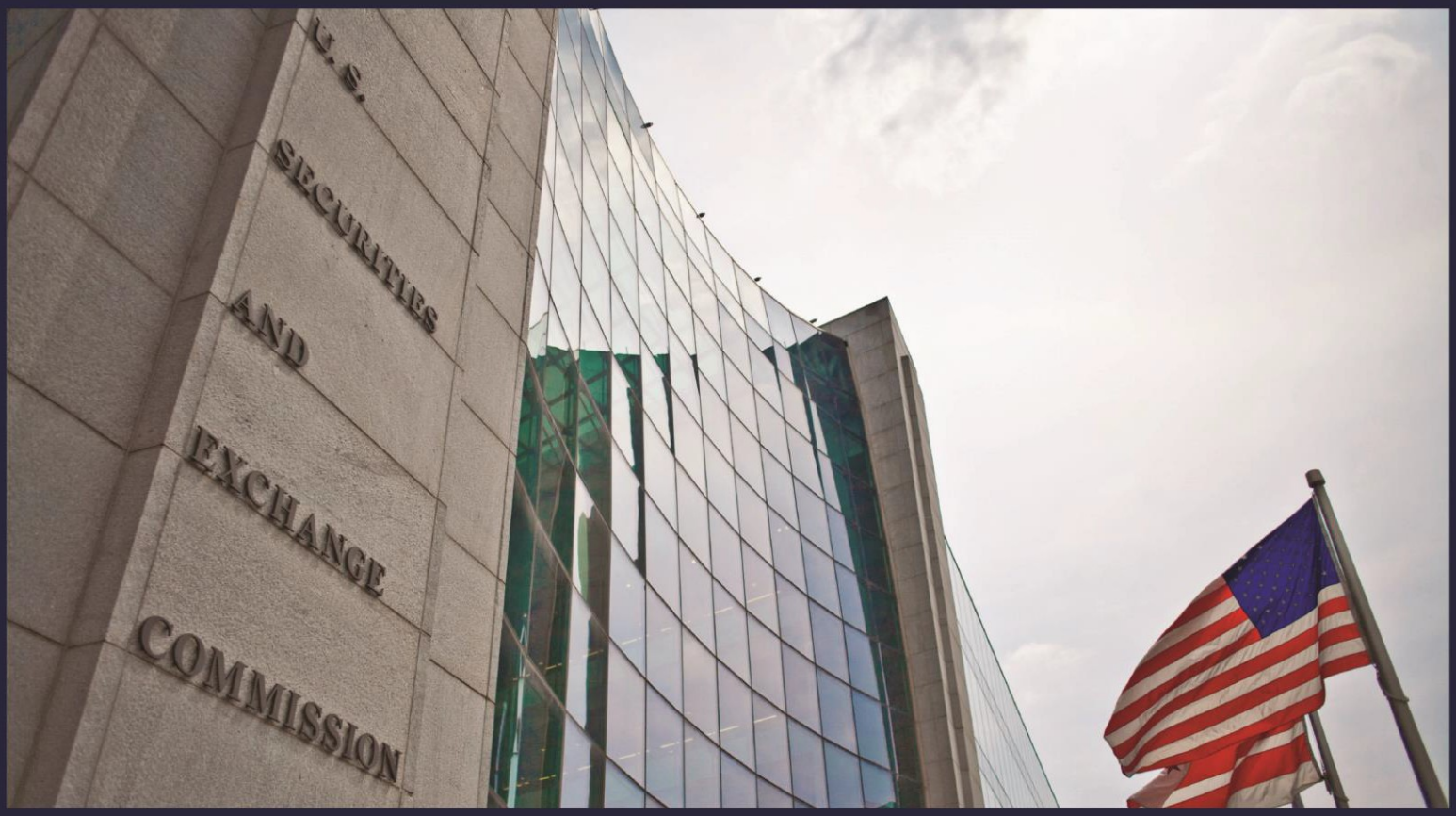
U.S. Securities and Exchange Commission

Office of Inspector General

Office of Audits

Evaluation of the EDGAR System's Governance and Incident Handling Processes



September 21, 2018
Report No. 550

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

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

September 21, 2018

TO: Kenneth Johnson, Chief Operating Officer

FROM: Carl W. Hoecker, Inspector General

SUBJECT: *Evaluation of the EDGAR System's Governance and Incident Handling Processes*, Report No. 550

Attached is the Office of Inspector General (OIG) final report detailing the results of our evaluation of the U.S. Securities and Exchange Commission's (SEC) Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system governance and incident handling processes. The report contains 14 recommendations that, if fully implemented, should improve the SEC's EDGAR system governance, security practices, and incident handling processes.

On September 10, 2018, we provided management with a draft of our report for review and comment. In its September 19, 2018, response, management concurred with our recommendations. We have included the response as Appendix III in the final report.

Within the next 45 days, please provide the OIG with a written corrective action plan that addresses the recommendations. The corrective action plan should include information such as the responsible official/point of contact, timeframe for completing required actions, and milestones identifying how the agency will address the recommendations.

We appreciate the courtesies and cooperation extended to us during the evaluation. If you have questions, please contact me or Rebecca L. Sharek, Deputy Inspector General for Audits, Evaluations, and Special Projects.

Attachment

cc: Jay Clayton, Chairman
Lucas Moskowitz, Chief of Staff, Office of Chairman Clayton
Sean Memon, Deputy Chief of Staff, Office of Chairman Clayton
Peter Uhlmann, Managing Executive, Office of Chairman Clayton
Kara M. Stein, Commissioner
Robert Peak, Advisor to the Commissioner, Office of Commissioner Stein
Robert J. Jackson Jr., Commissioner
Caroline Crenshaw, Counsel, Office of Commissioner Jackson
Prashant Yerramalli, Counsel, Office of Commissioner Jackson
Hester M. Peirce, Commissioner
Jonathan Carr, Counsel, Office of Commissioner Peirce
Elad Roisman, Commissioner
Christina Thomas, Counsel, Office of Commissioner Roisman

Robert B. Stebbins, General Counsel
Jeffrey Finnell, Deputy General Counsel for Adjudication and Legal Policy, Office of the General Counsel
Rick A. Fleming, Investor Advocate
John J. Nester, Director, Office of Public Affairs
Bryan Wood, Director, Office of Legislative and Intergovernmental Affairs
Pamela C. Dyson, Chief Information Officer, Office of Information Technology
Andrew V. Krug, Chief Information Security Officer, Office of Information Technology
Charles Riddle, Chief Technology Officer, Office of Information Technology
Mark Ambrose, Director, EDGAR Business Office
Julie Erhardt, Acting Chief Risk Officer, Office of the Chief Operating Officer

Executive Summary

Evaluation of the EDGAR System's Governance and Incident Handling Processes
Report No. 550
September 21, 2018

Why We Did This Evaluation

On September 20, 2017, the Chairman of the U.S. Securities and Exchange Commission (SEC or agency) publicly disclosed that an incident—specifically, a software vulnerability in a component of the agency's Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system—previously detected in 2016 resulted in unauthorized access to non-public information. On September 23, 2017, the Chairman, who began his service in May 2017 and was notified of the incident in August 2017, requested that the Office of Inspector General (OIG) review the agency's handling of, and response to, the 2016 incident. In response, the OIG initiated an evaluation. In July 2018, the OIG presented the Chairman and other SEC Commissioners with the non-public results of its evaluation relative to the 2016 EDGAR intrusion. This report presents the OIG's findings related to the information security practices applicable to the EDGAR system between fiscal years 2015 and 2017.

What We Recommended

We made 14 recommendations to improve the SEC's EDGAR system governance, security practices, and incident handling processes. We also noted that open recommendations from prior OIG work should address some of our observations, and we encourage management to implement agreed-to corrective actions. Management concurred with the recommendations, which will be closed upon completion and verification of corrective action.

What We Found

EDGAR is at the heart of the agency's mission of protecting investors; maintaining fair, orderly, and efficient markets; and facilitating capital formation. The availability of accurate, complete, and timely information from EDGAR is essential to the SEC's mission and the investing public. Without adequate controls to ensure the SEC identifies, handles, and responds to EDGAR system incidents in a timely manner, threat actors could gain unauthorized access to the system, which could lead to illicit trading, negative impacts to the economy and public access to filings, and loss of public confidence in the SEC.

We determined that, between fiscal years 2015 and 2017, the EDGAR system lacked adequate governance commensurate with the system's importance to the SEC's mission.

In addition, we determined that certain preventive controls either did not exist or operate as designed. Moreover, between September 2015 and September 2016, the SEC wasted at least $83,000 on a tool for which the SEC derived little, if any, benefit.

Finally, we found that the SEC lacked an effective incident handling process.

These weaknesses potentially increased the risk of EDGAR security incidents, and impeded the SEC's response efforts. The SEC has since strengthened EDGAR's system security posture, including the handling of and response to vulnerabilities. Among other actions, in August 2017, the agency established a Cyber Initiative Working Group to oversee and lead a number of priority cyber initiatives such as an EDGAR security uplift. As this and other work continues, opportunities for further improvement exist.

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

For additional information, contact the Office of Inspector General at (202) 551-6061 or http://www.sec.gov/oig.

Major Contributors to the Report

Kelli Brown-Barnes, Audit Manager

Mike Burger, Lead Auditor

John Dettinger, Auditor

Sean Morgan, Assistant Counsel

Sara Tete Nkongo, Auditor

David Witherspoon, Senior Attorney

To Report Fraud, Waste, or Abuse, Please Contact:

Web: https://www.sec.gov/oig

Telephone: 1-833-SEC-OIG1 (833-732-6441)

Address: U.S. Securities and Exchange Commission
Office of Inspector General
100 F Street, N.E.
Washington, DC 20549

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits, evaluations, or reviews, please send an e-mail to OIG Audit Planning at AUDplanning@sec.gov. Comments and requests can also be mailed to the attention of the Deputy Inspector General for Audits, Evaluations, and Special Projects at the address listed above.