AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2022
VOL. 8 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 2** **February-March 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [2] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

TSA Imposes New Cybersecurity Requirements for Rail and Air Sectors

By Ashden Fein, Moriah Daugherty and John Webster Leslie*

The Transportation Security Administration recently issued two security directives, which impose significant requirements on owners and operators of "higher-risk freight railroads, passenger rail, and rail transit." The agency also extended certain requirements of the security directives to airport and airline operators. The authors of this article discuss the security directives.

The Transportation Security Administration ("TSA") recently announced[1] the issuance of Security Directive 1580-21-01,[2] Enhancing Rail Cybersecurity, and Security Directive 1582-21-01,[3] Enhancing Public Transportation and Passenger Railroad Cybersecurity (together, the "Security Directives"), and "additional guidance for voluntary measures to strengthen cybersecurity across the transportation sector in response to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure." TSA's announcement clarifies that these actions are "among several steps DHS is taking to increase the cybersecurity of U.S. critical infrastructure."

The Security Directives, which became effective on December 31, 2021, impose significant requirements on owners and operators of "higher-risk freight railroads, passenger rail, and rail transit." TSA's announcement also explained that it has extended certain requirements of the Security Directives to airport and airline operators and has recommended that "all other lower-risk surface transportation owners and operators voluntarily implement" the requirements of the Security Directives.

FREIGHT AND PASSENGER RAIL

Specifically, the Security Directives require freight rail carriers identified in 49 C.F.R. § 1580.101 and owners and operators of a passenger railroad carrier or rail transit system identified in 49 C.F.R. § 1582.101 to undertake, among other things, "four critical actions":

---

* Ashden Fein (afein@cov.com) is a partner at Covington & Burling LLP advising clients on cybersecurity and national security matters, including crisis management and incident response, risk management and governance, government and internal investigations, and regulatory compliance. Moriah Daugherty (mdaugherty@cov.com) is an associate at the firm advising clients on a range of cybersecurity, data privacy, and national security matters. John Webster Leslie (jleslie@cov.com) is an associate at the firm representing and advising companies on an array of technology issues, including on cybersecurity, national security, investigations, and data privacy matters.

[1] https://www.dhs.gov/news/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation-owners-and.

[2] https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf.

[3] https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf.

1. Designate a cybersecurity coordinator "at the corporate level" who is "available to" TSA and the Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") "at all times" and provide the name, title, phone number, and email address of the cybersecurity coordinator and at least one alternate cybersecurity coordinator by email to TSA within seven days of the effective date of the Security Directives, upon commencement of new operations, or in the event of changes to this information;

2. Report a cybersecurity incident – which is defined to include "an event that is under investigation or evaluation . . . as a possible cybersecurity incident" – to CISA within 24 hours;

3. Develop and implement a cybersecurity incident response plan within 180 days from the effective date of the Security Directives (unless otherwise directed) to reduce the risk of an operational disruption to information technology and operational technology systems, and certify to TSA that it has met these requirements within seven days of completion; and

4. Complete a cybersecurity vulnerability assessment – which will include an assessment of current practices and activities to address cyber risks to information technology and operational technology systems, identification of gaps in current cybersecurity measures, and identification of remediation measures to address any identified vulnerabilities and gaps and develop a plan to implement these measures – and submit that assessment and remediation plan to TSA within 90 days of the effective date of the Security Directives.

The Security Directives also require owners and operators to comply with a range of additional requirements and procedures including, for example, confirming receipt of the Security Directives and notifying TSA if unable to implement any of the measures in the Security Directives within the required timeframes.

AVIATION

While the Security Directives are targeted at certain freight railroads, passenger rail, and rail transit, TSA's announcement also explained that the agency "recently updated its aviation security programs to require that airport and airline operators implement the first two provisions above"; that is, these operators must designate a cybersecurity coordinator and report cybersecurity incidents to CISA within 24 hours. TSA also announced its intention to "expand the requirements for the aviation sector and issue guidance to smaller operators."

INFORMATION SHARING

The Security Directives make clear that information produced under the requirements of these directives will be shared amongst the U.S. government. Specifically, the Security Directives clarify that any information provided to CISA under the Security Directives

"will" be shared with TSA, any information provided to TSA "will" be shared with CISA, and such information "may" be shared with the National Response Center and "other agencies as appropriate."

LOOKING FORWARD

These latest regulatory actions by TSA follows the issuance of two previous[4] TSA cybersecurity directives issued in May and July 2021, which targeted TSA-designated critical pipelines. These actions are also in line with DHS Secretary Alejandro Mayorkas' recent public remarks,[5] which previewed the issuance of the Security Directives and also announced a forthcoming rulemaking process to develop a "longer-term regime to strengthen cybersecurity and resilience in the transportation sector." These efforts are consistent with the U.S. government's ongoing focus on strengthening critical infrastructure cybersecurity.

More broadly, the White House has made U.S. cybersecurity a key issue over the past year, including by issuing[6] an Executive Order on Improving the Nation's Cybersecurity seeking to strengthen the federal government's ability to respond to and prevent cybersecurity threats and engaging with private sector leaders[7] to bolster the nation's cybersecurity. Accordingly, companies in all sectors – both in and out of the critical infrastructure space – should expect further developments in coming months.

---

[4] https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators; https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators.

[5] https://www.dhs.gov/news/2021/10/06/secretary-mayorkas-delivers-remarks-12th-annual-billington-cybersecurity-summit.

[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[7] https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.