Description of document:	Surface Transportation Board (STB) Disaster Recovery Plan 2019
Requested date:	2020
Release date:	29-October-2020
Posted date:	22-August-2022
Source of document:	FOIA/Privacy Officer Surface Transportation Board 395 E Street, S.W. Washington, D.C. 20423-0001 Fax: (202) 245-0456 Email: FOIA.Privacy@stb.gov FOIAonline

From: FOIA Privacy <foia.privacy@stb.gov>
Cc: Keats, Craig <Craig.Keats@stb.gov>; Toson, Marquis <Marquis.Toson@stb.gov>
Sent: Thu, Oct 29, 2020 4:12 pm
Subject: STB FOIA Request No. 20-029 (Partial Grant)

We are granting your FOIA request seeking the Surface Transportation Board's Disaster Recovery Plan developed in 2019, subject to certain redactions. After searching our records, we have located one record responsive to your request. We are redacting information that could be used to facilitate a cyberattack against the Board's IT platforms under FOIA Exemption 7(e), as attached.

Exemption 7(e)

The Board is an agency that administers the Interstate Commerce Act. In carrying out that function, the Board interprets the law, investigates violations, and enforces the statute. Under FOIA Exemption 7(e), courts have upheld the actions of agencies with similar responsibilities in withholding information and records that contain details of those agencies' information technologies. Prechtel v. FCC, 330 F. Supp. 3d 320, 335 (D.D.C. 2018) (protecting agency's electronic server logs because disclosure "would reveal sensitive information regarding [its] IT architecture, including security measures [it] takes to protect its systems from malicious activity," thereby providing a "roadmap" to circumvent agency's defensive efforts); Poitras v. DHS, 303 F. Supp. 3d 136, 159 (D.D.C. 2018) (withholding "'protected internal e-mail addresses, non-public intranet web addresses, and a secure internal e-mail tool'" because disclosure would increase risk of unauthorized access to agency's IT system (quoting agency declaration)); Levinthal v. FEC, 219 F. Supp. 3d 1, 8-9 (D.D.C. 2016) (protecting study that assessed vulnerabilities in information technology system to protect against possible security risks and unlawful access to agency system). The Board finds itself in similar circumstances to the agencies in the above-cited cases, based on its review of the responsive record.

The Board's Chief Security Officer (CSO) has determined that release of the redacted information in the Board's Disaster Recovery Plan would create clear security risks to the Board's information technology system. The redacted materials contain sensitive information that would disrupt the Board's investigative and enforcement functions by giving an adversary insight to the Board's information system tactics, technologies and protocols, increasing the risks of cyber-attacks and allowing them to be more informed and directed. Therefore, the Board is redacting information from its Disaster Recovery Plan that would increase the risk of cyber-attacks, while still providing what it can in recognition that the public has an interest in seeing that the Board has a disaster recovery plan.

Appeal Rights

You may appeal to the Chairman of the Surface Transportation Board within 90 days of receiving this determination to withhold certain information in the responsive record under Exemption 7(e). 5 U.S.C. § 552(b)(7)(e). Any appeal should be addressed to

Chairman Ann Begeman, 395 E Street, S.W., Washington DC 20423 and may be faxed ((202)245-0452) or emailed to Chairman.Staff@stb.gov.

Alternative Dispute Resolution

You may also seek dispute resolution services from the STB FOIA Public Liaison or the Office of Government Information Services (OGIS). OGIS offers mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. The Board encourages the use of OGIS's mediation services if you feel it would be helpful. Of course, using OGIS services does not affect your appeal rights. You may contact OGIS in any of the following ways:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road - OGIS
College Park, MD 20740-6001
E-mail: ogis@nara.gov
Web: https://ogis.archives.gov
Telephone: 202-741-5770
Fax: 202-741-5769
Toll-free: 1-877-684-6448

We will bill you for FOIA fees, if applicable. Please feel free to contact me if you have any questions, referring to FOIA Request No. 20-029.

Sincerely,

Christopher Oehrle
FOIA/Privacy Officer
Office of the General Counsel
Surface Transportation Board
395 E Street, S.W.
Washington, D.C. 20423-0001
Phone: (202) 245-0271; Fax: (202) 245-0456
FOIA.Privacy@stb.gov

From: FOIA Privacy <ogis@nara.gov>
Sent: Tue, Nov 3, 2020 10:56 am
Subject: Follow up request -- STB FOIA Request No. 20-029 (Partial Grant)

In response to your follow-up request asking that we release certain redacted information on page 16 of the Board's Disaster Recovery Plan, we are providing you with the unredacted titles of the Administrative Issuance. We are not providing the issuances' identification numbers because publicizing the identification conventions of STB issuances could facilitate an unauthorized party's ability to generate a more accurate and realistic-looking fake STB document. Therefore, please accept the attached page as a replacement for the same page released to you on October 29, 2020.

Please feel free to reach out to me if you would like to discuss this redaction, referring to STB FOIA Request No. 20-029.

Sincerely,

Christopher Oehrle
FOIA/Privacy Officer
Office of the General Counsel
Surface Transportation Board
395 E Street, S.W.
Washington, D.C. 20423-0001
Phone: (202) 245-0271; Fax: (202) 245-0456
FOIA.Privacy@stb.gov

Surface Transportation Board
Disaster Recovery Plan

Issuance No. 9-216
Effective Date: May 17, 2019
Version 1.0

Revision History

Version Number	Date	Description	Primary Author(s)
0.9	4/26/2019	First Draft	Office of Managing Director
1.0	5/17/2019	Final	Office of Managing Director

The Surface Transportation Board (STB) Disaster Recovery Plan is reviewed, at minimum, on an annual basis. Revisions are made as necessary and after testing exercises, to ensure a viable plan for recovering systems and information that must relocate to an alternate work site.

Approved by: RACHEL CAMPBELL Digitally signed by RACHEL CAMPBELL Date: 2019.05.17 13:35:52 -04'00'

Managing Director _____ Date _____

TABLE OF CONTENTS

1 PURPOSE

This Disaster Recovery Plan (DRP) defines the requirement for baseline disaster recovery to be developed and implemented by the Surface Board Transportation (STB). The purpose of a DRP is to provide procedures to relocate information and systems operations to an alternate or devolution site.

The STB has determined the alternate site for information and systems operations is [redacted]

The major goals of this DRP are to:
1. Limit loss of information
2. Minimize impact of mission essential functions

Constraints:

- The STB has determined the alternate work site for personnel is [redacted]
- [redacted]

2 AUTHORITIES

A. See a full list of Authorities in Appendix H.

3 DISSEMINATION

All information technology personnel, system owners, network/server administrators, and Uniform Rail Costing System (URCS) systems administrator and URCS system owner.

Name	Position	Email
[redacted]	[redacted]	[redacted]

4 SCOPE

This plan applies to mission critical applications in the event of a disaster that requires physical relocation of critical applications. Although not included in the table below, all infrastructure required to run the below is included within the scope (i.e., network infrastructure).

Application Name	Critical (Y/N)	Fixed Asset (Y/N)	Manufacturer
[redacted]	[redacted]	[redacted]	[redacted]

5 RELOCATION STRATEGY

5.1 UNIFORM RAIL COSTING SYSTEM

The Uniform Rail Costing System (URCS) Phase III and Productivity can physically relocate to [redacted]

5.2 CASE MANAGEMENT SYSTEM (CASE)

The Case Management System (CASE) is currently [redacted]

5.3 ALL OTHER INFORMATION TECHNOLOGY INFRASTRUCTURE EQUIPMENT

The STB has a [redacted]

5.4 TELECOMMUNICATIONS SYSTEMS

The STB's telecommunications systems will [redacted]

5.5 BACKUP OPERATIONS PROCEDURES

[redacted]

6 DISASTER PLAN INITIATION

6.1 DISASTER ACTION CHECKLIST

1. Assess degree of disruption on critical infrastructure and systems
2. Identify [redacted]
3. Notify [redacted]
4. Implement recovery [redacted]
5. Notify [redacted]
6. Notify users of the disruption and estimated time for restoration

6.2 RECOVERY ACTIONS PROCEDURES

[redacted]

[redacted]

7 TESTING THE DISASTER RECOVERY PLAN

The STB should conduct periodic testing of the disaster recovery plan. [redacted]

Conduct Recovery Test

1. Select purpose of test and what is being evaluated

[redacted]

Areas to Test

1. Recovery of individual application systems using tape back-up, both stored on-site and off-site

[redacted]

8 ROLES AND RESPONSIBILITIES

8.1 CHIEF INFORMATION OFFICER

The Chief Information Officer (CIO) and IT personnel have full responsibility for performing disaster recovery efforts for [redacted]

[redacted]

8.2 URCS SYSTEM OWNER AND SYSTEMS ADMINISTRATOR

URCS is a suite of applications that hosts the [redacted].

URCS is [redacted]

[redacted]

8.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) has responsibility for ensuring all security controls are maintained [redacted]

8.4 Facilities Manager

The Facilities Manager has responsibility for ensuring an [redacted]

APPENDIX A: [redacted]

NOTE: [redacted]

Scenario 1: [redacted]

Scenario 2: [redacted]

Scenario 3 [redacted]

FUTURE STATE: [redacted]

Scenario 3: [redacted]

Scenario 4: [redacted]

Scenario 5: [redacted]

[redacted]

APPENDIX B: [redacted]

[redacted]

APPENDIX C: [redacted]

[redacted]

APPENDIX D: [redacted]

APPENDIX E: [redacted]

APPENDIX F: [redacted]

[redacted]

APPENDIX G: [redacted]

APPENDIX H:AUTHORITIES

- The National Security Act of 1947, dated July 26, 1947, as amended.
- Executive Order 12148, *Federal Emergency Management*, dated July 20, 1979, as amended.
- Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, dated July 6, 2012, as amended.
- Executive Order 12656, *Assignment of Emergency Preparedness Respons*ibilities, dated November 18, 1988, as amended.
- Executive Order 13286, *Establishing the Office of Homeland Security*, dated February 28, 2003.
- National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy*, dated May 9, 2007.
- National Communications System Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, dated November 7, 2011, as amended.
- National Continuity Policy Implementation Plan, dated August 2007.

REFERENCES:

- Presidential Decision Directive 62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, dated May 22, 1998.
- NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
- NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, dated November 2010, as amended.
- National Infrastructure Protection Plan, dated 2010, as amended.
- NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2013 Edition, as amended.
- FEMA Continuity of Operations Plan Template.
- Comprehensive Preparedness Guide 101, *Producing Emergency Plans*, – Interim, FEMA, dated November 2010, as amended.
- STB Administrative Issuance [redacted]
- STB Administrative Issuance [redacted]
- STB Issuance [redacted]

APPENDIX H:AUTHORITIES

- The National Security Act of 1947, dated July 26, 1947, as amended.
- Executive Order 12148, *Federal Emergency Management*, dated July 20, 1979, as amended.
- Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, dated July 6, 2012, as amended.
- Executive Order 12656, *Assignment of Emergency Preparedness Respons*ibilities, dated November 18, 1988, as amended.
- Executive Order 13286, *Establishing the Office of Homeland Security*, dated February 28, 2003.
- National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy*, dated May 9, 2007.
- National Communications System Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, dated November 7, 2011, as amended.
- National Continuity Policy Implementation Plan, dated August 2007.

REFERENCES:

- Presidential Decision Directive 62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, dated May 22, 1998.
- NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
- NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, dated November 2010, as amended.
- National Infrastructure Protection Plan, dated 2010, as amended.
- NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2013 Edition, as amended.
- FEMA Continuity of Operations Plan Template.
- Comprehensive Preparedness Guide 101, *Producing Emergency Plans*, – Interim, FEMA, dated November 2010, as amended.
- STB Administrative Issuance [redacted], Contingency Planning Policy, March 2018.
- STB Administrative Issuance [redacted], Disaster Recovery Manual, January 2013.
- STB Issuance [redacted], Risk Assessment Policy, March 2018.