United States Government Accountability Office

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

April 2016

INFORMATION SECURITY

Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data

Accessible Version

INFORMATION SECURITY

Opportunities Exist for SEC to Improve Its Controls over Financial Systems and Data

Why GAO Did This Study

The 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. In carrying out its mission, the SEC relies on computerized information systems to collect, process, and store sensitive information, including financial data. Having effective information security controls in place is essential to protecting these systems and the information they contain.

This report details weaknesses GAO identified in the information security program at SEC during its audit of the commission's fiscal years 2015 and 2014 financial statements. GAO's 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 examined information security policies, plans, and procedures; tested controls over key financial applications; interviewed agency officials; and assessed corrective actions taken to address previously reported weaknesses.

What GAO Recommends

In addition to the 15 prior recommendations that have not been fully implemented, GAO is recommending that SEC take 6 additional actions to more fully implement its information security program. In a separate report with limited distribution, GAO recommended SEC take 30 actions to address newly identified control weaknesses. SEC concurred with GAO's recommendations.

View GAO-16-493. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wishuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Securities and Exchange Commission (SEC) improved its information security by addressing weaknesses previously identified by GAO, including separating the user production network from the internal management network. However, weaknesses continue to limit the effectiveness of other security controls. In particular:

- While SEC had issued policies and implemented controls based on those policies, it did not consistently protect access to its systems. Organizations should design and implement controls to prevent, limit, and detect unauthorized access to computer resources. The commission did not consistently protect its network from possible intrusions, identify and authenticate users, authorize access to resources, audit and monitor actions taken on its systems and network, and restrict physical access to sensitive assets.

- The commission did not consistently manage the configuration of its systems. Configuration management includes ensuring that hardware and software are configured with appropriate security features and that changes are systematically controlled. However, SEC did not maintain and monitor official configuration baselines for its financial systems and general support system.

- The commission did not always appropriately separate incompatible duties. Separation of duties involves dividing responsibilities so that a single individual does not control all critical stages of a process. However, SEC did not adequately separate duties among its three computing environments.

- While SEC had developed contingency and disaster recovery plans for its information systems, those plans were not fully reviewed, completed, or up-to-date. Contingency and disaster recovery planning are essential to resuming operations in the event of a disruption or disaster.

These weaknesses existed in part because SEC had not fully implemented an organization-wide information security program, as called for by federal law and guidance. In particular, the commission had not (1) consistently reviewed and updated its information security policies in a timely manner, (2) completely documented plans of action to address weaknesses, (3) documented a physical inventory of its systems and applications, and (4) fully implemented a program to continuously monitor the security of its systems and networks.

Finally, of 20 weaknesses previously identified by GAO that remained unresolved as of September 30, 2014, SEC had resolved 5 and made progress in addressing the other 15 as of September 30, 2015. Two resolved weaknesses were important to improving SEC security.

Collectively, these weaknesses increase the risk that SEC's systems could be compromised, jeopardizing the confidentiality, integrity, and availability of sensitive financial information. While not constituting material weaknesses or significant deficiencies, they warrant SEC management's attention.

United States Government Accountability Office

Contents

Abbreviations

CIO	chief information officer
EDGAR	Electronic Data Gathering, Analysis, and Retrieval
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
NIST	National Institute of Standards and Technology
POA&M	plan of action and milestones
SEC	Securities and Exchange Commission

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

April 28, 2016

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 November 16, 2015, we issued our report on the audit of the SEC's
fiscal years 2015 and 2014 financial statements.[2] Although we identified
deficiencies in SEC's internal control over financial reporting that we do not
consider to be material weaknesses or significant deficiencies, these
deficiencies warrant SEC management's attention.

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

---

[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 Fiscal Years 2015 and 2014
Financial Statements*, GAO-16-145R (Washington, D.C.: Nov. 16. 2015).

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 assessed the effectiveness of corrective actions taken to address our previously reported weaknesses. This work was performed to support our opinion on SEC's internal control over financial reporting as of September 30, 2015.

We performed our work 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 provided a reasonable basis for our findings and conclusions based on our audit objective. 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 destruction, fraud, or inappropriate disclosure of sensitive information. Accordingly, since 1997, we have designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Most recently, in the February 2015 update to our high-risk

list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)[3]—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.[4]

The Federal Information Security Modernization Act (FISMA) of 2014 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]

---

[3]Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

[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-15-290 (Washington, D.C.: February 2015).

[5]The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) partially superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, FISMA 2002 requirements relevant here that were incorporated and continued in FISMA 2014 and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[6]NIST, *Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53, revision 4 (Gaithersburg, Md.: April 2013).

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

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:

- Various modules in Delphi-Prism, a federal financial management system provided by the Department of Transportation's Federal Aviation Administration's Enterprise Service Center, are used by SEC for financial accounting, analyses, and reporting. Delphi-Prism produces SEC's financial statements.

- 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.

- FedInvest invests funds related to disgorgements and penalties.

- Federal Personnel and Payroll System/Quicktime processes personnel and payroll transactions.

- The SEC's 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 Chairman 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

SEC had implemented and made progress in strengthening information security controls, including implementing access controls, deploying multiple firewalls, establishing monitoring and logging capabilities, and resolving five weaknesses that we had previously identified. However, weaknesses limited the effectiveness of other controls in protecting the confidentiality, integrity, and availability of SEC's information systems. Specifically, SEC did not consistently control logical and physical access to its network, servers, applications, and databases; manage its configuration settings; segregate duties; or update its contingency plan. These weaknesses existed, in part, because SEC did not effectively implement key elements of its information security program, including keeping up-to-date policies and procedures, completely documenting plans of actions and milestones (POA&M) for control weakness remediation, establishing and maintaining configuration settings, and monitoring configuration settings for compliance with standards. Consequently, SEC's financial information and systems were exposed to increased risk of unauthorized disclosure, modification, and destruction.

SEC Did Not Consistently Control Access to Its Financial and General Support Systems

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 destruction. Specific access controls include boundary protection, identification and authentication of users, authorization restrictions, audit and monitoring capability, configuration management, separation of duties, 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 span of authority.

Although SEC had issued policies and implemented controls based on those policies, it did not consistently protect its network from possible intrusions, identify and authenticate users, authorize access to resources,

audit and monitor actions taken on its systems and network, and restrict physical access to sensitive assets.

Although Control Mechanisms Were Put in Place, SEC Did Not Adequately Protect the Internal Boundaries of Its Information Systems from Unauthorized Access

Boundary protection controls (1) logical connectivity into and out of networks and (2) 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 host or device level, logical boundaries can be controlled through inbound and outbound filtering provided by access control lists and personal firewalls. At the system level, any connections to the Internet, or to other external and internal networks or information systems, should occur through controlled interfaces. To be effective, remote access controls should be properly implemented in accordance with authorizations that have been granted.

SEC deployed multiple firewalls that were intended to prevent unauthorized access to its systems; however, it did not always restrict traffic passing through its firewalls. For example, SEC did not always configure access control lists to restrict potentially insecure traffic or ports on each of the six internal firewalls reviewed, subjecting the hosts to potentially vulnerable services. Also, SEC did not apply host firewall configuration rules on three of four hosts. As a result of these inadequate configurations, SEC introduced vulnerability to potentially unnecessary and undetectable access at multiple points in its network environment.

SEC Did Not Consistently Implement Controls for Identifying and Authenticating Users of the EDGAR/Fee Momentum 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 smart card combination. SEC policy requires enforcement of minimum password complexity and password expiration. In addition, SEC policy requires that multifactor authentication be implemented for network and local access to privileged and non-privileged accounts.

However, SEC did not fully implement controls for identifying and authenticating users. For example, it did not always enforce individual accountability, as 20 different users used the same password on multiple servers in the production, development and testing environments. Also, SEC configured the password for a key financial server to never expire.

Additionally, while SEC implemented multifactor authentication for remote access, it did not require multifactor authentication for network or console access managed by the agency's security group. As a result, SEC is at an increased risk that accounts could be compromised and used by unauthorized individuals to access sensitive financial data.

SEC Did Not Always Sufficiently Restrict Access to the EDGAR/Fee Momentum System

Authorization encompasses access privileges granted to a user, program, or process. It involves allowing or preventing actions by that user based on predefined rules. Authorization includes the principles of legitimate use and least privilege.[8] 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. SEC policy states that information system owners shall explicitly authorize access to configuration settings, file permissions, and privileges. SEC policy also states that information systems must prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards or countermeasures.

However, SEC did not always ensure that only authorized individuals were granted access to its systems. For example, it did not promptly remove 9 of 66 expired administrator accounts that we reviewed. In addition, SEC did not appropriately set configuration settings, file permissions, and privileged access to sensitive files, such as allowing group membership not explicitly authorized to access these files. As a result, users had excessive levels of access that were not required to perform their jobs. This could lead to unauthorized users who had penetrated SEC networks inadvertently or deliberately modifying financial data or other sensitive information.

SEC Did Not Consistently 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 investigating and responding to suspicious activities. Audit and monitoring controls can help security professionals routinely assess computer security, perform investigations

---

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

during and after an attack, and 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. SEC policy states that appropriate audit logs shall be generated at all times for SEC information systems, depending on the security categorization of the system and the level of risk associated with the loss, compromise, or unauthorized disclosure of the data processed or transmitted by the system.

However, SEC did not consistently enable audit log configuration settings to capture key security activities on its server hosts reviewed. For example, audit logs for policy settings were not set to be the same for the four server hosts reviewed. As a result, SEC was not able to monitor key activities on some of the server hosts and thus may not be able to detect or investigate unauthorized system activity.

Although SEC Generally Maintained Physical Security of Its Facilities, Weaknesses Existed

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.

SEC instituted physical security controls that included badge swipe readers to enter the building or use the elevators, alarm systems that would sound if exterior doors were propped open for extended periods of time, and additional check points to restrict access to areas housing the EDGAR working space.

However, the effectiveness of its physical security was reduced by weaknesses identified. For example, SEC's facilities service provider did not monitor the perimeter of the contingency site on a real-time basis. In addition, SEC did not adequately secure the server storage area at its contingency site. SEC also did not periodically conduct a physical inventory of employee badges. The insufficient physical access control over the commission's information systems place sensitive information and assets at greater risk from unauthorized access.

SEC Did Not Maintain Standard Baseline Configuration Settings

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 controlling 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. Also, effective configuration management provides reasonable assurance that systems are configured and operating securely and as intended. SEC policy states that the agency should maintain proper system configuration in compliance with official SEC baselines.

SEC did not maintain and monitor official configuration baselines for some of the platforms used to host financially significant systems and general support system that we reviewed. Consequently, increased risk exists that systems could be exposed to vulnerabilities that could be exploited by attackers seeking to gain unauthorized access.

Weaknesses in Segregation of Duties 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. SEC policy states that information system owners must separate duties of individuals as necessary to provide appropriate management and security oversight and define information system access authorizations to support the separation of duties.

However, SEC did not appropriately separate incompatible access to three computing environments for 20 individuals. SEC assigned multiple user accounts to individuals that gave the individuals access to the production, disaster recovery, and test/development environments. SEC officials stated that they had implemented the principles of separation of

duties and accepted the risk for those individuals that required access to multiple environments. However, SEC had not documented management's acceptance of this risk. Thus, an increased risk exists that unauthorized individuals from the disaster recovery environment and test/development environment could gain access to processes and data in the production environment, potentially impacting the integrity of the financial data.

SEC Did Not Fully Review and Update 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 interruption; (2) a plan to recover critical operations should interruptions occur that considers the activities performed at general support facilities, including data processing centers and telecommunication facilities; and (3) redundancy in critical systems. SEC policy states that the agency should provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. This includes establishing an alternate processing site that can operate as the network operation center that permits the transfer and resumption of essential business functions within 12 hours when the primary processing capabilities are unavailable. In addition, SEC policy states that the contingency plan should be reviewed at least annually and updated to address (1) changes to the Commission, information system, or environment of operation and (2) problems encountered during contingency plan implementation, execution, or testing.

Although SEC had developed contingency and disaster recovery plans and implemented controls for this planning, its plans were not complete or up to date. Specifically, SEC did not maintain a sufficiently prepared alternate network operations center in the event of a disaster. Also, SEC did not consistently review and update contingency planning documents. Consequently, SEC had limited ability to monitor the health of its network in the event of a failure at its primary data center.

SEC Did Not Fully Implement Its Information Security Program

The information security weaknesses existed in the SEC computing environment, in part, because SEC had not fully implemented key elements of its agency-wide information security program. Specifically, it did not always (1) review and update its policies in a timely manner, (2) completely document plans of actions and milestones items, (3) document its physical inventory, and (4) fully implement and effectively manage its continuous monitoring program.

SEC Did Not Always Review and Update Its Policies in a Timely Manner

Security control policies and procedures should be documented and approved by management. According to FISMA, each federal agency information security program must include policies and procedures that are based on risk assessments that cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system. SEC policy states that the agency should review and update policy and procedures annually.

SEC did not always review and update its information technology policies and guidance in a timely manner. Specifically, SEC had not reviewed and updated the 10 information technology policies that we reviewed for between 4 and 8 years. In addition, SEC did not review implementing policies for its User Access Program, and one of three of these policies reviewed was dated to 2007. Without appropriate review to ensure up-to-date policies and procedures, increased risk exists that information technology operations would not be in step with current security leading practices or reflect SEC's current operating environment.

SEC Did Not Always Completely Document POA&M Items

When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective. FISMA specifically requires that agency-wide information security programs include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. SEC policy states that a plan of action and milestones (POA&M) will be developed to plan, track, and manage the remedial actions required to address identified information security deficiencies. POA&Ms are based on the findings from security control assessments, security impact analyses, continuous monitoring activities, and other reported deficiencies, including but not limited to Office of Inspector General and GAO engagements. Further, SEC policy states that, at a minimum, each POA&M must include the following for each information security deficiency: tasks planned to correct the deficiency and to address any

residual risk, resources required to accomplish the planned tasks, responsible organizations for implementing the mitigation, any milestones to meet the tasks, scheduled completion dates for each milestone, and the status of corrective action activity.

SEC did not completely document POA&M items. While SEC had made progress in documenting POA&Ms in its repository, the following artifacts supporting closure were not adequately documented in 20 of 20 plans reviewed: tasks planned to correct the weakness and to address any residual risk, milestones in meeting the tasks with the scheduled completion dates, and the status of corrective action activity. Without adequate documentation to support POA&M progress, it would be difficult to determine whether the weakness is properly remedied.

SEC Did Not Always Document the Status of Its Information Systems

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. SEC policy states that the agency should develop, document, and maintain a current baseline configuration for information systems and, for moderate risk systems, review and update baseline configurations at least annually due to patches and common vulnerability enumeration announcements, and as an integral part of information system component installations and upgrades. The policy also states that information system owners of the general support system and major applications should be responsible for developing, documenting, and maintaining an inventory of information system components that accurately reflects the current information system, includes all components within the authorization boundary of the information system, maintains sufficient level of granularity for tracking and reporting, includes information deemed necessary to achieve effective property accountability, and reviews and updates the inventory as part of the system security plan update.

While SEC had a well-documented and up-to-date system security plan for a key financial system that included accurately identified program changes and version numbers, it did not document a comprehensive physical inventory of the systems and applications in its production environments. Specifically, SEC did not document, for each system or application, purpose, host names, operating system version, database version, and location of the system or application in the inventory. In addition, SEC did not adequately review and update current configuration baseline settings documentation for the operating systems. The baselines documentation was last reviewed and approved by SEC management in

fiscal year 2012, including those for the operating systems. Without maintaining an accurate inventory of systems and applications in production and conducting annual review of configuration baselines, SEC may not be able to obtain the current status of its systems and applications and the agency would not be able to identify unauthorized actions performed against the baseline.

SEC Did Not Fully Implement and Effectively Manage Its Continuous Monitoring Program

An important element of risk management is ensuring that policies and controls intended to reduce risk are effective on an ongoing basis. To do this effectively, top management should understand the agency's security risks and actively support and monitor the effectiveness of its security policies. SEC policy states that the agency shall develop a continuous monitoring strategy and implement a continuous monitoring program that includes establishment of system-dependent monthly automated scans for monitoring and reviews at least every other month, ongoing security control assessments, correlation and analysis of security related information generated by assessments and monitoring.

SEC invested in multiple tools with the ability to conduct compliance monitoring for its information systems. However, the agency had not developed a process, including the use of vulnerability scanners, to monitor the configuration of components of a key financial system and evaluate host compliance with SEC policy. For example:

- While scans were run to detect vulnerabilities on SEC systems identified in databases of common vulnerabilities, resulting reports were not sent to database personnel for them to take appropriate actions.
- Personnel for a key financial system were not granted access to the database scanning tool.
- SEC had not instituted processes to review the information produced by the vulnerability scanning tools, including necessary personnel and processes for conducting analysis.

Without implementing an effective process for monitoring, evaluating, and remedying identified weaknesses, SEC would not be aware of potential weaknesses that could affect the confidentiality, integrity and availability of its information systems.

SEC Made Limited Progress Remediating Previously Reported Information Security Control Weaknesses

SEC resolved 5 of the 20 previously reported information security control deficiencies in the areas of access controls, audit and monitoring, and separation of duties that remained unresolved as of September 30, 2014. In particular, SEC resolved 2 weaknesses important to improving its information security by separating the user production network from the internal management network and storing all critical system logs in a centralized location for a key financial system.

While SEC had made progress in addressing the remaining 15 of 20 previously reported weaknesses, these weaknesses still existed as of September 30, 2015. These 15 remaining weaknesses encompassed SEC's financial and general support systems.

Conclusions

While SEC had improved its information security by addressing previously identified weaknesses, the information security control weaknesses that continued to exist in its computing environment may jeopardize the confidentiality, integrity, and availability of information residing in and processed by the system. Specifically, the lack of adequate separation among SEC users in different computing environments increases the risk that users could gain unrestricted access to critical hardware or software and intentionally or inadvertently access, alter, or delete sensitive data or computer programs. Weaknesses in SEC's controls over access control, configuration management, segregation of duties, phys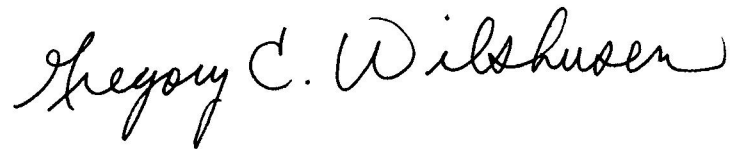ical security, and contingency and disaster recovery planning exist in part because SEC did not fully implement its information security program. In particular, SEC did not always review and update its policies in a timely manner, completely document POA&M items and physical inventory, and fully implement and effectively manage its continuous monitoring program. While SEC had no material weaknesses or significant deficiencies over financial reporting, the weaknesses identified could decrease the reliability of the data processed by key financial systems, which the commission relies on to communicate its financial position to Congress and the public.

Recommendations for Executive Action

We recommend that the Chair direct the Chief Information Officer to take six actions to more effectively manage its information security program:

- Review and appropriately update information technology and guidance consistent with SEC policy.

- Document artifacts that support recommendation closure consistent with SEC policy.

- Document a comprehensive physical inventory of the systems and applications in the production environment.

- Review and update current configuration baseline settings for the operating systems.

- Provide personnel appropriate access to continuous monitoring reports and tools to monitor, evaluate, and remedy identified weaknesses.

- Institute a process and assign the necessary personnel to review information produced by the vulnerability scanning tools to monitor, evaluate, and remedy identified weaknesses.

In a separate report with limited distribution, we are also making 30 recommendations to address newly identified control weaknesses related to access controls, configuration management, segregation of duties, physical security, and contingency and disaster recovery plans.

Agency Comments

We provided a draft of this report to SEC for its review and comment. In written comments signed by the Chief Information Officer (reproduced in app. II), SEC concurred with the six recommendations addressing its information security program. SEC also stated that the commission had taken action to address one recommendation and described actions to address the other five.

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. Because agency personnel serve as the primary source of information on the status of its open recommendations, we request that the commission also provide us with a copy of its statement of action to serve as preliminary information on the status of open recommendations.

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

Our objective was to determine the effectiveness of the Securities and Exchange Commission's (SEC) information security controls for ensuring the confidentiality, integrity, and availability of its key financial systems and information. To assess information systems controls, 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. This work was performed to support our opinion on SEC's internal control over financial reporting as of September 30, 2015.

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; and SEC's plans, policies, and standards. 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 risk 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 and applications, including financial systems and related general support system network devices (firewalls, switches, and routers) servers and systems.

---

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

We also evaluated the Statement on Standards for Attestation
Engagements report[2] and performed testing on key information technology
controls on the following applications and systems: Delphi-Prism, FedInvest,
EDGAR/Fee Momentum, 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.

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.

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 and programmatic personnel to determine
whether the data obtained were consistent with system configurations in
place at the time of our review. In addition, we observed configuration of
these settings in the network. Based on this assessment, we determined
the data were reliable for the purposes of this report.

We performed our work 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 provided a reasonable
basis for our findings and conclusions based on our audit objective.

---

[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.

Appendix II: Comments from the Securities and Exchange Commission

---

April 20, 2016

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) draft recommendations related to opportunities to improve our information security program identified during its audit of the SEC's financial statements for fiscal years 2015 and 2014 (Report GAO-16-493). 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 to include enhancing our capacity to rapidly respond to unauthorized or anomalous activity, improving our enterprise cyber security detection, protection, and prevention mechanisms, and implementing a defense-in-depth security model consistent with guidance from the National Institute of Standards and Technology. The SEC is committed to continuously strengthening our cyber security posture. We are confident in our ability to maintain the confidentiality, integrity, and availability of Commission assets, operations, and data, and welcome the opportunity to further enhance our strong system of internal security controls.

Although the information security issues you identify in the report are associated with internal systems protected by robust perimeter controls and other internal compensating controls, they demonstrate that we have not fully achieved our goals as they relate to implementing our Information Security Program. And while the SEC's defense-in-depth approach includes the use of access controls, redundant and diverse data integrity controls, and emergency response measures, your recommendations provide opportunities for the SEC to enhance its security posture.

As we discussed during your audit engagement, the SEC is continually engaged in efforts to implement additional enhancements to its security controls. One such effort completed just after the conclusion of your audit addressed all recommendations related to account and password management. As you are also aware, a related effort to centralize the management of all Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system components resulted in the retirement of most of the assets you've recommended be further hardened.

As it pertains to separation of duties, EDGAR relies on a team of specialized engineers and analysts who, at times, must perform multiple roles to ensure the SEC can meet its statutory obligations while being a responsible steward of resources. All SEC personnel complete all personnel security requirements as well as security and awareness training. The SEC has implemented numerous security controls implemented to identify and respond to potentially unauthorized individuals or anomalous activity within EDGAR. Further, there are numerous quality control and integrity checks within EDGAR's processing protocols.

Concerning physical access control, the SEC's contingency site operator provides hosting services for multiple Federal agencies. As such, perimeter monitoring and security is provided by the contingency site operator. We plan to discuss your findings with both the site operator and our partners at other agencies.

Report GAO-16-493 contained six recommendations with which the SEC concurs. Below, I have indicated the actions we have taken or intend to take for each recommendation. Further, I am pleased to report that the SEC has already implemented 15 of the recommendations you provided separately related to configuration management, audit logging, and contingency plans. We look forward to sharing our progress. The actions we've taken have already enabled us to more consistently enforce security controls, related processes, and capabilities.

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. I appreciate your continued support and the valuable assistance and guidance from your staff. If you have any questions, or you would like to discuss this response in more detail, please contact me at (202) 551-7095.

Sincerely,

Pamela C. Dyson
Chief Information Officer

Recommendation 1: Review and appropriately update information technology and guidance consistent with SEC policy.

Response: Concur. The Office of Information Technology (OIT) will ensure that all SEC information guidance materials adhere to established review schedules.

Recommendation 2: Document artifacts that support recommendation closure consistent with SEC policy.

Response: Concur. The SEC has taken action to consolidate all audit recommendations into a centralized capability to enhance the management and tracking of all activity related to weakness remediation.

Recommendations 3: Document a comprehensive physical inventory of the systems and applications in the production environment.

Response: Concur. The Commission's computing environment is an evolving and complex collection of information systems, platforms, and capabilities. In order to ensure an accurate and near real-time accounting of SEC information technology resources, the SEC leverages an automated capability. In accordance with this recommendation, OIT will work to ensure its physical asset inventory aligns with inventory data captured in automated mechanisms.

Recommendation 4: Review and update current configuration baseline settings for the operating systems.

Response: Concur. The OIT will ensure configuration baseline settings are current.

Recommendation 5: Provide personnel appropriate access to continuous monitoring reports and tools to monitor, evaluate, and remedy identified weaknesses.

Response: Concur. The SEC is focused on enhancing its continuous monitoring program consistent with the federal government's Information System Continuous Monitoring (ISCM) methodology to improve situational awareness of weaknesses and vulnerabilities.

Recommendation 6: Institute a process and assign the necessary personnel to review information produced by the vulnerability scanning tools to monitor, evaluate, and remedy identified weaknesses.

Response: Concur. The OIT will take action to ensure all necessary personnel have access to vulnerability scanning information in support of ISCM.

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 Gilmore, Hal Lewis, and Duc Ngo (Assistant Directors), Angela Bell, Lee McCracken, and Henry Sutanto.

Appendix IV: Accessible Data

Text of Appendix II:
Comments from the
Securities and Exchange
Commission

Page 1

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, D.C. 20549

April 20, 2016

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) draft recommendations related to opportunities to improve our information security program identified during its audit of the SEC's financial statements for fiscal years 2015 and 2014 (Report GAO-16-493). 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 to include enhancing our capacity to rapidly respond to unauthorized or anomalous activity, improving our enterprise cyber security detection, protection, and

prevention mechanisms, and implementing a defense-in-depth security model consistent with guidance from the National Institute of Standards and Technology. The SEC is committed to continuously strengthening our cyber security posture. We are confident in our ability to maintain the confidentiality, integrity, and availability of Commission assets, operations, and data, and welcome the opportunity to further enhance our strong system of internal security controls.

Although the information security issues you identify in the report are associated with internal systems protected by robust perimeter controls and other internal compensating controls, they demonstrate that we have not fully achieved our goals as they relate to implementing our Information Security Program. And while the SEC's defense-in-depth approach includes the use of access controls, redundant and diverse data integrity controls, and emergency response measures, your recommendations provide opportunities for the SEC to enhance its security posture.

As we discussed during your audit engagement, the SEC is continually engaged in efforts to implement additional enhancements to its security controls. One such effort completed just after the conclusion of your audit addressed all recommendations related to account and password management. As you are also aware, a related effort to centralize the management of all Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system components resulted in the retirement of most of the assets you've recommended be further hardened.

As it pertains to separation of duties, EDGAR relies on a team of specialized engineers and analysts who, at times, must perform multiple roles to ensure the SEC can meet its statutory obligations while being a responsible steward of resources. All SEC personnel complete all personnel security requirements as well as security and awareness training. The SEC has implemented numerous security controls implemented to identify and respond to potentially unauthorized individuals or anomalous activity within EDGAR. Further, there are numerous quality control and integrity checks within EDGAR's processing protocols.

Page 2

Concerning physical access control, the SEC's contingency site operator provides hosting services for multiple Federal agencies. As such, perimeter monitoring and security is provided by the contingency site operator. We plan to discuss your findings with both the site operator and our partners at other agencies.

Report GAO-16-493 contained six recommendations with which the SEC concurs. Below, I have indicated the actions we have taken or intend to take for each recommendation. Further, I am pleased to report that the SEC has already implemented 15 of the recommendations you provided separately related to configuration management, audit logging, and contingency plans. We look forward to sharing our progress. The actions we've taken have already enabled us to more consistently enforce security controls, related processes, and capabilities.

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. I appreciate your continued support and the valuable assistance and guidance from your staff. If you have any questions, or you would like to discuss this response in more detail, please contact me at (202) 551-7095.

Sincerely,

Pamela C. Dyson

Chief Information Officer

Page 3

Recommendation 1: Review and appropriately update information technology and guidance consistent with SEC policy.

Response: Concur. The Office of Information Technology (OIT) will ensure that all SEC information guidance materials adhere to established review schedules.

Recommendation 2: Document artifacts that support recommendation closure consistent with SEC policy.

Response: Concur. The SEC has taken action to consolidate all audit recommendations into a centralized capability to enhance the management and tracking of all activity related to weakness remediation.

Recommendations 3: Document a comprehensive physical inventory of the systems and applications in the production environment.

Response: Concur. The Commission's computing environment is an evolving and complex collection of information systems, platforms, and capabilities. In order to ensure an accurate and near real-time accounting of SEC information technology resources, the SEC leverages an

automated capability. In accordance with this recommendation, OIT will work to ensure its physical asset inventory aligns with inventory data captured in automated mechanisms.

Recommendation 4: Review and update current configuration baseline settings for the operating systems.

Response: Concur. The OIT will ensure configuration baseline settings are current.

Recommendation 5: Provide personnel appropriate access to continuous monitoring reports and tools to monitor, evaluate, and remedy identified weaknesses.

Response: Concur. The SEC is focused on enhancing its continuous monitoring program consistent with the federal government's Information System Continuous Monitoring (ISCM) methodology to improve situational awareness of weaknesses and vulnerabilities.

Recommendation 6: Institute a process and assign the necessary personnel to review information produced by the vulnerability scanning tools to monitor, evaluate, and remedy identified weaknesses.

Response: Concur. The OIT will take action to ensure all necessary personnel have access to vulnerability scanning information in support of ISCM.