Skadden

Privacy & Cybersecurity Update

TSA Implements New Cybersecurity Requirements for Critical Infrastructure

Two new federal regulations aimed at rail and air transportation highlight the continued focus of the federal government on strengthening critical infrastructure cybersecurity.

Background

On December 2, 2021, the Department of Homeland Security's Transportation Security Administration (TSA) announced two new security directives[1] and additional voluntary measures to bolster cybersecurity in the transportation sector. The security directives, which take effect on December 31, 2021, impose new requirements on higher-risk rail and air transit carriers, owners and operators. These directives follow an emergency security directive issued by TSA in May 2021 after a ransomware attack forced Colonial Pipeline, the largest fuel pipeline in the U.S., to shut down operations for several days, along with a follow-up security directive issued on July 26, 2021.

Overview of the December Security Directives

The directives require freight rail carriers[2] and the owners and operators of passenger railroad carrier or rail transit systems[3] to undertake four main actions:

1. **Designate a cybersecurity coordinator** to be available to liaise with TSA and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). The name, title, phone number and email address of the cybersecurity coordinator, along with that of at least one alternate cybersecurity coordinator, must be provided by email to TSA within seven days of the effective date of the security directives, when new operations commence or if there are changes to any of the provided information. The cybersecurity coordinator, who must be a U.S. citizen eligible for a security clearance, will serve as the main point-of-contact with TSA and CISA for cybersecurity-related matters.

[1] Security Directive 1580-21-01, Enhancing Rail Cybersecurity and Security Directive 1582-21-01, Enhancing Public Transportation and Passenger Railroad Cybersecurity

[2] Described in 49 C.F.R. § 1580.101

[3] Described in 49 C.F.R. § 1582.101

2. **Report cybersecurity incidents to CISA within 24 hours**. Such incidents include unauthorized access of an information technology or operation system and discovery of malware, as well as potential cybersecurity incidents and those still under investigation.
3. **Develop and implement a cybersecurity incident response plan** within 180 days from the effective date of the security directives unless otherwise directed. Owners and operators must conduct annual situational exercises to test the effectiveness of procedures outlined in the cybersecurity incident response plan. A statement of certification of the completion of development and implementation of such a plan must be submitted to TSA within seven days of completion.
4. **Complete a cybersecurity vulnerability assessment**. The assessment, which should document current practices that address risks to information technology and operational technology systems, should also identify gaps in current cybersecurity measures, as well as remediation measures. Such assessment and remediation plans must be provided to TSA within 90 days of the effective date of the security directives.

Information provided may be shared with other government agencies. Owners and operators must confirm receipt of the security directives via email and notify TSA if they cannot meet the required timeframes. Additionally, the first two requirements above have been extended to apply to airport and airline operators. Thus, airport and airline operators must designate a cybersecurity coordinator and report cybersecurity incidents to CISA within 24 hours.

Key Takeaways

These security directives are consistent with the Department of Homeland Security's efforts to strengthen cybersecurity within the transportation sector. Given that an estimated 85% of critical U.S. infrastructure and resources are privatized, the federal government continues to engage with private sector leaders to best respond to and prevent cybersecurity threats targeting critical infrastructure. Companies within the critical infrastructure industry and beyond should carefully review the new security directives, determine next steps to become compliant with the requirements if applicable and be aware that additional developments are likely.

Return to Table of Contents

OMB Issues Revised Guidance to Federal Agencies on Major Incident Cybersecurity Reporting Procedures

The White House Office of Management and Budget (OMB) provided further revised guidance to federal agencies on cybersecurity practices relating to Federal Information Security Modernization Act of 2014 (FISMA) oversight and metrics collection, including one-hour reporting obligations for "major incidents."

The OMB issued Memorandum M-22-05 on December 6, 2021, to provide guidance on Federal Information Security and Privacy Management Requirements (the cybersecurity guidance) for compliance with FISMA.[4] Specifically, the cybersecurity guidance sets forth a framework for determining that a "major" cyberattack or breach has occurred, and establishes a one-hour reporting obligation that is triggered by such determination.

Although the cybersecurity guidance is directed to public sector federal agencies, it may have implications for private sector companies as well. In addition to serving as a source of potential best practices with respect to cybersecurity, the definitions for various triggering incidents (including "major incidents") used by OMB may be applied, in whole or in part, in various proposed pieces of legislation relating to cybersecurity, data privacy and reporting requirements placed on private sector companies.

Baseline Reporting Obligation for Cybersecurity Incidents

As a threshold matter, the cybersecurity guidance notes that agencies are currently required to report cybersecurity incidents to CISA pursuant to the CISA Federal Incident Notification Requirements.[5] This includes an obligation to report any events under investigation for over 72 hours without successful determination of the event's root cause or nature (*i.e.*, malicious, suspicious or benign). CISA then provides summary and detailed monthly reporting to OMB regarding such incidents. According to the cybersecurity guidance, OMB and CISA are coordinating to develop strategies and technical standards to modernize and streamline the accuracy and efficiency of reporting from agencies to CISA, and from CISA to OMB. Such strategies include a plan for OMB to have real-time access to incident information by December 2022.

[4] The cybersecurity guidance (M-22-05) can be accessed here. The guidance replaces and rescinds earlier related guidance issued by OMB on November 9, 2020, (Memorandum M-21-02) and May 19, 2017, (Memorandum M-17-25).

[5] The CISA Federal Incident Notification Requirements can be accessed here.

Two-Prong Test for 'Major Incidents' and the One-Hour Reporting Requirement

As set out in the cybersecurity guidance, a heightened reporting framework applies to agencies when a "major incident" occurs, including requiring quicker reporting to OMB and notification to Congress. As required by FISMA, OMB established a definition of "major incident" in the cybersecurity guidance, which utilizes a two-pronged test based on whether or not an incident or breach involves personally identifiable information (PII), pursuant to which an incident constitutes a "major incident" if:

> (1) The incident is likely to result in demonstrable harm to the national security interests, foreign relations or the economy of the United States, or to the public confidence, civil liberties or public health and safety of the American people (including Level 3 to Level 5 incidents, according to the CISA Cyber Incident Scoring System); or
>
> (2) The incident is a breach that involves PII that, if exfiltrated, modified, deleted or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations or the economy of the United States, or to the public confidence, civil liberties or public health and safety of the American people."

OMB notes that agencies can consult with both OMB and CISA in making the determination of whether a particular incident rises to the level of a "major incident" under the test. Additionally, if a "cyber incident" under the Presidential Policy Directive-41 United States Cyber Incident Coordination protocol[6] also qualifies as a "major incident," certain coordination mechanisms and requirements come into effect.

When an incident is determined to be a "major incident," several reporting obligations are triggered under the cybersecurity guidance. First, within one hour of determining that a "major incident" has occurred, or of determining that a previously-reported incident qualifies as a "major incident," an agency must report that determination to both OMB and CISA. Second, within seven days of such determination, an agency also must notify certain congressional committees. Specifically, FISMA requires notification to:

- any appropriate authorization and appropriations committees;
- the House of Representatives committees on:
  - Oversight and Government Reform;
  - Homeland Security; and
  - Science, Space, and Technology; and
- the Senate committees on:
  - Homeland Security and Governmental Affairs; and
  - Commerce, Science, and Transportation.
- the Senate committees on: (a) Homeland Security and Governmental Affairs and (b) Commerce, Science, and Transportation.

In addition to the initial report to Congress, the cybersecurity guidance requires supplemental updates and reporting to Congress as further information is gathered regarding the scope of the threat, actors involved, remediation actions, known and potential harm, and plans for notification of affected individuals.

Key Takeaways

Federal agencies must diligently monitor for and assess any cybersecurity incidents to determine whether a particular incident rises to the level of a "major incident" under the cybersecurity guidance. If so, strict and immediate reporting obligations apply, particularly the duty to notify OMB and CISA within one hour after the determination. Private sector companies should watch for developments in the definition of "major incident" and related cybersecurity trigger events, as they may become subject to similar reporting obligations as the regulatory and legislative landscape evolves.

Return to Table of Contents

UK and US Governments To Develop Cross-Border Data Sharing Partnership

On December 8, 2021, U.K. Secretary of State for Digital, Culture, Media and Sport (DCMS) Nadine Dorries and U.S. Secretary of Commerce Gina M. Raimondo issued a joint statement on the development of a cross-border data sharing partnership, which would ultimately facilitate the transfer of personal data between the U.K. and U.S. This represents the next step in the two countries' shared commitment to promoting the "trustworthy use and exchange of data across borders" in order to achieve "a more peaceful and prosperous future," and will be welcome news to many organizations with trans-Atlantic operations.

Background

On July 16, 2020, the Court of Justice of the European Union (CJEU) ruled in *Irish Data Protection Commissioner vs Facebook and Maximillian Schrems (Schrems II)*, invalidating the EU-U.S. Privacy Shield, a mechanism relied on by many companies for the free and lawful transfer of EEA/U.K. personal

[6] The Presidential Policy Directive-41 can be accessed here.

data to the U.S. In its decision, the CJEU criticised the surveillance programs of the U.S. intelligence authorities for lacking legal protection for EEA/U.K. data subjects, and found the safeguarding mechanisms established in the EU-U.S. Privacy Shield to be insufficient. Following the *Schrems II* decision, transfers of personal data from the EEA/U.K. to the U.S. must instead be based on an alternative valid data transfer mechanism, such as standard contractual clauses (SCCs) or binding corporate rules, in order to be lawful. The CJEU also made clear that if SCCs were to be relied upon, additional contractual or technical measures to protect personal data would have to be implemented (*e.g.*, pseudonymisation or encryption). Though welcomed by many EEA/U.K. data subjects, this decision has placed significant limitations on companies undertaking frequent transfers of personal data to the U.S.[7]

Following the U.K.'s withdrawal from the EU (Brexit), the U.K. established its own independent data protection framework by transposing the EU General Data Protection Regulation 2016/679 (GDPR) into domestic law (U.K. GDPR), which is supplemented by the U.K. Data Protection Act 2018. The U.K. GDPR broadly mirrors the GDPR with regard to restricted transfers from the U.K. to third countries, such that transfers of personal data from the U.K. to third countries (*e.g.*, the U.S.) must be effected on the basis of a valid data transfer mechanism. However, as the U.K. has not yet recognized the new set of SCCs adopted by the European Commission on June 7, 2021, the old set of SCCs must currently be used for transfers of personal data out of the U.K. In practice, this has resulted in many organizations having to enter into both the new set of SCCs (for transfers out of the EEA) and the old set of SCCs (for transfers out of the U.K.). The U.K. Information Commissioner's Office also is in the process of developing its own U.K.-specific international data transfer agreement, meaning that organizations will yet again have to refile once published.[8]

On September 10, 2021, the DCMS announced that the U.K. government had launched a public consultation on proposed reform of the U.K. GDPR. In the consultation, the U.K. government — among other matters — made clear of its intention to issue its own adequacy regulations to facilitate the free transfer of personal data between the U.K. and its key trading partners, such as the U.S. This would allow transfers of personal data from the U.K. to the U.S. to take place without the need for a data transfer mechanism.[9]

Key Takeaways

The issue of cross-border data transfers has been an ongoing source of contention following *Schrems II* and Brexit, with many organizations currently dedicating significant attention and resources to ensuring that their transfers are legitimate. The joint statement[10] represents a significant step in the development of an adequacy framework between the U.K. and the U.S., which will be welcome news to many organizations that have trans-Atlantic operations and regularly transfer personal data from the U.K. to the U.S. The establishment of an U.K.-U.S. adequacy framework will remove the time and cost burden on U.K. data exporters of having to enter into a valid data transfer mechanism with U.S. data importers each time a transfer of personal data is contemplated.

It is currently unclear what the adequacy framework will look like (and what protections will be afforded to U.K. data subjects thereunder), as the U.K. and U.S. governments will continue their negotiations in early 2022. However, it is important to note that a substantial departure from the GDPR and European standards of data protection could have a significant impact on the U.K.'s ability to freely transfer data within the EEA, as the European Commission regularly reviews its adequacy decisions and, if it sees fit, can revoke them at any time.

Return to Table of Contents

[7] Read more about the *Schrems II* decision in our July 2020 *Privacy & Cybersecurity Update*, available here.

[8] Read more about the adoption of new SCCs by the European Commission in our June 2021 *Privacy & Cybersecurity Update*, available here.

[9] Read more about the consultation in our September 2021 *Privacy and Cybersecurity Update*, available here.

[10] The joint statement can be found on the U.K. government website here.

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000