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.

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.

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.)

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.