United States Government Accountability Office

Report to the Chair, U.S. Securities and Exchange Commission

April 2014

INFORMATION SECURITY

SEC Needs to Improve Controls over Financial Systems and Data

GAO-14-419

April 2014

INFORMATION SECURITY

SEC Needs to Improve Controls over Financial Systems and Data

GAO Highlights

Highlights of GAO-14-419, a report to the Chair, U.S Securities and Exchange Commission

Why GAO Did This Study

SEC is responsible for enforcing securities laws, issuing rules and regulations that protect investors, and helping to ensure that securities markets are fair and honest. In carrying out its mission, the commission relies extensively on computerized systems that collect and process financial and sensitive information. Accordingly, it is essential that SEC have effective information security controls in place to protect this information from misuse, fraudulent use, improper disclosure, manipulation, or destruction.

As part of its audit of SEC's fiscal years 2013 and 2012 financial statements, GAO assessed the commission's information security controls. The objective was to determine the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of SEC's key financial systems and information. To do this, GAO assessed security controls in key areas by reviewing SEC documents, testing selected systems, and interviewing relevant officials.

What GAO Recommends

GAO is recommending that SEC take two actions to (1) more effectively oversee contractors performing security-related tasks and (2) improve risk management. In a separate report for limited distribution, GAO is recommending that SEC take 49 specific actions to address weaknesses in security controls. In commenting on a draft of this report, SEC generally agreed with GAO's recommendations and described steps it is taking to address them.

View GAO-14-419.For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

Although the Securities and Exchange Commission (SEC) had implemented and made progress in strengthening information security controls, weaknesses limited their effectiveness in protecting the confidentiality, integrity, and availability of a key financial system. For this system's network, servers, applications, and databases, weaknesses in several controls were found, as the following examples illustrate:

- **Access controls:** SEC did not consistently protect its system boundary from possible intrusions; identify and authenticate users; authorize access to resources; encrypt sensitive data; audit and monitor actions taken on the commission's networks, systems, and databases; and restrict physical access to sensitive assets.
- **Configuration and patch management:** SEC did not securely configure the system at its new data center according to its configuration baseline requirements. In addition, it did not consistently apply software patches intended to fix vulnerabilities to servers and databases in a timely manner.
- **Segregation of duties:** SEC did not adequately segregate its development and production computing environments. For example, development user accounts were active on the system's production servers.
- **Contingency and disaster recovery planning:** Although SEC had developed contingency and disaster recovery plans, it did not ensure redundancy of a critical server.

The information security weaknesses existed, in part, because SEC did not effectively oversee and manage the implementation of information security controls during the migration of this key financial system to a new location. Specifically, during the migration, SEC did not (1) consistently oversee the information security-related work performed by the contractor and (2) effectively manage risk.

Until SEC mitigates control deficiencies and strengthens the implementation of its security program, its financial information and systems may be exposed to unauthorized disclosure, modification, use, and disruption. These weaknesses, considered collectively, contributed to GAO's determination that SEC had a significant deficiency in internal control over financial reporting for fiscal year 2013.

Contents

Abbreviations

CIO	chief information officer
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
SEC	Securities and Exchange Commission
SP	special publication

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 17, 2014

The Honorable Mary Jo White
Chair
U.S. Securities and Exchange Commission

Dear Ms. White:

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

On December 16, 2013, we issued our report on the audit of the SEC's fiscal years 2013 and 2012 financial statements.[2] In that report, we identified, among other things, information security control weaknesses that, considered collectively, represent a significant deficiency[3] in SEC's internal control over financial reporting.

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

[2]GAO, *Financial Audit: Securities and Exchange Commission's Financial Statements for Fiscal Years 2013 and 2012*, GAO-14-213R (Washington, D.C.: Dec. 16. 2013).

[3]A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements of the entity's financial statements on a timely basis. While important enough to merit attention by those charged with governance, a significant deficiency is less severe than a material weakness, which is a deficiency in internal control such that there is a reasonable possibility that a material misstatement will not be prevented, or detected and corrected on a timely basis.

This report presents more detailed information and our recommendations related to the specific information security control weaknesses that we identified during our audit. Our objective was to determine the effectiveness of information security controls for protecting the confidentiality, integrity, and availability of SEC's key financial systems and information. To do this, we examined the commission's information security policies, plans, and procedures; tested controls over key financial applications; interviewed key agency officials; and reviewed our prior reports to identify previously reported weaknesses and assessed the effectiveness of corrective actions taken.

We performed our work in accordance with U.S. generally accepted government auditing standards. We believe that our audit provided a reasonable basis for our conclusions in this report. See appendix I for more details on our objective, scope, and methodology.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business and is especially important for government agencies, where maintaining the public's trust is essential. While the dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have enabled agencies such as SEC to better accomplish their missions and provide information to the public, agencies' reliance on this technology also exposes federal networks and systems to various threats. This can include threats originating from foreign nation states, domestic criminals, hackers, and disgruntled employees. Concerns about these threats are well founded because of the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and advances in the sophistication and effectiveness of attack technology, among other reasons. 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.

We and federal inspectors general have reported on persistent information security weaknesses that place federal agencies at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, since 1997, we have designated information security as a

government-wide high-risk area, and we continued to do so in the most recent update to our high-risk list.[4]

The Federal Information Security Management Act (FISMA) of 2002 is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[5] FISMA requires each agency to develop, document, and implement an agency-wide security program to provide security for the information and systems that support the operations and assets of the agency, including information and information systems provided or managed by another agency, contractor, or other source. Additionally, FISMA assigns responsibility to the National Institute of Standards and Technology (NIST) to provide standards and guidelines to agencies on information security. NIST has issued related standards and guidelines, including *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication (NIST SP) 800-53,[6] and *Contingency Planning Guide for Federal Information Systems*, NIST SP 800-34.[7]

SEC Relies on Information Technology to Support Operations and Financial Reporting

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 or disgorgements and penalties from enforcement activities, and for financial reporting, SEC relies on numerous enterprise applications, including the following:

[4]See, GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and most recently, GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

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

[6]NIST, *Recommended Security Controls for Federal Information Systems and Organizations,* Special Publication 800-53, revision 3 (Gaithersburg, Md.: August 2009). In April 2013, NIST issued revision 4 of this publication; however, revision 3 was in effect for SEC during our review.

[7]NIST, *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34, revision 1 (Gaithersburg, Md.: May 2010).

- The Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system performs the automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others that are required to file certain information with SEC. Its purpose is to accelerate the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the commission.
- EDGAR/Fee Momentum, a subsystem of EDGAR, maintains accounting information pertaining to fees received from registrants.
- End User Computing Spreadsheets and/or User Developed Applications are used by SEC to prepare, analyze, summarize, and report on its financial data.
- The Financial Reporting and Analysis Tool facilitates the compilation of monthly, quarterly, and year-end financial reports. This tool also helps perform data reconciliation and analysis of the principal financial statements.
- The ImageNow application is a workflow tool that tracks, reviews, and approves documents related to disgorgements, penalties, and court registry.
- The general support system provides (1) business application services to internal and external customers and (2) security services necessary to support these applications.

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

Information Security Weaknesses Placed SEC Financial Data at Risk

Although SEC had implemented and made progress in strengthening information security controls, weaknesses limited their effectiveness in protecting the confidentiality, integrity, and availability of a key financial system. SEC did not consistently control access to this financial system's network, servers, applications, and databases; manage its configuration; segregate duties; and plan for contingencies and disasters. These weaknesses existed, in part, because SEC did not effectively oversee and manage the migration of the key financial system to a new location. Consequently, SEC's financial information and systems were exposed to

increased risk of unauthorized access, disclosure, modification, and disruption.

SEC Did Not Consistently Control Access to a Key Financial System

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

Although SEC had issued policies and implemented controls based on those policies, it did not consistently protect its network boundary from possible intrusions; identify and authenticate users; authorize access to resources; ensure that sensitive data are encrypted; audit and monitor actions taken on the commission's systems and network; and restrict physical access to sensitive assets.

Although Control Mechanisms Were Put in Place, SEC Did Not Adequately Protect the Boundaries of a Key Financial System

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network-connected devices. Implementing multiple layers of security to protect an information system's internal and external boundaries provides defense in depth. By using a defense-in-depth strategy, entities can reduce the risk of a successful cyber attack. For example, multiple firewalls could be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems. At the system level, any connections to the Internet, or to other external and internal networks or information systems, should occur through controlled interfaces (for example, proxies, gateways, routers and switches, firewalls, and concentrators). At the host or device level, logical boundaries can be controlled through inbound and outbound filtering provided by access control lists and personal firewalls.

SEC deployed multiple firewalls that were intended to prevent unauthorized access to its systems; however, it did not securely configure access control lists on firewalls inside a key financial system's environment. For example, its network devices and firewall settings inappropriately permitted users in the production environment to access the system's network management server. In addition, the system's production Internet firewalls were configured to allow systems in the "demilitarized zone"[8] to connect to each other. As a result of these configurations, SEC introduced vulnerability to unnecessary and potentially undetectable access at multiple points in the key financial system's network environment.

SEC Did Not Consistently Implement Controls for Identifying and Authenticating Users of a Key Financial System

Information systems need to be managed to effectively control user accounts and identify and authenticate users. Users and devices should be appropriately identified and authenticated through the implementation of adequate logical access controls. Users can be authenticated using mechanisms such as a password and user ID combination. SEC policy requires strong password controls for authentication, such as passwords that are at least 8 eight alphanumeric characters in length and that expire after a predetermined period of time.

However, SEC did not consistently implement strong password controls for identifying and authenticating users to certain servers, network devices, and databases in the key financial system's environment. For example, password length on a network management device and a server contained fewer characters than required. User account passwords on another server were configured to never expire. Additionally, two databases had a user password that had the same name as the user account. As a result, SEC is at increased risk that accounts could be compromised and used by unauthorized individuals to access sensitive information.

[8]The "demilitarized zone," commonly referred to as the DMZ, is a perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

SEC Did Not Always Sufficiently Restrict Access to a Key Financial System

Authorization encompasses access privileges granted to a user, program, or process. It is used to allow or prevent actions by that user based on predefined rules. Authorization includes the principles of legitimate use and least privilege.[9] Operating systems have some built-in authorization features such as user rights and privileges, groups of users, and permissions for files and folders. Network devices, such as routers, may have access control lists that can be used to authorize users who can access and perform certain actions on the device. Access rights and privileges are used to implement security policies that determine what a user can do after being allowed into the system. Maintaining access rights, permissions, and privileges is one of the most important aspects of administering system security.

However, SEC did not always employ the principle of least privilege when authorizing access permissions to a key financial system. Specifically, it did not appropriately restrict access to security-related parameters and users' rights and privileges for several network devices, databases, and servers supporting key financial applications. As a result, users had excessive levels of access that were not required to perform their jobs. This could lead to data being inappropriately modified, either inadvertently or deliberately.

SEC Did Not Effectively Protect Sensitive Data While in Transmission

Cryptographic controls can be used to help protect the integrity and confidentiality of data and computer programs by rendering data unintelligible to unauthorized users and/or protecting the integrity of transmitted or stored data. Cryptography involves the use of mathematical functions called algorithms and strings of seemingly random bits called keys to (1) encrypt a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential; (2) provide an electronic signature that can be used to determine if any changes have been made to the related file, thus ensuring the file's integrity; or (3) link a message or document to a specific individual's or group's key, thus ensuring that the "signer" of the file can be identified. NIST guidance states that the use of encryption by organizations can reduce the probability of unauthorized disclosure of information. NIST also recommends that organizations employ cryptographic mechanisms

[9]Users should have the least amount of privileges (access to services) necessary to perform their duties.

to prevent unauthorized disclosure of information during transmission, encrypt passwords while being stored and transmitted, and establish a trusted communications path between users and security functions of information systems.

However, SEC did not configure settings of the logging and database servers supporting key financial applications to use encryption when transmitting data. As a result, increased risk exists that transmitted data can be intercepted, viewed, and modified.

SEC Did Not Adequately Maintain Audit Trails of Security-Relevant Events

Audit and monitoring involves the regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the appropriate investigation and reporting of such activity. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for investigation of and response to suspicious activities. Audit and monitoring controls can help security professionals routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. Network-based intrusion detection systems capture or "sniff" and analyze network traffic in various parts of a network. FISMA requires that each federal agency implement an information security program that includes procedures for detecting, reporting, and responding to security incidents.

However, SEC had not consistently configured certain servers supporting a key financial system to maintain audit trails for all security-relevant events. For example, several of these network devices did not perform "failed access control lists access violation" logging. Also, while SEC had initiated deployment of tools to monitor its network infrastructure, critical systems' local logs were not sent to a centralized syslog server that logs security events. In addition, the syslog server was offline for more than 1 month. As a result, increased risk exists that SEC will be unable to determine (1) if certain malicious incidents have occurred and (2) who or what caused them.

SEC Generally Protected Access to Its Facilities but Did Not Sufficiently Control Physical Access to a Sensitive Computing Area

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Adequate physical security controls over computer facilities and resources should be established that are commensurate with the risks of physical damage or access. Physical security controls over the overall facility and areas housing sensitive information technology components include, among other things, policies and practices for granting and discontinuing access authorizations; controlling badges, ID cards, smartcards, and other entry devices; controlling entry during and after normal business hours; and controlling the entry and removal of computer resources (such as equipment and storage media) from the facility. Physical controls also include environmental controls, such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies.

While SEC improved physical security controls after relocating its primary data center to a secure location, SEC did not sufficiently control physical access to a key financial system's administrator area in headquarters. For example, system administrators' workstations were located in an open area that was accessible by all personnel with access to the SEC headquarters building. The insufficient physical access control over the system administrators' workstations reduces SEC's ability to protect the system from unauthorized access.

SEC Did Not Always Securely Configure or Install Patches on a Key Financial System

Configuration management involves the identification and management of security features for all hardware, software, and firmware components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. FISMA requires each federal agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements. Systems with secure configurations have less vulnerability and are better able to thwart network attacks. Effective configuration management provides reasonable assurance that systems are configured and operating securely and as intended. In addition to periodically looking for software vulnerabilities and fixing them, security software should be kept current by establishing effective programs for patch management, virus protection, and other emerging threats. Also, software releases should be adequately controlled to prevent the use of noncurrent software.

Although it had configuration management related policies, plans and procedures in place, SEC did not configure a key financial system at its new data center according to SEC's secure configuration baseline. For example, the system's server ran multiple insecure services. In addition,

while SEC had formed a patch vulnerability group to monitor vulnerabilities and evaluate the results of vulnerability scan reports, it did not routinely and consistently patch servers supporting key financial applications in a timely manner. Moreover, SEC used outdated versions of software and products that were no longer supported by their respective vendors. Consequently, increased risk exists that the system was exposed to vulnerabilities that could be exploited by attackers seeking to gain unauthorized access.

Segregation of Duties Was Generally in Place, but Weaknesses Increase Risk

To reduce the risk of error or fraud, duties and responsibilities for authorizing, processing, recording, and reviewing transactions should be separated to ensure that one individual does not control all critical stages of a process. Effective segregation of duties starts with effective entity-wide policies and procedures that are implemented at the system and application levels. Often, segregation of incompatible duties is achieved by dividing responsibilities among two or more organizational groups, which diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. According to NIST SP 800-53, revision 3, to prevent collusive malevolent activity, organizations should separate the duties of individuals as necessary and implement separation of duties through assigned information system access authorizations.

During fiscal year 2013, SEC implemented segregation of duties controls for key information technology processes. For example, SEC had implemented segregation of duties for the administrative accounts tested. In addition, based on our inquiries, SEC employees from the Office of Information Technology Security, Office of Financial Management, and system operations understood their duties and responsibilities.

However, production servers for the key financial system had active development user accounts. As a result, increased risk exists that unauthorized individuals from the development environment could pose a threat to the system's processes in the production environment.

SEC Did Not Fully Update or Test Contingency and Disaster Recovery Plans

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If contingency and disaster recovery plans are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. Given these severe implications, it is important that an entity have in place (1) up-to-date procedures for protecting information resources and minimizing the risk of unplanned interruptions, (2) a tested plan to recover critical operations should interruptions occur, and (3) redundancy in critical systems.

Although SEC had developed contingency and disaster recovery plans and implemented controls for this planning, it did not (1) update its contingency and disaster recovery plans to reflect its computing environment, (2) test disaster recovery procedures to ascertain recovery after the move to its newly built data center, and (3) ensure redundancy of a critical server for the key financial system. Consequently, SEC had limited assurance that financial information could be recovered and made available to meet agency priorities and requirements in the event of a failure at its primary data center.

SEC Did Not Effectively Oversee and Manage the Implementation of Information Security Controls during Migration of a Key Financial System

The information security weaknesses existed in the key financial system, in part, because SEC did not effectively oversee and manage the implementation of information security controls during the migration of the system to a new production environment. Specifically, SEC did not consistently provide adequate contractor oversight and implement an effective risk management process during the migration to the new production environment at its data center in June 2013.

SEC Did Not Consistently Provide Adequate Contractor Oversight

SEC relied on a contractor to migrate the key financial system to a new production environment, which included the completion of critical security-related tasks. The Office of Federal Procurement Policy's *Guide to Best Practices for Contract Administration* states that a good contract administration program is essential to improving contractor performance under federal contracts. It also states that those entrusted with the duty to ensure that the government gets all that it has bargained for must be competent in the practices of contract administration. In addition, NIST guidance states that the head of an agency should establish appropriate accountability for information security and provide active support and oversight of monitoring and improvement for the information security program. Moreover, SEC policy states that the agency is to monitor

project development throughout the life cycle to ensure that security controls are incorporated and security project milestones are met.

However, SEC did not adequately oversee the contractor's efforts related to the migration of the system from SEC's operation center to its data center in a different location. Specifically, SEC did not assign information security personnel to monitor and evaluate the contractor's performance in completing required security tasks. In addition, while the project plan included security-related tasks and milestones, SEC officials did not review the system's security and project migration plans to verify that security-related roles, resources, and responsibilities were identified. Further, SEC did not confirm that the contractor completed the security-related project tasks prior to the decision to go live, including (1) implementing the baseline security configuration on the system's servers, (2) testing the security of its servers, (3) building a monitoring capability inside its network environment, and (4) identifying and committing resources to perform security configuration and testing after the server build-out. SEC officials attributed this lack of rigorous oversight to their reliance on the ability of the contractor to adequately complete the effort. As a result, senior management officials were unaware that security-related project tasks had not been completed when the agency approved the system to go live.

SEC Did Not Effectively Manage Risk Associated with the Migration of a Key Financial System

According to NIST SP 800-37,[10] agencies are to identify and mitigate risks and, prior to placing information systems into operation, ensure that (1) information system-related security risks are being adequately addressed on an ongoing basis and (2) the authorizing official explicitly understands and accepts the risk to organizational operations and assets. In addition, the key financial system's security plan states that SEC is to monitor changes to the system and conduct security impact analyses to determine the effects of the changes. Prior to change implementation, and as part of the change approval process, the organization is to analyze changes to the system for potential security impacts. After the system is changed (including upgrades and modifications), the

[10]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* SP 800-37, revision 1 (Gaithersburg, Md.: February 2010). The framework consists of a six-step process involving (1) security categorization, (2) security control selection, (3) security control implementation, (4) security control assessment, (5) information system authorization, and (6) security control monitoring. It also provides a process that integrates information security and risk management activities into the system development life cycle.

organization should check the security features to verify that the features are still functioning properly.

To improve its information security risk management process, in February 2013 SEC established the Operational Risk Management Office to proactively identify operational risks in all division offices. As part of the agency's risk management process, the heads of business lines are responsible for identifying risks and controls. SEC also established a Risk Committee with the purpose of formalizing the risk framing process and creating an SEC-wide information security risk management strategy, based on decisions and priorities set by the Risk Committee. The risk decisions and risk priorities are to be used as guiding principles by management officials in implementing daily and operational IT tasks.

However, SEC did not effectively manage risk associated with the migration of a key financial system to a new location. Specifically, (1) SEC's Information Security Risk Committee did not identify and convey risks related to the data center move (and to the system) to the agency's Operational Risk Management Program Office, which is responsible for developing and overseeing SEC's operational risk management and internal control program and evaluating the results of internal control reviews and information technology system reviews performed by the internal control divisions and offices; (2) SEC did not perform a security impact analysis after the system servers were rebuilt and major changes were made to the systems; and (3) SEC did not act to mitigate security-related risks identified and communicated in the system's weekly status reports by the contractor prior to the go-live date. Consequently, SEC did not have timely awareness of potential security vulnerabilities, which resulted in pervasive control weaknesses in the system when the new production environment went live.

SEC Made Limited Progress Remediating Previously Reported Information Security Control Weaknesses

SEC resolved two of the seven previously reported information system control deficiencies in the areas of access controls and audit and monitoring.[11] For example, SEC disabled inactive administrator accounts and enabled audit and monitoring capability on a server. However, five of the seven previously reported weaknesses still exist. These five remaining weaknesses encompassed SEC's financial and general

[11]GAO-13-274R.

support systems. For example, SEC did not always configure its remote host and network infrastructure devices to require the use of strong passwords; effectively enforce logical access controls, including controls in the user separation process across its IT systems at the network levels; and consistently apply patches or perform necessary system updates.

Conclusions

SEC continues to make progress in improving information security controls over its key financial systems. However, information security control weaknesses in a key financial system's production environment may jeopardize the confidentiality, integrity, and availability of information residing in and processed by the system. These included deficiencies in SEC's controls over access control, configuration management, segregation of duties, and contingency and disaster recovery planning. In addition, SEC did not consistently provide adequate contractor oversight and implement an effective risk management process during the migration of an important financial system to its new location. Cumulatively, these weaknesses decreased assurance regarding the reliability of the data processed by the key financial system and increased the risk that unauthorized individuals could gain access to critical hardware or software and intentionally or inadvertently access, alter, or delete sensitive data or computer programs. Consequently, the combination of the continuing and new information security weaknesses existing as of September 30, 2013, considered collectively, represented a significant deficiency in SEC's internal control over financial reporting. Until SEC mitigates its control deficiencies and strengthens oversight of contractors performing security-related tasks as part of its information security program, it will continue to be at risk of ongoing deficiencies in the security controls over its financial and support systems and the information they contain.

Recommendations for Executive Action

As part of fully implementing a comprehensive information security program, we recommend that the Chair direct the Chief Information Officer to take the following two actions:

1. Assign information security personnel to monitor and evaluate contractor performance in implementing information security controls in SEC's information technology projects.
2. Implement a risk management process to ensure that similar contract oversight weakness are not widespread that includes (1) identifying

and conveying risks, (2) performing security impact analyses, and (3) mitigating identified risks as appropriate.

In a separate report with limited distribution, we are also making 49 detailed recommendations consisting of actions to be taken to correct specific information security weaknesses related to access control, configuration management, segregation of duties, and contingency and disaster recovery plans.

Agency Comments and Our Evaluation

We provided a draft of this report to SEC for its review and comment. In its written comments (reproduced in app. II), SEC generally agreed with our recommendations. SEC acknowledged that the appropriate level of attention was not applied to contractor oversight during the migration of the financial system and stated that contractual, procedural, and corrective measures are taking place to prevent similar occurrences. In addition, SEC agreed with the specific points we made about the risk management process and stated that this process continues to be improved.

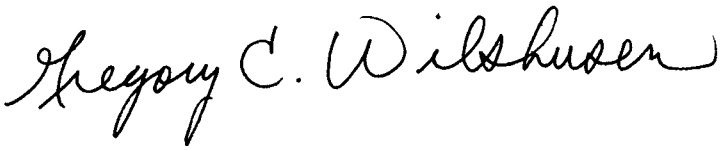
This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. § 720 to submit a written statement on the actions taken on the recommendations by the head of the agency. The statement must be submitted to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Oversight and Government Reform not later than 60 days from the date of this report. A written statement must also be sent to the House and Senate Committees on Appropriations with your agency's first request for appropriations made more than 60 days after the date of this report.

We are also sending copies of this report to interested congressional parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

We acknowledge and appreciate the cooperation and assistance provided by SEC management and staff during our audit. If you have any questions about this report or need assistance in addressing these issues, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Nabajyoti Barkakati at (202) 512-4499 or

barkakatin@gao.gov. GAO staff who made significant contributions to this report are listed in appendix III.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

Dr. Nabajyoti Barkakati
Director, Center for Technology and Engineering

Appendix I: Objective, Scope, and Methodology

As part of our audit of the Securities and Exchange Commission's (SEC) fiscal years 2012 and 2013 financial statements, we assessed the commission's information security controls. The objective was to determine the effectiveness of SEC's information security controls for ensuring the confidentiality, integrity, and availability of its key financial systems and information. To do this, we identified and reviewed SEC information systems control policies and procedures, conducted tests of controls, and held interviews with key security representatives and management officials concerning whether information security controls were in place, adequately designed, and operating effectively.

We evaluated controls based on our *Federal Information System Controls Audit Manual* (FISCAM), which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information;[1] National Institute of Standards and Technology standards and special publications; SEC's plans, policies, and standards; and the National Security Agency's *60 Minute Network Security Guide*. We assessed the effectiveness of both general and application controls by

- performing information system controls walkthroughs surrounding the initiation, authorization, processing, recording, and reporting of financial data (via interviews, inquiries, observations, and inspections);
- reviewing systems security assessment and authorization documents;
- reviewing SEC policies and procedures;
- observing technical controls implemented on selected systems;
- testing specific controls; and
- scanning and manually assessing SEC systems including general support systems and financial applications.

We also evaluated the Statement on Standards for Attestation Engagements report[2] and performed testing on key information

[1]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

[2]Statement on Standards for Attestation Engagements 16 reports are reports typically prepared by an independent auditor based on a review of the controls relevant to user entities' internal control over financial reporting as discussed in the American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization*. A service organization provides services to the entity whose financial statements are being audited.

technology controls on the following applications and systems: Delphi-Prism, FedInvest, and Federal Personnel and Payroll System/Quicktime.

We selected which systems to evaluate based on a consideration of financial systems and service providers integral to SEC's financial statements.

The evaluation and testing of SEC information system controls, including the evaluation of the status of SEC's corrective actions during fiscal year 2013 to address open recommendations from our prior years' reports, was performed jointly with the independent firm of Williams, Adley, & Company-DC, LLP. We agreed on the scope of the audit work, monitored the firm's progress, and reviewed the related audit documentation to determine that the firm's findings were adequately supported.

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

To assess the reliability of the data we analyzed, such as information system control settings, security assessment and authorization documents, and security policies and procedures, we corroborated them by interviewing SEC officials, programmatic personnel, and system administrators to determine whether the data obtained were consistent with system configurations in place at the time of our review. Based on this assessment, we determined the data were reliable for the purposes of this report.

We performed our work in accordance with U.S. generally accepted government auditing standards. We believe that our audit provided a reasonable basis for our conclusions in this report.

Appendix II: Comments from the Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549
March 31, 2014

Mr. Gregory C. Wilshusen
Director
Information Security Issues
United States Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) recommendations related to information security weaknesses identified during its audit of the SEC's financial statements for fiscal years 2013 and 2012 (Report GAO-14-419). We value the independent insights and opinions of our auditors and the perspective they provide. I am pleased that the GAO's audit found that the SEC has made progress in strengthening our information security controls. The SEC has made a significant investment in technology to assist in protecting our environment over the past three years. We will continue to evaluate our risk posture and make additional improvements in our program.

The information security issues you identify in the report demonstrate that we have not achieved our goals as they relate to information and systems protection. While we are confident in our defense-in-depth approach to security, you identified a breakdown in our established verification processes and vendor management.

GAO's first recommendation is to "[a]ssign information security personnel to monitor and evaluate contractor performance in implementing information security controls in SEC's information technology projects." As you indicate in your findings, the weaknesses observed during this audit were due in part to a lack of contractor oversight during its migration of a financial system to one of our two new data centers. At the time of the migration, our new automated system compliance oversight tools were not yet fully deployed to that particular environment. The appropriate level of attention was not applied to contractor oversight during the migration of the financial system identified in your report. As a result, that particular system was deployed without meeting our configuration requirements. Upon GAO notifying us of the configuration issues, we immediately shut down that system and reverted to the original, properly configured environment. Our subsequent move to the second data center was a clean evolution to a properly configured environment.

While we regret the lack of contractor oversight of the system migration, we remain confident that our layered defense architecture would have allowed us to detect and respond to attempted intrusions in a timely fashion, and our forensic investigation yielded no evidence of compromise to that system. Contractual, procedural, and corrective measures are taking place to

prevent any similar occurrence. Our information security personnel do, and will continue to, monitor and assess the effectiveness of controls in our environment. That information will be used by managers and Contracting Officer's Representatives (COR) to aid in overseeing and evaluating contractor performance.

GAO's second recommendation is to "[i]mplement a risk management process to ensure that similar contract oversight weaknesses are not widespread that includes (1) identifying and conveying risks, (2) performing security impact analyses, and (3) mitigating identified risks as appropriate." The Office of Information Technology has implemented project risk management processes and an Information Security Risk Management Program that include identifying and conveying risks, performing security impact analyses, and mitigating identified risks, as appropriate. We continue to improve and refine our risk management process, including the Operational Risk Management Office, and agree with the specific points in GAO's second recommendation.

Concerning the failure to update or test disaster recovery plans identified in GAO's findings, time constraints did not allow for an immediate disaster recovery test of the financial system addressed in your report. However, individual components of the system were tested in both new data centers, and data was being replicated. We continue to follow up on your finding with full disaster recovery testing on a planned basis.

In 2014, the SEC will continue to optimize our controls and further improve the security of our systems that support financial processes and our overall risk management process. I very much appreciate the professional manner in which you and your team conducted the audit for fiscal years 2013 and 2012. I look forward to continuing our productive dialogue in the coming months on the SEC's efforts to address the areas noted in your report. If you have any questions, please feel free to contact me.

Sincerely,

Thomas A. Bayer
Chief Information Officer

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Staff Acknowledgments

In addition to the contacts named above, GAO staff who made major contributions to this report are Michael W. Gilmore and Duc Ngo (Assistant Directors), Angela Bell, Lee McCracken, and Henry Sutanto.