applications;
- Implemented specific patches and configuration changes identified for key applications and databases;
- Improved user access reporting by monitoring active user accounts and ensuring that separated employees do not have access to systems and applications;



Mr. Gregory C. Wilshusen
Page 2

- Attained, for the second year, a 99 percent completion rate for yearly security awareness training;
- Certified and accredited more than 96 percent of the agency's major systems; and
- Implemented a notification and monitoring system to monitor entry and exit from designated high security areas.

We fully agree with GAO's four primary recommendations, and are on track to address them in the current fiscal year. Specifically, we will:

- Ensure that security plans are complete and current with all required information;
- Document and monitor specialized training initiatives for incident handling teams;
- Complete the annual testing of security controls for the general ledger application and general support system; and
- Provide adequate backup for critical data files on key workstations, and ensure that critical application contingency plans contain current information.

Information security continues to be a critical priority for this agency. The SEC is committed to proper stewardship of the sensitive information the public routinely entrusts to us. We appreciate the GAO's leadership and ongoing support in helping the SEC achieve its goals, and appreciate the high standards to which the GAO holds us.

If you have any additional questions, please feel free to contact me or our Chief Information Officer, Corey Booth, at 202-551-2100.

Sincerely,

Chris Cox

Christopher Cox
Chairman

cc: Corey Booth, Chief Information Officer

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Staff Acknowledgments

In addition to the contacts named above, Ed Alexander, David Hayes, and William Wadsworth (Assistant Directors), Angela Bell, Kirk Daubenspeck, Patrick Dugan, Mickie Gray, Sharon Kitrell, Stephanie Lee, Henry Sutanto, Amos Tevelow, Chris Warweg, and Jayne Wilson made key contributions to this report.

(310595)

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 "E-mail 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, DC 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

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

Public Affairs

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

PRINTED ON ♻ RECYCLED PAPER