UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
STATION PLACE
100 F STREET, NE
WASHINGTON, DC 20549-2465

Office of FOIA Services

April 12, 2017

Mr. John Greenewald
The Black Vault
[redacted]

Re: Freedom of Information Act (FOIA), 5 U.S.C. § 552
Request No. 17-01971-FOIA

Dear Mr. Greenewald:

This letter is in response to your request, dated February 27, 2017 and received in this office on February 28, 2017, for a copy of the SEC "Incident Response Capability Handbook" as referenced by the 2009 FISMA Executive Summary.

The search for records resulted in the location and production of the requested Handbook, consisting of 44 pages. We are releasing 13 pages from the Handbook. The balance of the Handbook, as well as portions of the released pages, are protected from disclosure under 5 U.S.C. § 552(b)(7)(E), 17 CFR § 200.80(b)(7)(i)(v). If released, the information could reasonably be expected to reveal specific investigative techniques and procedures.

I am the deciding official with regard to this adverse determination. You have the right to appeal my decision to the SEC's General Counsel under 5 U.S.C. § 552(a)(6), 17 CFR § 200.80(d)(5)(iv). The appeal must be received within ninety (90) calendar days of the date of this adverse decision. Your appeal must be in writing, clearly marked "Freedom of Information Act Appeal," and should identify the requested records. The appeal may include facts and authorities you consider appropriate.

You may file your appeal by completing the online Appeal form located at https://www.sec.gov/forms/request_appeal, or mail your appeal to the Office of FOIA Services of the Securities and Exchange Commission located at Station Place, 100 F Street NE, Mail Stop 2465, Washington, D.C. 20549, or deliver it to Room 1120 at that address. Also, send a copy to the SEC Office of the General Counsel, Mail Stop 9612, or deliver it to Room 1120 at the Station Place address.

You also have the right to seek assistance from me as a FOIA Public Liaison or contact the Office of Government Information Services (OGIS) for dispute resolution services. OGIS can be reached at 1-877-684-6448 or https://ogis.archives.gov/?p=/ogis/index.html.

If you have any questions, please contact Frank Mandic of my staff at mandicf@sec.gov. You may also contact me at foiapa@sec.gov or (202) 551-7900.

Sincerely,

Dave Henshall
FOIA Branch Chief

SEC
Incident Response
Capability Handbook

April 2014

Securities and Exchange Commission
Office of Information Technology
Security Operations

TABLE OF CONTENTS

Incident Response Capability Handbook

1. Introduction

1.1.Purpose

(b)(7)(E)

1.2. Scope

(b)(7)(E)

1.3. Authority

This section enumerates the Federal laws, regulatory guidance, and directives that drive the SEC information security programs that inform the formation of an Incident Response Plan.

- Federal Information Security Management Act (FISMA) of 2002
- Computer Fraud and Abuse Act of 1986, as amended.
- OMB Circular No. A 130, Appendix III "Security of Federal Automated Information Systems"
- Federal Information Processing Standard - 199 "Standards for Security Categorization of Federal Information and Information Systems" February 2004.
- NIST SP 800-53 Rev. 4 – Recommended Security Controls for Federal Information Systems, April 2013
- NIST SP 800-61 Rev. 2–Computer Security Incident Handling Guide, August 2012
- SEC Regulation (SECR) 24-04, "Information Technology Security Program"
- SEC OD 24-04.07- Information Security Incident Management, April 2006
- SEC OD- 24-04.02.01 – Sensitive Data Protection, May 2006

2. Procedures for Responding to Incidents

2.1. Background

(b)(7)(E)

(b)(7)(E)

2.2. Events and Incidents

(b)(7)(E)

2.3. Definitions

Definitions are located on the SEC Office of Information Technology's (OIT's) web site under "IT Definitions and Glossary."

2.4. Reportable Incident Criteria for the SEC

(b)(7)(E)

2.5. CSIRC Incident Identification

(b)(7)(E)

(b)(7)(E)

3. Incident Response Processes

3.1. Preparation Stage

(b)(7)(E)

3.2. Detection and Analysis Stage

(b)(7)(E)

Page 06 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

(b)(7)(E)

3.3. Containment, Eradication and Recovery Stage

(b)(7)(E)

3.4. Handling Digital Evidence (Forensics Examination)

(b)(7)(E)

3.5. Data Analysis

(b)(7)(E)

3.6. Recovery

(b)(7)(E)

4. Post-Incident Activity Stage

(b)(7)(E)

(b)(7)(E)

5. Roles and Responsibilities

(b)(7)(E)

Page 10 of 44

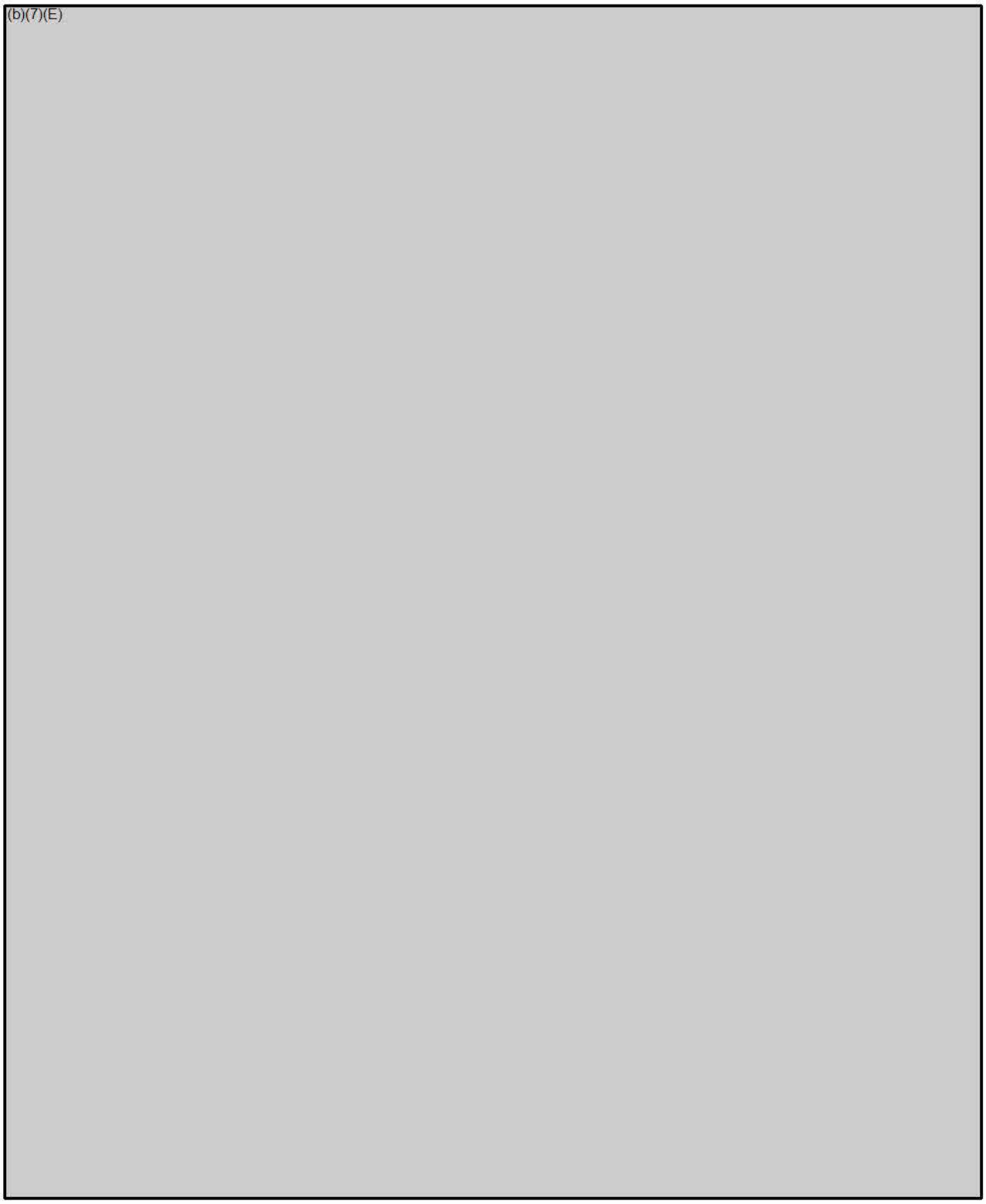
Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Appendix A-Root Cause Analysis

(b)(7)(E)



Page 12 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Appendix B-Standards and Guidelines

(b)(7)(E)

Page 14 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 15 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 17 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 18 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 19 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 20 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 21 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 22 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 23 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 24 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 25 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 26 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 27 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 28 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 29 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 30 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 31 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 32 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 33 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 34 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 35 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 37 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

2. Chain of Custody Form

SECURITIES AND EXCHANGE COMMISSSION INFORMATION SECURITY & PRIVACY PROPERTY AND CHAIN OF CUSTODY DOCUMENT		Case Number	
Name and Title From Whom Received		Address and Telephone Number	
Location Where Obtained		Reason Obtained	Date/Time Obtained
Item #	Quantity	Description of Articles	
		Chain of Custody	
Issue	Date	Released By	Received By	Reason
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	

Location ____________________			Property Number ____________________	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	
		Signature	Signature	
		Name/Title	Name/Title	

FINAL RELEASE AUTHORITY

Items(s) ____________________ on this document pertaining to the investigation involving ____________________ ____________________ is/are no longer required as evidence and may be disposed of as indicated below.

(Printed Name/Title) (Signature) (Date)

Released to Owner or Other (Name/Address) ____________________

Destroyed by (describe) ____________________

Other (Explain) ____________________

Page 40 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 41 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 42 of 44

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Appendix D-Security Service Contacts

(b)(7)(E)