King & Spalding

Client Alert

Special Matters and Government Investigations

APRIL 18, 2024

For more information, contact:

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Alexander Davey
+1 713 276 7376
adavey@kslaw.com

Christina Caitlin McLaughlin
+1 404 572 5217
cmclaughlin@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
Tel. +1 202 737 0500

Department of Homeland Security Proposes Rule for Reporting of Cyber Incidents

On April 4, 2024, the Cybersecurity and Infrastructure Security Agency ("CISA") published for public comment a long-awaited proposed rule to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").[1] CIRCIA was signed into law on March 15, 2022 and requires covered entities to report "significant" cyber incidents within 72 hours and ransomware payments within 24 hours. Under the new law, covered entities are also subject to supplemental reporting requirements and data preservation obligations.

CISA estimates that the rule will cost the public and private sector over $2.6 billion between now and 2033, and it anticipates receiving over 200,000 reports from over 316,000 entities during that time.[2] CISA also anticipates dedicating significant resources to implementation of the rule, having submitted a budget request for $116 million in additional funding to implement the new program, which will require "major technology enhancements" and an additional 122 full-time employees.[3]

COVERED ENTITIES

The proposed rule defines "covered entity" broadly to include: (1) any organization that falls within one of 16 "critical infrastructure sectors"—which cover a myriad of industries, from critical manufacturing to financial services[4] and (2) either exceeds U.S. Small Business Association size thresholds or, regardless of size, is covered by specifically enumerated criteria related to certain critical infrastructure sectors.[5]

The list of critical infrastructure sectors is broad, and simply being an "active participant" in that sector is enough.[6] For example, CISA notes that the Commercial Facilities Sector includes "a mix of entities, such as the nation's 1.1 million malls, shopping centers, and other retail establishments; over 52,000 hotel-based properties; nearly 1,400 casinos and associated resorts; 1 million office buildings; 5.6 million multi-family

rental buildings, and nearly 125,000 establishments designed for public assembly, such as stadiums, arenas, movie theaters, museums, zoos, libraries, and other performance venues".[7]

According to CISA, advertising firms, law firms, political parties, graphic design firms, think tanks, and public interest groups might not fall within the critical infrastructure sectors.[8]

An entity satisfies the size threshold if it exceeds the U.S. Small Business Administration's small business size standard based on either employees or annual revenue, depending on the industry.[9] For the applicable thresholds, see 13 C.F.R. pt. 121. In addition, there are specific sector-based criteria that bring certain small businesses within CIRCIA reporting requirements.[10]

SIGNIFICANT CYBER INCIDENTS

CIRCIA limits reporting obligations to "significant" cyber incidents only.[11] The proposed rule defines a significant cyber incident as any one of the following four situations:

1. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network.
2. A serious impact on the safety and resiliency of a covered entity's operational systems and processes.
3. A disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services.
4. Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider.[12]

Under these definitions, covered entities would need to consider whether a cyber incident is sufficiently serious or substantial to trigger reporting requirements. As discussed below, underreporting can subject an entity to a variety of penalties.

INFORMATION TO BE REPORTED

Reports must describe the cyber incident or ransomware attack, including details such as the function of the affected networks, the tactics used to perpetrate the incident, the suspected culprit, and any mitigation efforts taken in response to the incident.[13]

EXCEPTIONS TO REPORTING REQUIREMENTS

There are several exceptions to CIRCIA's reporting requirements.

- A covered entity does not need to report to CISA if it is already required to report substantially similar information on a substantially similar timeline to another federal agency—and that agency has an approved information-sharing agreement with CISA.[14]
- A covered entity need not submit two separate reports if it experiences a significant cyber incident accompanied by a ransom demand. In this situation, it may submit a combined report.[15]
- Reporting requirements don't apply to entities or certain functions of entities that are owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System (DNS).[16]

- Reporting requirements don't apply to federal agencies when they are already required to report an incident to CISA pursuant to the Federal Information Security Modernization Act of 2014 (FISMA).[17]

REPORTING TIMELINES

Reports on significant cyber incidents are due no later than 72 hours after the entity "reasonably believes" a covered incident has occurred, and reports on ransomware payments are due no later than 24 hours after the payment has been disbursed.[18]

This strict timeline means that entities will likely be required to report on incidents that are still under active investigation, while the entity's understanding of the incident is incomplete and evolving.

And CISA is clear that having incomplete information is not an excuse for a tardy report.[19] Rather, an entity that reasonably believes a covered incident has occurred must report it and subsequently must "promptly" file a supplemental report with any newly discovered information.[20]

DATA PRESERVATION REQUIREMENTS

In addition to the reporting requirements, the proposed rule also creates obligations to preserve data and records for at least two years, relating to an array of technical and incident information, including: threat actor communications, indicators of compromise, network traffic, attack vector, forensic reports, forensic images, logs, and other items.[21] In considering how best to prepare for these requirements, covered entities may wish to consider the structure of their specific networks and IT systems, as well as potential data storage needs.

LEGAL PROTECTIONS FOR REPORTED INFORMATION

The rule contains several protections for submitting reports and responding to requests for information (RFIs) from CISA. These include:

- Designation as commercial, financial, and proprietary information;
- Exemption from disclosure under the Freedom of Information Act;
- Protection against waiver of privilege or other protection provided by law;
- Ex parte communications waiver;
- Prohibition on use of reports or RFI responses in regulatory actions;
- Protection against future liability from submitting a report or responding to an RFI; and
- Limits on authorized uses[22] of the information by CISA.[23]

PENALTIES FOR FAILING TO REPORT

If CISA believes that an entity has failed to comply with CIRCIA, it can issue a request for information and/or a subpoena and is empowered to refer non-compliance to the Attorney General for civil enforcement.[24] Non-compliant entities may also face acquisition penalties, including suspension and debarment.[25]

COMMENT PERIOD

Entities who believe they may face compliance obligations under CIRCIA may wish to comment on the proposed rule. CISA will accept comments on the proposed rule for 60 days after its publication—until June 3, 2024.

The final rule likely will not become effective until early 2026.

[1] Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 Fed. Reg. 23644 (Apr. 4, 2024) (to be codified at 6 C.F.R. pt. 226).
[2] 89 Fed. Reg. at 23648.
[3] U.S. DEP'T OF HOMELAND SEC., FY 2025 BUDGET IN BRIEF 4, 61 (2024).
[4] The critical infrastructure sectors are named in Presidential Policy Directive 21. They are: (1) Chemical; (2) Commercial Facilities; (3) Communications; (4) Critical Manufacturing; (5) Dams; (6) Defense Industrial Base; (7) Emergency Services; (8) Energy; (9) Financial Services; (10) Food and Agriculture; (11) Government Facilities; (12) Healthcare and Public Health; (13) Information Technology; (14) Nuclear Reactors, Materials, and Waste; (15) Transportation Systems; (16) Water and Wastewater Systems. WHITE HOUSE, OFF. IF THE PRESIDENT, PRESIDENTIAL POLICY DIRECTIVE—CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Feb. 12, 2013).
[5] As one example, an entity that does not meet the size threshold but falls within a critical infrastructure sector is a covered entity if it: (i) knowingly provides or supports information technology hardware, software, systems, or services to the Federal government; (ii) has developed and continues to sell, license, or maintain any software that has certain enumerated attributes, such as direct or privileged access to networking or computing resources; (iii) is an original equipment manufacturer, vendor, or integrator of operational technology hardware or software components; or (iv) performs functions related to domain name operations. 6 C.F.R. § 226.2 (b)(12).
[6] *See* 89 Fed. Reg. at 23676 ("[A] wide variety of entities, including at least some entities that do not own or operate systems or assets that meet the definition of critical infrastructure in PPD-21 but are active participants in critical infrastructure sectors and communities, are considered 'in a critical infrastructure sector.'"), 23759 ("[T]here are a wide variety of types of entities that are active participants in critical infrastructure sectors and communities and are considered 'in a critical infrastructure sector.'").
[7] *Id.* at 23677.
[8] *Id.* at 23678.
[9] 6 C.F.R. § 226.2(a).
[10] *Id.* § 226.2(b)(1)–(16).
[11] The proposed rule defines a "cyber incident" as "an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or actually jeopardizes, without lawful authority, an information system." 6 C.F.R. § 226.1.
[12] *Id.*
[13] *Id.* §§ 226.8, 226.9.
[14] *Id.* § 226.4(a).
[15] *Id.* § 226.3(c).
[16] *Id.* § 226.4(b).
[17] *Id.* § 226.4(c).

[18] *Id.* § 226.5.
[19] *See* 89 Fed. Reg. at 23665 ("CISA is aware that in some cases, a covered entity will not know for certain the cause of the incident within the first few days following the occurrence of the incident. . . [A] covered entity does not need to know the cause of the incident with certainty for it to be a reportable substantial cyber incident…CISA believes its ability to achieve the regulatory purposes of CIRCIA would be greatly undermined if covered entities were allowed to delay reporting until an incident has been confirmed to have been perpetrated without lawful authority. Therefore, an incident whose cause is undetermined, but for which the covered entity has a reasonable belief that the incident may have been perpetrated without lawful authority, must be reported if the incident otherwise meets the reporting criteria.").
[20] 6 C.F.R. § 226.13.
[21] *Id.*
[22] Information provided to CISA in a CIRCIA report or in a response to an RFI may only be disclosed to, retained by, and used by the Federal government for certain enumerated purposes: (i) cybersecurity; (ii) identifying a cybersecurity threat; (iii) responding to or preventing or mitigating a specific threat of death or serious bodily or economic harm; (iv) responding to, investigating, prosecuting, preventing, or mitigating a serious threat to a minor; and (v) preventing, investigating, disrupting, or prosecuting certain offenses relating to events required to be reported to CISA, fraud and identity theft, espionage and censorship, or protection of trade secrets. *Id.* § 226.18(c)(3).
[23] *Id.* § 226.18.
[24] *Id.* §§ 226.15–17.
[25] *Id.* § 226.18.

Special Matters & Government Investigations Partners

Gary Adamson
New York
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
New York
+1 212 556 2376
abaker@kslaw.com

Matthew H. Baughman
Atlanta
+1 404 572 4751
mbaughman@kslaw.com

J.C. Boggs
Washington, DC
+1 202 626 2383
jboggs@kslaw.com

Amy B. Boring
Atlanta
+1 404 572 2829
aboring@kslaw.com

Christopher C. Burris
Atlanta
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
New York
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
Northern Virginia
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
Washington, DC
+1 202 661 7828
mciatti@kslaw.com

Daniel R. Coats
Washington, DC
+1 202 626 2642
dcoats@kslaw.com

Patrick M. Collins
Chicago
+1 312 764 6901
pcollins@kslaw.com

Alexander M. Crenshaw
Washington, DC
+1 202 626 8996
acrenshaw@kslaw.com

Sumon Dantiki
Washington, DC
+1 202 626 5591
sdantiki@kslaw.com

Ethan P. Davis
San Francisco
+1 415 318 1228
edavis@kslaw.com

Alan R. Dial
Washington, DC
+1 202 661 7977
adial@kslaw.com

Dan Donovan
Washington, DC
+1 202 626 7815
ddonovan@kslaw.com

Robert L. Ehrlich, Jr.
Washington, DC
+1 202 626 9710
rehrlich@kslaw.com

David Farber
Washington, DC
+1 202 626 2941
dfarber@kslaw.com

Zachary Fardon
Chicago
+1 312 764 6960
zfardon@kslaw.com

Ehren Halse
San Francisco
+1 415 318 1216
ehalse@kslaw.com

Zachary J. Harmon
Washington, DC
+1 202 626 5594
zharmon@kslaw.com

Ted Hester
Washington, DC
+1 202 626 2901
thester@kslaw.com

Max Hill, K.C.
London
+44 20 7551 2130
mhill@kslaw.com

Amy Schuller Hitchcock
Sacramento/San Francisco
+1 916 321 4819
ahitchcock@kslaw.com

John A. Horn
Atlanta
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
New York
+1 212 556 2278
ahruska@kslaw.com

Mark A. Jensen
Washington, DC
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
Washington, DC
+1 202 626 8984
djohnson@kslaw.com

William Johnson
New York
+1 212 556 2125
wjohnson@kslaw.com

Allison F. Kassir
Washington, DC
+1 202 626 5600
akassir@kslaw.com

M. Alexander (Alec) Koch
Washington, DC
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
New York
+1 212 556 2207
ykotlarsky@kslaw.com

Steve Kupka
Washington, DC
+1 202 626 5518
skupka@kslaw.com

Jade R. Lambert
Chicago
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
Los Angeles
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
Washington, DC
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
New York
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
Houston
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
Atlanta
+1 404 572 2447
alipson@kslaw.com

Daniel E. Lungren
Washington, DC
+1 202 626 9120
dlungren@kslaw.com

William S. McClintock
Washington, DC
+1 202 626 2922
wmcclintock@kslaw.com

Amelia Medina
Washington, DC
+1 202 626 5587
amedina@kslaw.com

Kendrick B. Meek
Washington, DC
+212 626 5613
kmeek@kslaw.com

Andrew Michaelson
New York
+212 790 5358
amichaelson@kslaw.com

Jim C. Miller III
Washington, DC
+1 202 626 5580
jmiller@kslaw.com

Patrick Montgomery
Washington, DC
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
Atlanta/Washington, DC
+1 404 572 4730
pbmurphy@kslaw.com

Grant W. Nichols
Austin/Washington, DC
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
Washington, DC
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
Chicago
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
Washington, DC
+1 202 626 3732
mpauze@kslaw.com

Michael A. Plotnick
Washington, DC
+1 202 626 3736
mplotnick@kslaw.com

Olivia Radin
New York
+1 212 556 2138
oradin@kslaw.com

John C. Richter
Washington, DC
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
Washington, DC
+1 202 626 9220
rrosenstein@kslaw.com

Daniel C. Sale
Washington, DC
+1 202 626 2900
dsale@kslaw.com

Greg Scott
Sacramento/San Francisco
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
Singapore
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
New York
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
San Francisco
+1 415 318 1221
mshepard@kslaw.com

Thomas Spulak
Miami
+1 305 462 6023
tspulak@kslaw.com

Aaron Stephens
London
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
Denver
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
Paris
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
Washington, DC
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
Northern Virginia
+1 703 245 1018
rvacura@kslaw.com

Richard Walker
Washington, DC
+1 202 626 2620
rwalker@kslaw.com

Anthony A. Williams
Washington, DC
+1 202 626 3730
awilliams@kslaw.com

David K. Willingham
Los Angeles
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
Washington, DC
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
Atlanta/Washington, DC
+1 404 572 2723
syates@kslaw.com