HACKING HEALTHCARE

Hacking Heathcare - Weekly Blog

TLP:WHITE

Oct 24, 2025

This week, Health-ISAC®'s Hacking Healthcare® provides an update on the continuing U.S. government shutdown and negotiations around reauthorization of the Cybersecurity Information Sharing Act of 2015 ("CISA 2015"). We examine what has changed since the shutdown started, what to expect in the event the shutdown is resolved, and some approaches Health-ISAC members may wish to consider given the continuing lack of CISA 2015 protections.

Welcome back to Hacking Healthcare®.

CISA 2015 Reauthorization

Despite outspoken support from both Republicans and Democrats, Congress has yet to find a breakthrough to reauthorize CISA 2015.

In addition to efforts preexisting the shutdown, the most recent development was the introduction of the bi-partisan bill *S.2983 - Extending Expired Cybersecurity Authorities Act*.[i] This bill would cleanly reauthorize the CISA 2015 for another 10 years and would retroactively apply to October 1. Additionally, in an attempt to create distance between CISA 2015 and the Cybersecurity and Infrastructure Security Agency ("CISA") with which it shares an acronym, the bill would rename CISA 2015 to the *Protecting America from Cyber Threats Act*. Importantly, S. 2983 has passed through the Rule 14 process, a procedure which allows it to be

considered on the floor of the Senate without going through the Senate Homeland Security and Government Affairs Committee where Sen. Paul (R-KY) has continued to block attempts to move reauthorization forward.

Should the bill successfully pass through the senate, it may still have some hurdles to clear with Republicans in the House of Representatives. Some House Republicans have voiced similar concerns as Sen. Paul around the CISA agency, and they may seek to temper any CISA 2015 reauthorization bill, potentially by shortening the length of any reauthorization.

Finally, it appears that the potential reauthorization of CISA 2015 through the National Defense Authorization Act ("NDAA"), the annual "must pass" end of year legislative package, is in doubt. Neither the Senate NDAA nor the House of Representatives NDAA includes CISA reauthorization language. Democrats in the Senate pointed to Sen. Paul as the reason it failed to make the cut.[ii]

Shutdown: Cybersecurity and Infrastructure Security Agency (CISA) Personnel Reductions

The Trump administration's remaking of the federal workforce has continued during the shutdown. With nearly 65% of CISA staff presumably furloughed as outlined in the Department of Homeland Security's ("DHS") shutdown plan,[iii] the agency was already in a reduced capacity when further reductions in force and mandatory reassignments were announced. These appear to have focused primarily on the Stakeholder Engagement Division and Infrastructure Security Division.[iv] [v] However, it is worth noting that these further reductions appear consistent with long signaled cuts. CISA's Fiscal Year 26 Congressional Budget Justification from earlier in the year proposed massive decreases in funding for the stakeholder engagement in particular (cutting the Stakeholder Engagement budget line item down from ~$43 million to $3 million).[vi]

We will not go into depth on U.S. government shutdown procedures and effects, but for those interested there are useful primers available.[vii]

Action & Analysis

Included with Health-ISAC Membership

[i]https://www.congress.gov/bill/119th-congress/senate-bill/2983?s
[ii]https://insidecybersecurity.com/daily-news/senate-passes-fiscal-2026-ndaa-without-reauthorization-major-info-sharing-law

[iii]https://www.dhs.gov/sites/default/files/2025-09/2025_0930_dhs_procedures_related_to_a_lapse_in_appropriations.pdf
[iv]https://www.nextgov.com/cybersecurity/2025/10/multiple-cisa-divisions-targeted-shutdown-layoffs-people-familiar-say/408773/?oref=ng-home-top-story
[v]https://www.cybersecuritydive.com/news/cisa-layoffs-reassignments-dhs-white-house-government-shutdown/802723/
[vi] https://www.dhs.gov/sites/default/files/2025-06/25_0613_cisa_fy26-congressional-budget-justificatin.pdf
[vii] For those interested in learning more about how U.S. government shutdowns occur and how they are resolved, The Brookings Institution has a good primer here: https://www.brookings.edu/articles/what-is-a-government-shutdown-and-why-are-we-likely-to-have-another-one/ and the U.S. Congressional Research Service has useful guides here: https://www.congress.gov/crs-product/R47693
[viii] https://www.reuters.com/world/us/us-investment-boom-is-sustainable-bessent-says-2025-10-15/

Reference(s)	brookings, cybersecuritydive, dhs, reuters, dhs, nextgov, insidecybersecurity, congress, congress
Report Source(s)	Health-ISAC

Release Date
Oct 24, 2025 (UTC)

Alert ID 75471e99

View Alert

Share Feedback
was this helpful? |

Tags CISA 2015, Information Sharing, Government, Shutdown, Congress

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

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**