



governmentattic.org

"Rummaging in the government's attic"

Description of document: Table of contents and title page of the Securities and Exchange Commission (SEC), Office of Information Technology, Security Operations, SEC Incident Response Capability Handbook, 2014

Requested date: 13-February-2017

Appealed date: 23-February-2017

Released date: 10-March-2017

Posted date: 07-August-2017

Source of document: FOIA Request
Securities and Exchange Commission
100 F Street NE
Mail Stop 2465
Washington D.C. 20549
Fax: 202-772-9337
[Online Request for Copies of Documents](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



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

OFFICE OF THE
GENERAL COUNSEL

Stop 9612

March 10, 2017

Re: Appeal, Freedom of Information Act Request No. 17-01451-FOIA, designated on appeal as No. 17-00237-APPS

This responds to your Freedom of Information Act (FOIA) appeal of the FOIA Officer's decision regarding your January 25, 2017 FOIA request for a "copy of the table of contents and title page of the SEC, Office of Information Technology, Security Operations, SEC Incident Response Handbook, April 2014." By letter dated February 23, 2017, the FOIA Office informed you that its search did not locate any responsive records. On February 23, 2017, you filed an appeal challenging the FOIA Office's determination that no responsive records exist.

As my staff has located the records you seek, your appeal is granted. Enclosed are copies of the table of contents and title page of the SEC's April 2014 Security Incident Response Handbook. If you have any questions regarding this determination, please contact Mark Tallarico, Senior Counsel, at 202-551-5132.

For the Commission
by delegated authority,

A handwritten signature in black ink, appearing to read "R. Humes".

Richard M. Humes
Associate General Counsel

Enclosures

SEC Incident Response Capability Handbook



April 2014

Securities and Exchange Commission
Office of Information Technology
Security Operations

TABLE OF CONTENTS

- 1. Introduction..... 1
 - 1.1. Purpose 1
 - 1.2. Scope 1
 - 1.3. Authority 1
- 2. Procedures for Responding to Incidents 1
 - 2.1. Background 1
 - 2.2. Events and Incidents..... 2
 - 2.3. Definitions..... 2
 - 2.4. Reportable Incident Criteria for the SEC 2
 - 2.5. CSIRC Incident Identification..... 2
- 3. Incident Response Processes..... 3
 - 3.1. Preparation Stage..... 3
 - 3.2. Detection and Analysis Stage..... 3
 - 3.3. Containment, Eradication and Recovery Stage..... 5
 - 3.4. Handling Digital Evidence (Forensics Examination) 5
 - 3.5. Data Analysis 6
 - 3.6. Recovery 6
- 4. Post-Incident Activity Stage 6
- 5. Roles and Responsibilities 7
- Appendix A-Root Cause Analysis 9**
- Appendix B-Standards and Guidelines..... 11**
- Appendix C-Forms..... 34**
- Appendix D-Security Service Contacts 42**