Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 43daee8f | May 19, 2023, 10:21 AM

This week, *Hacking Healthcare* provides an overview of a new U.S. Senate bill that purports to address the cybersecurity barriers affecting rural hospitals. We examine what the provisions of the bill call for, assess the likelihood of it making a significant positive impact, and then place it within the larger conversation on critical infrastructure cybersecurity that is currently taking place in the United States.

Welcome back to *Hacking Healthcare*.

Rural Hospital Cybersecurity Targeted for Aid by new Senate Bill

With both the Biden administration and Congress increasingly concerned about the cybersecurity of critical infrastructure sectors, it's heartening to see at least some of those efforts are targeting small and rural entities, which often lack the resources to consistently improve their cybersecurity maturity. For example, toward the end of last week, a new bill was introduced into the U.S. Senate that seeks to address cybersecurity maturity of rural hospitals. Just how effective these efforts are likely to be is uncertain.

S. 1560, the *Rural Hospital Cybersecurity Enhancement Act*, is a bipartisan bill introduced on May 11 by Sens. Josh Hawley (R-MO) and Gary Peters (D-MI). The bill's primary purpose is to "require the development of a comprehensive rural hospital cybersecurity workforce development strategy," but it would also require the Cybersecurity and Infrastructure Security Agency (CISA) to develop "instructional materials for rural hospitals that can be used to train staff on fundamental cybersecurity efforts."[i]

The bill's central component is an effort to address the workforce shortages of cyber professionals available to rural hospitals. To accomplish this goal, the bill would require the Secretary of the Department of Homeland Security (DHS) and the Director of CISA to develop a comprehensive cybersecurity workforce development strategy focusing on rural hospitals.

The strategy would, at a minimum, need to consider:[ii]

1. Partnerships between rural hospitals, educational institutions, private sector entities, and nonprofit organizations to develop, promote, and expand cybersecurity education and training

programs tailored to the needs of rural hospitals.

2. The development of a cybersecurity curriculum and teaching resources that focus on teaching technical skills and abilities related to cybersecurity in rural hospitals for use in community colleges, vocational schools, and other educational institutions located in rural areas.

3. Recommendations for legislation, rulemaking, or guidance to implement the components of the rural hospital cybersecurity workforce development strategy.

Going forward, the Secretary of DHS will also need to submit reports to Congress on:[iii]

1. Updates to the rural hospital cybersecurity workforce development strategy, as appropriate;

2. Any programs or initiatives established pursuant to the rural hospital cybersecurity workforce development strategy, as well as the number of individuals trained or educated through such programs or initiatives;

3. Additional recommendations for legislation, rulemaking, or guidance to implement the components of the rural hospital cybersecurity workforce development strategy; and

4. The effectiveness of the rural hospital cybersecurity workforce development strategy in addressing the need for skilled cybersecurity professionals in rural hospitals.

The bill is currently with the Committee on Homeland Security and Governmental Affairs.

Action & Analysis
****Included with Health-ISAC Membership****

Congress

Tuesday, May 16
House of Representatives: Energy and Commerce Committee Oversight and Investigations Subcommittee Hearing: “Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies”

Wednesday, May 17
No relevant meetings

Thursday, May 18
No relevant hearings

International Hearings/Meetings

No relevant meetings

EU

No relevant meetings

[i] https://www.congress.gov/bill/118th-congress/senate-bill/1560/text?s=1&r=4
[ii] https://www.congress.gov/bill/118th-congress/senate-bill/1560/text?s=1&r=4
[iii] https://www.congress.gov/bill/118th-congress/senate-bill/1560/text?s=1&r=4
[iv] https://www.congress.gov/bill/118th-congress/senate-bill/1560/text?s=1&r=4
[v] https://www.congress.gov/bill/118th-congress/senate-bill/1560/text?s=1&r=4

Reference | References

congress
Health-ISAC

Report Source(s)

Health-ISAC

Tags

Legislation, Hacking Healthcare, Workforce, Congress, Senate

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

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, 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.

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.