



---

July 2017

# INFORMATION SECURITY

## SEC Improved Control of Financial Systems but Needs to Take Additional Actions

# GAO Highlights

Highlights of [GAO-17-469](#), a report to the Chair, U.S. Securities and Exchange Commission

## Why GAO Did This Study

SEC enforces securities laws, issues rules and regulations that provide protection for investors, and helps to ensure that securities markets are fair and honest. SEC uses 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.

Pursuant to statutory authority, GAO assesses the effectiveness of SEC's internal control structure and procedures for financial reporting. As part of its audit of SEC's fiscal years 2016 and 2015 financial statements, GAO assessed whether controls were effective in protecting the confidentiality, integrity, and availability of key financial systems and information. To do this, GAO examined SEC's information security policies and procedures, tested controls, and interviewed key officials on whether controls were in place, adequately designed, and operating effectively.

## What GAO Recommends

In addition to the 11 prior recommendations that have not been fully implemented, GAO recommends that SEC take 13 actions to address newly identified control deficiencies and 2 actions to more fully implement its information security program. In commenting on a draft of this report, SEC concurred with GAO's recommendations.

View [GAO-17-469](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) or Dr. Nabajyoti Barkakati at (202) 512-4499 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov)

July 2017

## INFORMATION SECURITY

# SEC Improved Control of Financial Systems but Needs to Take Additional Actions

## What GAO Found

The Securities and Exchange Commission (SEC) improved the security controls over its key financial systems and information. In particular, as of September 2016, the commission had resolved 47 of the 58 recommendations we had previously made that had not been implemented by the conclusion of the FY 2015 audit. However, SEC had not fully implemented 11 recommendations that included consistently protecting its network boundaries from possible intrusions, identifying and authenticating users, authorizing access to resources, auditing and monitoring actions taken on its systems and network, or encrypting sensitive information while in transmission.

In addition, 15 newly identified control deficiencies limited the effectiveness of SEC's controls for protecting the confidentiality, integrity, and availability of its information systems. For example, the commission did not consistently control logical access to its financial and general support systems. In addition, although the commission enhanced its configuration management controls, it used unsupported software to process financial data. Further, SEC did not adequately segregate incompatible duties for one of its personnel. These weaknesses existed, in part, because SEC did not fully implement key elements of its information security program. For example, SEC did not maintain up-to-date network diagrams and asset inventories in its system security plans for its general support system and its key financial system application to accurately and completely reflect the current operating environment. The commission also did not fully implement and continuously monitor those systems' security configurations. Twenty-six information security control recommendations related to 26 deficiencies found in SEC's financial and general support systems remained unresolved as of September 30, 2016. (See table.)

**SEC Progress Toward Implementing GAO Information Security Recommendations as of September 30, 2016**

Information security control area	Prior GAO recommendations open outstanding at start of fiscal year (FY) 2016 audit	Recommendations closed during FY 2016 audit	New recommendations	Outstanding recommendations end of FY 2016 audit
Information security program	7	(3)	2	6
Access controls	29	(26)	11	14
Other controls	22	(18)	2	6
Totals	58	(47)	15	26

Source: GAO analysis of Securities and Exchange Commission data. | GAO-17-469

Cumulatively, the deficiencies decreased assurance about the reliability of the data processed by key SEC financial systems. While not individually or collectively constituting a material weakness or significant deficiency, these deficiencies warrant SEC management's attention. Until SEC mitigates these deficiencies, its financial and support systems and the information they contain will continue to be at unnecessary risk of compromise.

---

# Contents

---

Letter		1
	Background	2
	Although SEC Strengthened Its Controls, Information Security Deficiencies Placed Financial Data at Risk	5
	Conclusions	14
	Recommendations for Executive Action	15
	Agency Comments and Our Evaluation	15
Appendix I	Objective, Scope, and Methodology	17
Appendix II	Comments from the Securities and Exchange Commission	20
Appendix III	GAO Contacts and Staff Acknowledgments	22
Table		
	Table 1: SEC Made Progress Implementing GAO Information- Security Recommendations	6

---

---

## Abbreviations

ACL	access control list
CIO	chief information officer
EDGAR	Electronic Data Gathering, Analysis, and Retrieval
ESC	Enterprise Service Center
FISMA	Federal Information Security Management Act of 2002 and Federal Information Security Modernization Act of 2014
GSS	General Support System
NIST	National Institute of Standards and Technology
SEC	Securities and Exchange Commission

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



July 27, 2017

The Honorable Jay Clayton  
Chairman  
U.S. Securities and Exchange Commission

Dear Mr. Clayton:

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. The commission relies extensively on computerized systems to support its demanding financial and mission-related responsibilities. 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 the commission have effective information security controls in place.<sup>1</sup>

Pursuant to statutory authority, GAO assesses the effectiveness of SEC's internal control structure and procedures for financial reporting.<sup>2</sup> On November 15, 2016, we issued our report on the audit of SEC's fiscal years 2016 and 2015 financial statements.<sup>3</sup> Although we identified deficiencies in the commission's internal control over financial reporting that we do not consider to be material weaknesses or significant deficiencies, these deficiencies warrant management's attention.

This report presents more detailed information and our recommendations related to the specific information security control deficiencies that we

---

<sup>1</sup>Information security controls include security management, access controls, configuration management, separation 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.

<sup>2</sup>The statutory basis for GAO's review is fully described on pages 1 and 2 of GAO, *Financial Audit: Securities and Exchange Commission's Fiscal Years 2016 and 2015 Financial Statements*, GAO-17-158R (Washington, D.C.: Nov. 15, 2016).

<sup>3</sup>Ibid.

---

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 pertinent to our financial audit, including the system that maintains accounting information pertaining to fees received and general support systems; interviewed key agency officials; and assessed the effectiveness of corrective actions taken to address our previously reported deficiencies. This work was performed to support our opinion on SEC's internal control over financial reporting as of September 30, 2016. See appendix I for more details on our objective, scope, and methodology.

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.

---

## 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 and the information stored on them to various threats.

Cyber threats can be unintentional or intentional. Unintentional or nonadversarial threat sources include failures in equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters. They also include natural disasters and failures of critical infrastructure on which the organization depends but are outside of the control of the organization. Intentional or adversarial threats sources include threats originating from foreign nation states, 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 cyberattack 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 deficiencies that place federal agencies at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, since 1997, we have designated federal information security as a government-wide high-risk area.<sup>4</sup> This was expanded to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015

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.<sup>5</sup> FISMA requires each agency to develop, document, and implement an agency-wide security program. The program is 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. Accordingly, NIST has issued related

---

<sup>4</sup>GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and most recently, GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

<sup>5</sup>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 of the 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 new requirements in FISMA 2014, to 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.

---

standards and guidelines, including *Recommended Security Controls for Federal Information Systems and Organizations*, NIST Special Publication (NIST SP) 800-53,<sup>6</sup> and *Contingency Planning Guide for Federal Information Systems*, NIST SP 800-34.<sup>7</sup>

---

## SEC Relies on Information Technology to Support Its 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<sup>8</sup> paid from enforcement activities, and for financial reporting, SEC relies on numerous enterprise applications, including:

- Delphi-Prism is the financial accounting and reporting system operated by the Federal Aviation Administration's<sup>9</sup> Enterprise Service Center (ESC). SEC uses various modules of this system for financial accounting, analyses, and reporting. Delphi-Prism also produces the SEC financial statements.
- Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system which 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, which maintains accounting information pertaining to fees received from registrants.

---

<sup>6</sup>National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, Md.: April 2013).

<sup>7</sup>National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34, revision 1 (Gaithersburg, Md.: May 2010).

<sup>8</sup>A disgorgement is the repayment of illegally gained profits (or avoided losses) for distribution to harmed investors whenever feasible. A penalty is a monetary payment from a violator of securities law that SEC obtains pursuant to statutory authority. A penalty is fundamentally a punitive measure, although penalties occasionally can be used to compensate harmed investors.

<sup>9</sup>The Federal Aviation Administration is a component agency of the Department of Transportation.



- 
- FedInvest, which invests funds related to disgorgements and penalties.
  - Federal Personnel and Payroll System/Quicktime (FPPS/Quicktime), which processes personnel and payroll transactions.
  - General Support System (GSS), which provides (1) business application services to internal and external customers and (2) security services necessary to support these applications. SEC's GSS is a combination of infrastructure that includes the Windows-based local area network that authorizes SEC employees and contractors to use the underlying network environment, and various perimeter security devices such as routers, firewalls, and switches.

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 security for the information and 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 also requires the CIO to designate a senior agency information security officer to carry out the information security-related responsibilities.

---

## Although SEC Strengthened Its Controls, Information Security Deficiencies Placed Financial Data at Risk

During GAO's fiscal year 2016 audit, SEC had demonstrated considerable progress in improving information security by implementing 47 of the 58 recommendations we had made in prior audits that had not been implemented by the conclusion of the fiscal year 2015 audit. Nevertheless, although SEC submitted evidence of taking action to resolve all 58 previously reported recommendations, its actions were not sufficient to fully resolve 11 recommendations.

In addition, 15 deficiencies identified during the fiscal year 2016 audit limited the effectiveness of SEC's controls for protecting the confidentiality, integrity, and availability of its information systems. For example, the commission did not consistently control logical access to its financial and general support systems. It also used unsupported software to process financial data. Further, while SEC generally implemented separation of duties, it allowed incompatible duties for one person. These deficiencies existed, in part, because the commission did not fully implement key elements of its information security program.

The newly identified deficiencies resulted in 2 recommendations to SEC to more fully implement aspects of its information security program and 13 recommendations to enhance access controls and other security controls over its financial systems. Table 1 summarizes SEC's progress toward addressing the prior and newly identified information security recommendations.

**Table 1: SEC Made Progress Implementing GAO Information-Security Recommendations**

Control area	Prior recommendations not implemented by the conclusion of the FY 2015 audit	Recommendations implemented by the end of FY 2016 audit	Prior recommendations not fully implemented at the end of FY 2016 audit	New recommendations made during FY 2016 audit	Total outstanding recommendations at the conclusion of FY 2016 audit
<b>Access controls</b>					
Boundary protection	5	4	1	5	6
Identification and authentication	9	(8)	1	1	2
Authorization	8	(7)	1	3	4
Cryptography	3	(3)	0	1	1
Audit and monitoring	4	(4)	0	1	1
Physical security	6	(5)	1	0	1
<b>Other security controls</b>					
Configuration management	9	(6)	3	1	4
Separation of duties	2	(2)	0	1	1
Contingency planning	5	(5)	0	0	0
<b>Information security program</b>	7	(3)	4	2	6
<b>Total:</b>	<b>58</b>	<b>(47)</b>	<b>11</b>	<b>15</b>	<b>26</b>

Source: GAO analysis of Securities and Exchange Commission data.

Cumulatively, the deficiencies decreased assurance about the reliability of the data processed by key SEC financial systems. While not individually or collectively constituting a material weakness or significant deficiency, these deficiencies warrant SEC management's attention. Until SEC mitigates these deficiencies, its financial and support systems and the information they contain will continue to be at unnecessary risk of compromise.

---

---

**SEC Made Significant Progress Remediating Previously Reported Information Security Control Deficiencies**

SEC resolved 47 of the 58 previously reported information system control deficiencies in the areas of security management, access controls, configuration management, and separation of duties.<sup>10</sup> For example, the commission offered physical security awareness training to its employees; enforced password expiration on the key financial application server; set access permission for sensitive files; and operated a fully functioning contingency operations site that would be used in the event of a disaster.

Nevertheless, SEC had not fully mitigated 11 of the 58 previously reported deficiencies affecting its financial and general support systems. For example, SEC had not maintained and monitored firewall configuration baseline rules for its firewalls and it had not documented a comprehensive physical inventory of the systems and applications in the production environment. As of September 2016, SEC was still at risk because it did not have baselines needed to define and monitor changes to its systems, applications, and inventory.

---

**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 loss. Specific access controls include (1) boundary protection, (2) identification and authentication of users, (3) authorization restrictions, (4) cryptography, (5) audit and monitoring procedures, and (6) 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: (1) protect its network boundaries from possible intrusions; (2) identify and authenticate users; (3) authorize

---

<sup>10</sup>See table 1 for details.

---

access to resources; (4) audit and monitor actions taken on the commission's systems and network; and (5) encrypt sensitive information while in transmission.

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

Boundary protection controls provide logical connectivity into and out of networks as well as 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 cyberattack. For example, multiple firewalls can 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<sup>11</sup> (ACL) and host-based 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.

For one key financial system, SEC consolidated all internal firewalls in order to better manage its boundary protection controls; however, it configured the ACLs on the host-based firewalls supporting the key financial system's servers to allow excessive inbound and outbound traffic. As a result, SEC introduced a vulnerability that could allow unauthorized access to the system.

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

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 identification combination. SEC policy requires default passwords in operating systems, databases, and web servers to be changed upon installation. Also, the policy states that information system owners should review user accounts and associated access privileges policy to ensure appropriate access and that terminated or transferred employees do not retain improper information system access.

---

<sup>11</sup>Access control list (ACL) consists of a register of users (including groups, machines, processes) who have been given permission to use a particular system resource, and lists the types of access for which they have authorization.

---

SEC Did Not Always  
Sufficiently Restrict Access to  
Financial Systems

However, SEC did not fully implement controls for identifying and authenticating users. For example, it did not always enforce individual accountability as 13 of 42 user accounts reviewed had the same default password in the three key financial systems' servers that we reviewed. Also, SEC did not disable these 13 active user accounts although they had never been used. As a result, increased risk exists that the accounts could be compromised and used by unauthorized individuals to access sensitive financial data.

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."<sup>12</sup> 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 system owners shall explicitly authorize access to file permissions and privileges, including approving, authorizing, and documenting system account actions (create, modify, disable, remove) for the specified resources in which the users have primary responsibility as well as reviewing access authorizations and granting or denying access to SEC information and information systems. SEC policy also states that information systems must prevent nonprivileged users from executing privileged functions; including disabling, circumventing, or altering implemented security safeguards or countermeasures.

However, SEC did not always adequately restrict access privileges to ensure that only authorized individuals were granted access to its systems. In addition, SEC did not consistently monitor the role-based access privileges assigned to user groups for an externally managed financial system. The Enterprise Service Center (ESC) assigned SEC users to user groups with access privileges in the ESC Prism application that were not always consistent with the privileges authorized by SEC policy or access request forms. For example, ESC assigned 16 of 24 ESC Prism users to groups that were not used by SEC. As a result, users had excessive levels of access that were not required to perform their jobs. This could lead insiders or attackers who penetrate SEC networks to

---

<sup>12</sup>Users should have the least amount of privileges (access to services) necessary to perform their duties.

---

inadvertently or deliberately modify financial data or other sensitive information.

**SEC Did Not Fully Encrypt Sensitive Information**

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. 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 to prevent unauthorized disclosure of information stored on agency networks.

However, SEC did not fully encrypt sensitive information stored on servers supporting a key financial system. Without proper encryption, increased risk exists that unauthorized users could identify and use the information to gain inappropriate access to system resources.

**SEC Did Not Fully Implement an Intrusion Detection Capability on a Financial System**

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. These controls can help security professionals routinely assess computer security, perform investigations 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. Using automated mechanisms can help integrate audit monitoring, analysis, and reporting into an overall process for investigating and responding to suspicious activities. SEC policy states that intrusion detection parameters should be explicitly set.

However, SEC did not fully implement an intrusion detection capability for key financial systems. As a result, SEC may not be able to detect or investigate some unauthorized system activity.

**Although SEC Improved Its Configuration Management Controls, It Used Unsupported Software**

Configuration management controls provides reasonable assurance that systems are configured securely and operating as intended. As part of its configuration management efforts, SEC policy requires protection from malicious code, including detection and eradication. In addition, patch management, a component of configuration management, is an important element in mitigating the risks associated with known vulnerabilities.

---

When a vulnerability is discovered, the vendor may release a patch<sup>13</sup> to mitigate the risk. If a patch is not applied in a timely manner or if a vendor no longer supports the system and does not prepare a patch, an attacker can exploit a known vulnerability not yet mitigated, enabling unauthorized access to the system or enabling users to have access to greater privileges than authorized.

SEC improved several configuration management controls for its financial information systems. For example, it conducted malicious code reviews and ensured only approved software changes were made. In addition, SEC enhanced its patch management process by scheduling and deploying patches for its two operating system platforms on its financial application servers.

However, SEC also used software that was no longer supported by the software's vendor. Specifically, the commission continued to use an outdated version of an operating system on its key financial systems although the operating system's vendor stopped supporting this version of the software over a decade ago and no longer develops or releases patches for the software. As a result, increased risk exists that an attacker could exploit newly discovered vulnerabilities associated with the outdated operating system.

### SEC Generally Implemented Separation of Duties with One Exception

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 separation of duties starts with effective entity-wide policies and procedures that are implemented at the system and application levels. Often, separation 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 separation 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

---

<sup>13</sup>A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

---

management and security oversight and define information system access authorizations to support the separation of duties.

SEC was successful in employing separation of duties control, with one exception. Of the 217 ESC Prism users, the commission assigned one user to two roles that violated the separation of duties' principle. Although the violation only involved one person, it was significant because of the importance of the roles involved. The user was assigned to both the "contracting officer's security group" and the "requisitioner's security group with requisition approval." According to an SEC official, users assigned to the contracting officers security group have the access permissions to approve and obligate awards, and users assigned to the requisitioner's security group can, with approval, commit funds. As a result of being in both security groups, this person had the ability to both approve and obligate awards and then commit funds.

---

### SEC Did Not Fully Implement Aspects of Its Information Security Program

An information security program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. An underlying reason for the information security control deficiencies in SEC's financial systems was that, although the agency developed and documented an information security program, it did not fully implement aspects of the program. In particular, SEC did not always update system security plans or fully implement its continuous monitoring capability. In addition, SEC made significant progress resolving previous-reported deficiencies but several deficiencies remained partially unresolved.

### SEC Did Not Always Keep Systems Security Plans Complete and Accurate

FISMA requires each federal agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements, including subordinate plans for providing adequate information security for networks, facilities, and systems or groups of systems, as appropriate. Consistent with this requirement, SEC policy states that information system owners of the GSS and major applications should be responsible for developing, documenting, and maintaining an inventory of information system components that: accurately reflects the current system; includes all components within the authorization boundary of the system; and provides the level of granularity deemed necessary for tracking and reporting within the system. In addition, SEC policy requires that the system component inventory be reviewed and updated when components are installed or removed and when system



---

security plans are updated. Further, SEC policy states that the system security plan should be updated throughout the system life cycle.

However, SEC did not update its system security plans to reflect the current operational environment. For example, it did not update network diagrams and asset inventories in the system security plans for GSS and a key financial system. Each of the several iterations of network diagrams and supporting schedules SEC provided to us during the audit reflected incomplete or inaccurate representations of the operating environment. To illustrate, inconsistencies existed among the network diagrams, reports from SEC's automated asset tracking tool, and results from the automated scanning of the environment. Additionally, several previously decommissioned components remained installed, powered on, and accessible on its network.

The system security plans were not current because SEC personnel did not update the plans, asset inventory, or network diagrams during the current modernization of the key financial system's environment. The modernization effort, along with other routine maintenance, had increased the frequency of hardware added to or removed from the environment. The commission did not remove assets from the inventory or update the network diagram until the hardware had been physically removed from the data center even though the hardware was not operational. Without up-to-date, complete, and accurate system inventories and network diagrams in the system security plans, SEC lacks the baseline configurations settings to adequately secure its systems.

### SEC Did Not Fully Implement Continuous Monitoring

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. NIST guidance and SEC policy state that the agency should develop a continuous monitoring strategy. SEC policy requires implementation of a continuous monitoring program that is to include (1) establishment of system-dependent monthly automated scans, (2) ongoing security control assessments, and (3) correlation and analysis of security related information generated by assessments.

SEC did not fully implement and continuously monitor its secure configurations. While it made improvements to address prior-year GAO recommendations by developing and documenting approved secure configuration baselines based on NIST's National Checklist Program, SEC had not fully implemented those secure configurations across the

---

infrastructure present in the GSS and key financial systems. Further, although the commission employed a technology to facilitate automated configuration compliance scanning throughout the GSS and the key financial systems, it determined this technology to be too inefficient and cumbersome to facilitate automated scanning of technical configuration compliance and, during the fiscal year 2016 audit, was in the process of replacing it with a new capability. Thus, it did not consistently perform compliance scanning on multiple operating systems, databases, and network devices.

However, such scanning is important for identifying vulnerabilities existing in a network. Our scans of SEC IT resources identified vulnerabilities affecting operating systems, databases, and network devices. Although additional analysis and coordination by responsible SEC organizations may have determined that some of the potential vulnerabilities may have been mitigated by compensating controls or other factors, the lack of processes noted above increase the risk that known vulnerabilities or misconfigurations will not be identified and remediated in a timely manner. Without implementing an effective process for monitoring, evaluating, and remedying identified deficiencies, SEC would not be aware of potential deficiencies that could affect the integrity and availability of its information systems.

---

## Conclusions

Information security control deficiencies in the SEC computing environment may jeopardize the confidentiality, integrity, and availability of information residing in and processed by its systems. Specifically, SEC configured its internal firewalls to allow too many internal users without legitimate business needs to access a key financial system environment. SEC also did not enable host based firewalls on all key financial system and a major operating system server, which made them vulnerable to unauthorized changes. In addition, SEC operated a financial system server with an unsupported operating system, risking exposure of financial data.

Further, deficiencies exist in part because SEC did not maintain up-to-date network diagrams and asset inventories in the system security plans for GSS and a key financial system to accurately and completely reflect the current operating environment, and it also did not fully implement and continuously monitor GSS and the key financial system's secure configurations. Cumulatively, these deficiencies decreased assurance regarding the reliability of the data processed by key financial systems. Until SEC mitigates its control deficiencies, its financial and support

---

systems and the information they contain will continue to be at unnecessary risk of compromise.

---

## Recommendations for Executive Action

We recommend that Chairman of the SEC take two actions to more effectively manage its information security program:

- Maintain up-to-date network diagrams and asset inventories in the system security plans for GSS and a key financial system to accurately and completely reflect the current operating environment.
- Perform continuous monitoring using automated configuration and vulnerability scanning on the operating systems, databases, and network devices.

To address specific deficiencies in information security controls, we made 13 detailed recommendations in a separate limited official use only report. Those recommendations address access control, configuration management, and separation of duties.

---

## Agency Comments and Our Evaluation

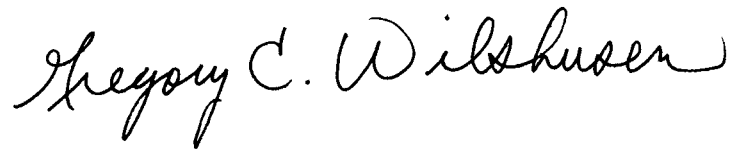
We received written comments on a draft of this report from SEC. In its comments, which are reprinted in appendix II, the commission concurred with the two recommendations addressing its information security program. If effectively implemented, these actions should enhance the effectiveness of SEC's controls over its financial systems. In addition, SEC's Chief Information Security Officer provided technical comments on the draft report via e-mail, which we considered and incorporated, as appropriate.

---

---

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](mailto:wilshuseng@gao.gov) or Nabajyoti Barkakati at (202) 512-4499 or [barkakatin@gao.gov](mailto: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

---

Pursuant to statutory authority, GAO assesses the effectiveness of the Securities and Exchange Commission's (SEC) internal control structure and procedures for financial reporting. Our 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 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, 2016.

We concentrated our evaluation primarily on the controls for systems and applications associated with financial processing. These systems were the (1) Delphi-Prism; (2) Electronic Data Gathering, Analysis, and Retrieval (EDGAR); (3) EDGAR/Fee Momentum; (4) FedInvest; (5) Federal Personnel and Payroll System/Quicktime and (6) general support systems. Our selection of the systems to evaluate was based on consideration of financial systems and service providers integral to SEC's financial statements.

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;<sup>14</sup> 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 SEC policies and procedures;
- observing technical controls implemented on selected systems;
- testing specific controls; and

---

<sup>14</sup>GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

- 
- scanning and manually assessing SEC systems and applications, including EDGAR/Fee Momentum, and related general support system network devices, and servers.

We also evaluated the Statement on Standards for Attestation Engagements report<sup>15</sup> and performed testing on key information technology controls on the following applications and systems: Delphi-Prism, FedInvest, and Federal Personnel and Payroll System.

To determine the status of SEC's actions to correct or mitigate previously reported information security deficiencies, we identified and reviewed its information security policies, procedures, practices, and guidance. We reviewed prior GAO reports to identify previously reported deficiencies and examined the commission's corrective action plans to determine which deficiencies it had reported as 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, specific control evaluations for each accounting cycle, and security policies and procedures, we corroborated them by interviewing SEC officials, including programmatic personnel, and system administrators 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

---

<sup>15</sup>SEC's service provider contracts with an independent auditor to perform an audit of controls related to its service operations under Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. SSAE No. 16 provides authoritative guidance for service auditors to report on the design and operating effectiveness of controls at organizations that provide services to user entities, such as SEC, when those controls are likely to be relevant to user entities' internal control over financial reporting. The issuance of a service auditor's report prepared in accordance with SSAE No. 16 signifies that a service organization has had its control objectives and control activities examined by an independent auditing firm. The service auditor's report includes valuable information regarding the service organization's controls and the effectiveness of those controls, and also identifies complementary user entity controls that should be implemented by the user entity to ensure that its control objectives are met. AT Section 801, Reporting on Controls at a Service Organization, defines complementary user entity controls as controls that management of the service organization assumes, in designing the service to be provided, will be implemented by user entities, and that if necessary to achieve the control objectives stated in management's description of the service organization's system, are identified as such in that description.

---

assessment, we determined the data were reliable for the purposes of this report.

We performed this 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.

# Appendix II: Comments from the Securities and Exchange Commission



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

July 14, 2017

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 information security identified during its audit of the SEC's financial statements for fiscal years 2016 and 2015 (Report GAO-17-469). 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 made considerable progress in implementing our information security program and remediating previously reported information security control deficiencies. The SEC is committed to continuously assessing and strengthening our information security posture.

The SEC concurs with both of the recommendations in your report. Below, I have indicated the actions we have taken or intend to take for each recommendation. I am also happy to report that many of the GAO's observations related to initiatives the SEC was actively implementing during the FY16 audit period have now been completed. This includes modernizing a major financial system and completing a major enhancement to our vulnerability management capability.

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:** Maintain up-to-date network diagrams and asset inventories in the system security plans for GSS and a key financial system to accurately and completely reflect the current operating environment.

**Response:** Concur. The Office of Information Technology (OIT) will take action to ensure appropriate system stakeholders are aware of authoritative network diagrams and inventories and develop protocols to ensure materials are reviewed and updated on a periodic basis.

**Recommendation 2:** Perform continuous monitoring using automated configuration and vulnerability scanning on the operating systems, databases, and network devices.

**Response:** Concur. OIT recently replaced its legacy vulnerability management system with an enhanced capability. OIT has taken action to implement a number of new protocols to better streamline compliance and vulnerability scanning.

---

# Appendix III: GAO Contacts and Staff Acknowledgments

---

---

## GAO Contacts

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

Nabajyoti Barkakati, (202) 512-4499 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov)

---

## Staff Acknowledgments

In addition to the contacts named above, GAO staff who made major contributions to this report are Michael Gilmore and Duc Ngo (Assistant Directors); Angela Bell; Monica Perez-Nelson; Priscilla Smith; Henry Sutanto (Analyst-in-Charge) and Adam Vodraska.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [LinkedIn](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov) and read [The Watchblog](#).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

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

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

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

---

## Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.