Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : 935d4679 | Mar 29, 2024, 01:46 PM

This week, *Hacking Healthcare*™ is all about cyber incident reporting. We begin with a brief update on the state of the Cyber Incident Reporting for Critical Infrastructure (CIRCIA) proposed rule. Next, we take a longer look at an European Union (EU) & United States (US) effort meant to help address the proliferation of divergent cyber incident reporting regimes.

Welcome back to Hacking HealthcareTM.

Cyber Incident Reporting for Critical Infrastructure (CIRCIA) Proposed Rule Arrives!

After a long two-year wait, the CIRCIA proposed rulemaking has arrived.[i]

As a reminder of what this is, CIRCIA was passed by Congress and signed into law in March 2022. It requires the Cybersecurity and Infrastructure Security Agency (CISA) "to 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 Health-ISAC and Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group have been engaged on this issue since the process started, and you can find their initial comments on how CISA should approach the initial draft in the following public comments submitted in late 2022:

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

Now with the proposed rulemaking landing in the Federal Register, we finally get to see CISA's current thinking. We plan to examine all 447-pages of the CIRCIA draft to assess its impact on the healthcare sector in an upcoming issue of Hacking HealthcareTM, so stay tuned.

For those attending the upcoming Health-ISAC Spring Summit, we just added a roundtable discussion to the agenda on this subject so we hope to see you there.

US & EU Cyber Incident Reporting Initiative

Among the most significant issues with cyber incident reporting for the private sector is the number of unaligned reporting regimes that entities are subject to. This problem is so significant that within the US, a special government council was created just to try and help coordinate and harmonize federal cyber incident reporting requirements.[i] However, this issue extends beyond national borders. Entities that operate globally face the increasingly daunting prospect of trying to comply with potentially dozens of different cyber incident reporting regimes with varying requirements. In recognition of this issue, the US and EU have taken the first steps towards potentially ameliorating this burden.[ii]

DHS and DG Connect Initiative

On March 20, the European Commission's Directorate General for Communications, Networks, Content, and Technology (DG CONNECT) and the US Department of Homeland Security (DHS) jointly published a statement announcing an initiative to compare and try to align cyber incident reporting approaches.[iii], [iv] Officials from both organizations touted the effort as means to further collaborate on cybersecurity issues while also "[minimizing] the administrative burden on reporting entities."[v]

The first step in this effort was to publish a report alongside the announcement. The report, titled, Comparative Assessment of the DHS Harmonization of Cyber Incident Reporting to the Federal Government Report and the Rules on Incident Reporting in the EU Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS 2 Directive), may not roll off the tongue, but it does accurately describe what it is.[vi]

The 16-page report provides an easy-to-follow comparison of DHS's cyber incident reporting guidance with NIS 2 in terms of definitions, reporting thresholds, reporting triggers, timelines, reporting mechanisms, report contents, and more.

Next Steps

Iranga Kahangama, DHS Assistant Secretary for Cyber, Infrastructure, Risk and Resilience, has laid out where DHS and DG Connect may go from here.

“Over the next year our teams plan to continue our cooperation on a more technical level, including by mapping elements such as cybersecurity incident taxonomies, reporting templates, and the content of reports and formats. We will conduct an in-depth crosswalk of the DHS-developed Model Reporting Form against the NIS 2 required contents of reports to identify where there is overlap and disparities in the types of data being requested.”

Action & Analysis

Included with Health-ISAC Membership

Upcoming International Hearings/Meetings

EU

- No relevant meetings at this time

US

- No relevant meetings at this time

Rest of World

- No relevant meetings at this time

[i] https://public-inspection.federalregister.gov/2024-06526.pdf

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

[i] https://www.dhs.gov/news/2022/07/25/readout-inaugural-cyber-incident-reporting-council-meeting

[ii] https://digital-strategy.ec.europa.eu/en/news/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better-align

[iii] https://digital-strategy.ec.europa.eu/en/news/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better-align

[iv] https://www.dhs.gov/news/2024/03/20/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better

[v] https://www.dhs.gov/news/2024/03/20/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better

[vi] https://www.dhs.gov/sites/default/files/2024-03/24_0320_plcy_comp-assessment-dhs-cyber-incident-rpting-fed-gvt-and-rules-incident-rpting-eu-directive-measures-high-common-level-cybersecurity-across-union-nis-2-directive-508.pdf

Report Source(s)

Health-ISAC

Release Date

Mar 29, 2024, 11:59 PM

Tags

Cyber Incident Reporting for Critical Infrastructure, Incident Reporting, CIRCIA, Hacking Healthcare

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.

For Questions or Comments:

Please email us at toc@h-isac.org