Hacking Healthcare- Weekly Blog

Hacking Healthcare TLP:WHITE Alert ID : 1ef74519 Feb 19, 2025, 03:39 PM

This week, Health-ISAC®'s Hacking Healthcare® examines one of the United States' foundational cyber information sharing laws. Join us as we explain what the Cybersecurity Information Sharing Act of 2015 is and why it is so important. Then, in our Action & Analysis section, we break down what a lack of reauthorization might mean for entities that rely on it to facilitate cyber information sharing and how Health-ISAC organizations can help support efforts to ensure it is reauthorized.

Welcome back to Hacking Healthcare®.

CISA 2015 Reauthorization

It is widely acknowledged that cyber information sharing provides enormous benefits for participants and that it is a critical component of keeping networks and infrastructure safe. While the public and private sectors have room for further improvement, a significant factor in cyber information sharing within the United States reaching the level of maturity it is at today is thanks to the Cybersecurity Information Sharing Act of 2015 (CISA 2015). Unfortunately, the framework and protections that it provides may not be around much longer.

What Is CISA 2015?

Passed into law in late 2015, CISA 2015 was a bipartisan proposal that sought to encourage voluntary cyber information sharing between the government and the private sector and within the private sector itself. Included in the final law were provisions that:[i]

- Defined terms like "cybersecurity threat," "cyber threat indicator," "defensive measure," and "information system" - Sec. 102
- Instructed federal government entities to develop the means to facilitate and promote the "timely sharing" of threat indicators, defensive measures, and information relating to cybersecurity threats and outlined conditions for sharing with federal entities, non-federal entities, and the general public - Sec. 103
- Provided authorizations, with exceptions, for non-federal entities to share or receive information with non-federal entities or the government. - Sec. 104

And critically:

- Provided relatively extensive liability protections to entities acting within the bounds of CISA 2015, as well as enough privacy and civil liberties protections to mitigate concerned groups - Sec. 106

All of these elements combined to create a framework that signaled intent from the federal government that voluntary cyber information sharing was a practice that should be embraced. The Cybersecurity and Infrastructure Security Agency (CISA) has utilized CISA 2015 as a foundation for many of its information-sharing programs and processes. Former CISA Executive Director Brandon Wales relayed as much at a January Congressional hearing by stating that "This Act is an important tool to facilitate the flow of critical cyber intelligence between industry and government, and letting it expire would be a huge step back."[ii]

So, what is the reauthorization issue?

What Is Reauthorization?

Within the United States, not all laws exist in perpetuity. It isn't uncommon for proposed laws and regulations to include a "sunset provision," which outlines a date by which the enacted law would cease to be effective, barring some additional action to extend or "reauthorize" it.

There are a variety of reasons why a proposed legislation or regulation might be introduced with a "sunset provision." It might be believed that the issue being addressed is time sensitive, or it might be that it is unclear just how a law or regulation might work in practice, and a sunset provision can help act as a backstop for unintended consequences, or it may help ensure that a created government program doesn't go funded and staffed forever regardless of its continued usefulness.

Regardless of why CISA 2015 has a sunset provision, although it is likely related to the complicated nature of its development and the negotiations and compromises that were required to get it into law, CISA 2015 is currently set to sunset on September 30, 2025.

If Congress does not take action to replace or reauthorize CISA 2015 before that date, the law will lapse, and the framework and protections outlined within it will no longer be effective.

Action & Analysis

Included with Health-ISAC Membership

[i] https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act

[ii] https://insidecybersecurity.com/daily-news/it-info-sharing-leader-emphasizes-importance-reauthorizing-cisa-2015-law-industry-players

[iii] https://www.cisa.gov/sites/default/files/2024-04/NonFederal-Entity-Sharing-Guidance-April-2024-Update.pdf

[iv] https://www.cisa.gov/sites/default/files/2023-07/Final%20Procedures%20Related%20to%20the%20Receipt%20of%20Cyber%20Threat%20Indicato

[v] https://www.cisa.gov/sites/default/files/2023-02/cisa_2015_pcl_final_guidelines_2022_periodic_review_508c.pdf

Report Source(s)

Health-ISAC

Reference

cisa
cisa
cisa
insidecybersecurity
cisa

Tags

CISA 2015, Legislation, Hacking Healthcare, Trump administration, Information Sharing, Congress

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 Councils 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 Councils 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-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs 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 Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org