Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : 4dac6187 | Apr 26, 2024, 02:26 PM

This week, *Hacking Healthcare*™ provides a brief overview of the Cyber Incident Reporting For Critical Infrastructure Act of 2022 (CIRCIA) proposed draft. We provide some background on what CIRCIA is, breakdown some notable details from the new proposed draft, and then highlight some considerations for Health-ISAC members.

Welcome back to *Hacking Healthcare*™.

Health-ISAC Americas Hobby Exercise 2024

The Health-ISAC is once again ramping up preparations for our annual Americas Hobby Exercise! For new Health-ISAC members, the Hobby Exercise is an annual Healthcare and Public Health (HPH) event designed to engage the healthcare sector and strategic partners on significant security and resilience challenges. The overarching objective is to inform and provide opportunities for organizational continuous improvement while increasing healthcare sector resiliency.

The following link to last year's Hobby Exercise After Action Report provides a good overview of the kinds of interaction and value you can expect from this year's event:

https://h-isac.org/hobby-exercise-2023-after-action-report/

This year's exercise will be held on June 6 at Venable LLPs in Washington, D.C. Members are encouraged to register their interest in participation at the following link:

https://portal.h-isac.org/s/community-event?id=a1Y7V00000ZmFVwUAN

Health-ISAC Monthly Threat Brief

As a reminder, next Tuesday and Thursday, the Health-ISAC will be holding its monthly Threat Briefs. These hour-long presentations from the Health-ISAC staff and Health-ISAC partners briefs members on current and emerging technical, physical, legal, and regulatory threats to the HPH sector. This month's briefing will include a discussion the topic of CIRCIA. The Threat Brief is a service provided only to Health-ISAC members.

Cyber Incident Reporting for Critical Infrastructure (CIRCIA) Proposed Rule

CIRCIA has been among the more anticipated pieces of legislation in the United States since President Biden signed it into law back in March of 2022. While we are still a long way off from a final rule and implementation, the recently released 447-page[i] proposed rule is a draft that summarizes the Cybersecurity and Infrastructure Security Agency's (CISA) current approach for public comment.

Background: What is CIRCIA?

The Biden administration and the United States Congress have increasingly turned their attention to shoring up their country's cybersecurity and resiliency through various laws and executive orders over the past few years. With ransomware running rampant and major cyber attacks impacting critical infrastructure sectors, one such approach that was pursued was the implementation of mandatory cyber incident and ransomware payment reporting. This approach has increasingly gained traction globally, albeit with little standardization and harmonization, and the result was CIRCIA.

CIRCIA required that the Cybersecurity and Infrastructure Security Agency (CISA) "develop and implement regulations requiring covered entities to report to CISA covered cyber incidents and ransom payments.[ii] While Congress laid down some required inclusions and guardrails for what this incident reporting regime would look like, such as requiring covered entities to report covered incidents within 72 hours, the details of who would be covered, what incidents would be covered, and the nature and content of the reports was broadly left up to a CISA rulemaking process.

The complexity, scope, and potential for legal challenge all likely played a part in the decision to give CISA years to take in public and private sector feedback to finally deliver the report that was released in the Federal Register on April 4.[iii]

The Proposed Rule

At 447 pages, the CIRCIA proposed rule is a mammoth document. However, it should be noted only the last 40 or so pages are the actual rule text. The vast majority of the document provides background on CIRCIA and CISA's legal authority, the purpose of the regulation, the cyber incident reporting landscape, comments that were received during initial listening sessions, cost benefit analysis, and other related topics.

The ~40 pages of the rule itself provide CISA's current thinking on:

- Definitions
- Applicability
- Required reporting on covered cyber incidents and ransom payments
- Exceptions to required reporting on covered cyber incidents and ransom payments
- CIRCIA Report submission deadlines
- Required manner and form of CIRCIA Reports
- Required information for CIRCIA Reports
- Required information for Covered Cyber Incident Reports
- Required information for Ransom Payment Reports
- Required information for Joint Covered Cyber Incident and Ransom Payment Reports
- Required information for Supplemental Reports
- Third party reporting procedures and requirement

It also discusses enforcement and penalties for non-compliance.

Action & Analysis

Included with Health-ISAC Membership

Upcoming International Hearings/Meetings

- **EU**
    1. No relevant meetings at this time
- **US**
    1. No relevant meetings at this time
- **Rest of World**
    1. No relevant meetings at this time

[i] The page numbers used in this week's threat brief refer to the initial version of the CIRCIA NPRM posted on the Federal Register's "Public Inspection" page. The PDF version now available has been reformatted into a 133-page document.

[ii] https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf

[iii] https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

[iv] https://www.ecfr.gov/current/title-13/chapter-I/part-121

[v] https://www.venable.com/insights/publications/2024/04/circia-cyber-incident-reporting-for-practically

[vi] https://www.venable.com/professionals/g/harley-l-geiger

[vii] https://www.venable.com/insights/publications/2024/04/circia-cyber-incident-reporting-for-practically

[viii] https://www.venable.com/insights/publications/2024/04/circia-cyber-incident-reporting-for-practically

[ix] https://www.venable.com/insights/publications/2024/04/circia-cyber-incident-reporting-for-practically

[x] https://www.venable.com/insights/publications/2024/04/circia-cyber-incident-reporting-for-practically

[xi] https://www.regulations.gov/comment/CISA-2022-0010-0123

Report Source(s)

Health-ISAC

Reference | References

Health-ISAC
federalregister
regulations
Health-ISAC
CISA
venable
ecfr
venable

Tags

Incident Reporting, CIRCIA, Hobby Exercise, Hacking Healthcare, MTB, Ransomware

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org