December 7th, 2021

TLP White

This week, *Hacking Healthcare* begins by examining the personal accountability aspects of Australia's Critical Infrastructure Bill. Next, we break down the membership announcement of the Cybersecurity and Infrastructure Security Agency's (CISA) new Cybersecurity Advisory Board and try to tease out what to expect from its first meeting. Finally, we wrap up with a brief update on cyber incident reporting. Welcome back to *Hacking Healthcare*.

Author's Note: *It was great to meet many of you at the H-ISAC Summit in San Diego. My thanks to the awesome team at H-ISAC for putting together a great event. Thanks for your great feedback on what to do here at Hacking Healthcare, and I look forward to seeing you again at the next Summit.*

1. **Australia's Critical Infrastructure Bill Raises Questions of Leadership Accountability**
   Australia's hotly debated *Security Legislation Amendment (Critical Infrastructure) Bill 2021* finally passed both houses of Parliament last month and appears on its way to coming into force.[1] With the text now finalized and its future enforcement anticipated as likely coming before the end of the year, we would like to draw attention to its impact on personal accountability.

   It's worth briefly recapping the bill as this specific piece of legislation was first introduced over a year ago and has gone through several revisions as it worked its way through both chambers of Parliament. The bill amends *Security of Critical Infrastructure Act 2018* with an eye toward "[enhancing] the existing framework for managing risks relating to critical infrastructure by introducing additional positive security obligations for critical infrastructure assets."[2] This ultimately included "sector-specific requirements and mandatory cyber incident reporting; enhanced cyber security obligations for assets of national significance; [and] government assistance to relevant entities for critical infrastructure sector assets in response to significant cyber attacks."[3]

   The bill's most controversial aspect is considered by many to be the degree to which the federal government can intervene in how a private-sector organization responds to a cyber incident. It allows the federal government to give specific directions to an organization when a cyber incident rises to a sufficiently high level of severity, impacts

critical infrastructure or national security, and where no other existing regulatory system would allow for an effective response. Failure to comply with legally authorized directions under this bill may lead to a penalty of two years of imprisonment.[4] This approach is set to heighten the importance of cybersecurity within senior management, and it raises questions and concerns.

Action & Analysis

Included with H-ISAC Membership

2. **CISA Cybersecurity Advisory Committee Announces Diverse Set of Members**

CISA's new Cybersecurity Advisory Committee has announced its initial membership, and the eclectic group chosen may bode well for those hoping it will provide CISA with the kinds of outside perspectives that are often marginalized or absent from cybersecurity policy discussions. It remains an open question as to how these diverse voices will coalesce, but we believe this is a promising start.

The Cybersecurity Advisory Committee is a relatively new organization that was established in June of this year after its authorization in last year's National Defense Authorization Act. The Committee's charter describes its mission and function as making "recommendations on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency."[5] The Committee's membership plan further elaborates that the goal is to "provide independent, strategic, and actionable consensus recommendations to CISA" on a broad range of issues that may include risk management, information exchange, and public-private partnership.[6]

While industry and various critical infrastructure sectors are well represented on the committee, the membership also includes the hacker community, cybersecurity journalism, think tanks, academia, and state and local officials. The wide range of backgrounds represented in the membership is the fulfillment of remarks made by CISA Director Jen Easterly last month, when she was quoted as saying she wanted to "ignite the power of hackers and researchers and academics."[7]

The Committee's charter recommended between one and three representatives from twelve specific industries, which included healthcare and chemical, but it allows "other relevant fields identified by the [CISA] Director" to be added. Furthermore, the charter allows the Committee to be composed of thirty-five members, which will allow the current roster of twenty-three to be expanded as needed.

The twenty-three announced members include Johnson & Johnson CISO Marene Allison; Austin (Texas) Mayor Steve Adler; founder and President of Def Con Communications Jeff Moss; former longtime New York Times lead cybersecurity reporter Nicole Perlroth;

and Illinois Homeland Security Advisor and Director of the Illinois Emergency Management Agency (IEMA) Alicia Tate-Nadeau. The full list can be found on CISA's Cybersecurity Advisory Committee page at CISA.gov.[8]

Action & Analysis

Included with H-ISAC Membership

3. NDAA Incident Reporting Update

Negotiations on the annual *National Defense Authorization Act* (NDAA) have come to a close without the inclusion of cyber incident reporting. Despite strong bi-partisan support in both the House and Senate, lawmakers were unable to find an agreement on a path forward in the limited time available. The failure to include cyber incident reporting in the NDAA almost certainly signals that the issue will go unaddressed in 2021 and creates uncertainty for 2022.

As a reminder, the NDAA is essentially considered "must pass" legislation that has been successfully pushed through for around 60 consecutive years. This status makes it a prime candidate for members of Congress to attempt to tack on legislation in the form of amendments, and the Senate version alone was the subject over 700. Most of these amendments never had much of a chance to be seriously considered, but cyber incident reporting was an issue that appeared to have a real chance of making the cut.

For reference, the Senate cyber incident-reporting language included:

- **Covered Entities:** To be determined by rulemaking to an extent, but the healthcare sector would be expected to be covered
- **Covered Events:** Cyber Incidents / ransomware payments – Details to be determined through rulemaking
- **Reporting Timelines:** 72 hours after a covered entity reasonably believes that a covered cyber incident has occurred / 24 hours after a ransom payment has been made
- **Reporting Requirements:** Covered entities are required to submit supplemental reports if situations change after their initial reporting
- **Third-Party Reporting:** Covered entities may use/request third parties to submit required reports on their behalf
- **Compliance:** CISA may subpoena organizations for information
- **Information Sharing Protection:** Legislation prohibits the use of reported information in any regulatory action, exempts the information from Freedom of Information Act requests, and preserves protections such as trade secret protection and attorney-client privilege

- **Rulemaking Timeline:** Proposed rulemaking within two years, with a Final Rule within eighteen months after that.

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, December 7th:

- Senate – Committee on Finance: Hearings to examine promoting competition, growth, and privacy protection in the technology sector.

Wednesday, December 8th:

- No relevant hearings

Thursday, December 9th:

- No relevant hearings

International Hearings/Meetings –

- No relevant meetings

EU –

- No relevant meetings

Conferences, Webinars, and Summits –

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

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who 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, and 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.

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

---

[1] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

---

[2] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

[3] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657

[4]https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6657_aspassed/toc_pdf/20182b01.pdf;fileType=application%2Fpdf

[5]https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Advisory%20Committee%20Charter_508%20Compliant.pdf

[6] https://www.cisa.gov/sites/default/files/publications/CCAC_Member_Balance_Plan.pdf

[7] https://www.nextgov.com/cybersecurity/2021/11/cisa-director-appoint-hackers-cybersecurity-advisory-committee/186776/

[8] https://www.cisa.gov/csac-members