Hogan Lovells

Aerospace & Defense Insights

Critical input needed: U.S. critical infrastructure asked to engage on proposed cyber reporting rules

Stacy Hadeka, Paul Otto, Pete Marta, Mike Mason, Scott Loughlin, Allison Holt Ryan, Mike Scheimer, Jasmeet Ahuja, Dan Ongaro, and Alaa Salaheldin

Through Aerospace & Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

The Cybersecurity and Infrastructure Security Agency (CISA) has issued a Request for Information (RFI) and announced "public listening sessions" soliciting input in advance of formal rulemaking under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

CIRCIA was enacted in March 2022 amid growing concern around cybersecurity threats and incidents impacting U.S. critical infrastructure. Among other requirements, CIRCIA calls on CISA to establish a mandatory regime under which certain critical infrastructure entities in the A&D industry must report (1) certain cyber incidents to CISA within 72 hours of reasonable belief of occurrence and (2) a ransom payment within 24 hours of making payment. Entities that may fall within one of the critical infrastructure sectors are advised to consider providing input to CISA to define CIRCIA's scope of applicability and what criteria may make sense to adopt to appropriately narrow the scope of applicability and avoid confusion as to who may be covered.

CIRCIA delegates broad rulemaking authority to CISA, which is tasked with promulgating regulations to further define critical applicability and reporting requirements under the law. Under CIRCIA, CISA must publish a Notice of Proposed Rulemaking by March 2024 and final rules within 18 months of the proposed rules, or no later than September 2025. Entities that fall within a critical infrastructure sector—such as the Defense Industrial Base, Critical Manufacturing, Information Technology, and Transportation Systems Sectors—may wish to consider submitting comments now (whether through industry groups or otherwise) to help appropriately define the scope of applicability and corresponding reporting obligations. The RFI is open for comments through **November 14, 2022**. CISA also is holding a series of "public listening sessions" for stakeholders to provide feedback on the upcoming regulations, with ten such sessions occurring across the United States spanning September through November 2022.[1]

CISA is welcoming public comment on any topic related to the upcoming rulemaking, and also has identified a list of 32 non-exhaustive topics of interest to CISA including definitions and interpretations of terminology, estimates of likely number of reports to be expected, as well as reporting triggers and requirements under the law.

1. The DC listening session was scheduled for October 19, 2022. *See* 87 Fed. Reg. 60409 (Oct. 5, 2022).

Key topics open for comment include:

What is a covered entity?

One of the most significant definitions left to CISA rulemaking is the precise definition of a "covered entity" required to comply with CIRCIA's requirements. CIRCIA initially scopes the definition of a "covered entity" as an entity that falls within one of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (PPD-21), and as further defined by regulations promulgated by CISA. This includes the following sectors relevant to the A&D industry: Defense Industrial Base, Critical Manufacturing, Information Technology, and Transportation Systems.

There are open questions as to how broad the definition of a "covered entity" will be. For instance, should the definition be narrowed to cover only the most critical entities. Or, should CISA take a broad approach to include third-party service providers to critical infrastructure entities. For instance, the Department of Defense's (DoD) cyber incident reporting requirements apply not only to a prime contractor, but can also apply to their subcontractors. *See* 48 C.F.R. § 252.204-7012. Comments addressing these particular considerations will be important.

Moreover, when submitting comments, entities may wish to consider the three factors defined within CIRCIA to guide CISA's rulemaking on the scope of "covered entities" for reporting purposes: (1) the consequences that a disruption to or compromise to the entity could cause to national security, economic security, or public health and safety; (2) the likelihood that the entity may be targeted by a malicious cyber actor; and (3) the extent to which damage, disruption, or unauthorized access to the entity would likely enable the disruption of the reliable operation of critical infrastructure.

What is a reportable incident?

CIRCIA requires covered entities to report a "covered cyber incident" to CISA within 72 hours, and CISA is seeking further input on the definition of the terms used to define incidents. A "cyber incident" is currently defined under the law 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. But not all such incidents will be reportable, as under CIRCIA only "substantial cyber incidents" may constitute "covered cyber incidents" subject to reporting obligations—and CISA also seeks input on what constitutes a 'substantial' incident.

Entities may wish to comment on these incident definitions to help CISA better align the definition with existing cyber incident reporting requirements and industry practice around incident tracking and reporting. Notably, CISA's RFI specifically requests input on similarities and differences from other federal incident reporting triggers, which could include the current DoD 72 hour cyber incident reporting requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. Entities may also wish to highlight relevant state and international reporting thresholds as well.

Entities are well advised to think through how their existing incident response processes would define and rate incidents—to better understand what the CISA reporting requirements would mean for such processes and where changes may be required—as this may influence how entities provide insights to CISA in advance of these incident definitions being finalized.

Harmonization with existing regulations.

CISA further solicits feedback on how it can best harmonize reporting requirements under CIRCIA with reporting obligations under existing laws and regulations. Entities are encouraged to comment on the similarities, differences, and potential conflicts between CIRCIA's requirements and requirements under existing laws and regulations. Companies in the A&D industry sector can draw from the current DoD cyber incident reporting requirements and other agency-specific reporting requirements in providing feedback to CISA.

What should trigger reporting requirements?

CISA has requested detailed information regarding reporting requirements under CIRCIA, including when the 72-hour timeline for reporting cyber incidents and 24-hour timeline for reporting ransom payments should begin. CISA expressly requests comments on what should constitute a "reasonable

belief" that a covered cyber incident has occurred, such as to trigger the 72-hour reporting timeline; this is likely to be a key question for legal advisors supporting entities in meeting the final regulations.

Format, manner, and content of reports.

Entities are encouraged to comment on the format, manner, and content of required reports for covered cyber incidents and ransom payments. For instance, DoD's Cyber Crime Center (DC3) lays out specific categories of information that should be reported within 72 hours of discovery of cyber incidents (the initial "Incident Collection Form"), which includes the following, among others:[2]

- Date incident discovered
- Location(s) of compromise
- Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
- Description of technique or method used in cyber incident
- Incident outcome (successful compromise, failed attempt, unknown)
- Incident/Compromise narrative (Ex: Chronological explanation of event/incident, threat actor TTPs, indicators of compromise, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred)

Moreover, DoD directs contractors that do not have all the required information within 72 hours of discovery of a cyber incident to report whatever information is available at that time and submit a follow-on report when additional information becomes available.[3]

In addition to initial cyber incident reports made within the 72-hour timeline, CISA has requested comments on the process, format, manner, and content of supplemental reports. Notably, CISA has solicited feedback on what constitutes "substantial new or different information" such that a supplemental report would be required, as well as feedback on criteria by which a covered entity may determine that a "covered cyber incident at issue has concluded and has been fully mitigated and resolved."

What is a ransomware attack and a ransom payment?

In a first-of-its-kind reporting requirement, CIRCIA requires covered entities to report a ransom payment to CISA within 24 hours. A "ransom payment" is defined under CIRCIA as the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack. A "ransomware attack" is defined as an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment.

Entities may wish to comment on the definitions of "ransom payment" and "ransomware attack" to help guide the final reporting requirement.

Additional topics for comment.

In addition to the key areas for comment discussed above, CISA further solicits comments around how third-party entities should be permitted to make reports on behalf of covered entities and how a third party can meet responsibilities to advise an impacted covered entity of its ransom payment reporting obligations. CISA further solicits comments on policies, procedures, and requirements related to enforcement of CIRCIA requirements, requests for information, protection of reporting entities, and information preservation and retention requirements, as well as any other policies, procedures, or requirements that would benefit covered entities.

Although not expressly discussed in the RFI, one open issue that may increase litigation risk for covered entities is whether reports submitted to CISA will be made public.

2. *See* https://dibnet.dod.mil/portal/intranet/#reporting-2.
3. *See* DoD Frequently Asked Questions (FAQs) Regarding the Implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 DFARS Subpart 239.76 and PGI Subpart 239.76, Q44 at 38 (Nov. 23, 2021).

Conclusion

CISA is soliciting input over the course of Fall 2022, with written comments to the RFI due by November 14, 2022. A&D entities operating in critical infrastructure—such as the Defense Industrial Base, Critical Manufacturing, Information Technology, and Transportation Systems Sectors—may wish to monitor industry input by joining listening sessions, discuss potential implications with trusted advisors and industry groups, and consider providing comments to key issues facing them with the upcoming rulemaking now, before CISA begins to calcify its position on scope of applicability and reporting requirements under CIRCIA as part of its forthcoming rulemaking process.

Stacy Hadeka
Counsel | Washington, D.C.
T: +1 202 637 3678
E: stacy.hadeka@hoganlovells.com

Paul Otto
Partner | Washington, D.C.
T: +1 202 637 5887
E: paul.otto@hoganlovells.com

Peter Marta
Partner | New York
T: +1 212 918 3528
E: peter.marta@hoganlovells.com

Michael Mason
Partner | Washington, D.C.
T: +1 202 637 5499
E: mike.mason@hoganlovells.com

Scott Loughlin
Partner | Washington, D.C.
T: +1 202 637 5565
E: scott.loughlin@hoganlovells.com

Allison Holt Ryan
Partner | Washington, D.C.
T: +1 202 637 5872
E: allison.holt-ryan@hoganlovells.com

Michael Scheimer
Partner | Washington, D.C.
T: +1 202 637 6584
E: michael.scheimer@hoganlovells.com

Jasmeet Ahuja
Counsel | Philadelphia & New York
T: +1 267 675 4667 (Philadelphia)
T: +1 212 918 3667 (New York)
E: jasmeet.ahuja@hoganlovells.com

Dan Ongaro
Associate | Minneapolis
T: +1 202 637 5756
E: dan.ongaro@hoganlovells.com

Alaa Salaheldin
Associate | Washington, D.C.
T: +1 202 637 4856
E: alaa.salaheldin@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com