***Inspector General's Report on Covered Systems* (August 11, 2016)**

In accordance with the Cybersecurity Act of 2015 (the Act),[1] the U.S. Securities and Exchange Commission (SEC) Office of Inspector General (OIG) reported to Congressional committees of jurisdiction information about the SEC's covered systems. The term ''covered system'' means a national security system as defined in 40 U.S.C. § 11103 or a Federal computer system that provides access to personally identifiable information. SEC information systems meet the definition of "covered system" as the systems provide access to personally identifiable information.

To respond to the Act's reporting requirements, the OIG interviewed SEC Office of Information Technology personnel, including the Chief Information Security Officer, and reviewed information for a sample of the SEC's covered systems. We reported the following information for the SEC's covered systems based on the requirements of the Act:

- Description of logical access policies and practices.
- Description and list of the logical access controls and multifactor authentication used to govern privileged users access.
- Reasons for not using logical access controls and multifactor authentication if applicable.
- Description of information security management practices including policies and procedures used to conduct inventories of software and licenses, capabilities utilized to monitor and detect exfiltration and other threats, description of how monitoring and detecting capabilities are utilized, and reasons why monitoring and detecting capabilities are not used if applicable.
- Description of policies and procedures used to ensure entities, including contractors, providing services to the SEC are implementing the information security management practices identified in the Act.

Because this report contains sensitive information about the SEC's information security program, we are not releasing it publicly.

[1] Pub. L. 114-113, Division N, 129 Stat. 2242 (2015).