HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

TLP:WHITE

Jun 06, 2025

This week, Health-ISAC®'s Hacking Healthcare® examines where things stand several months into the Trump Administration's term regarding healthcare and cybersecurity. This edition of Hacking Healthcare will recap some of the significant developments from the beginning of Trump's term to Thursday's confirmation hearings, and then will assess what we might expect to see happen next.

Welcome back to Hacking Healthcare®.

Trump Administration Update: Cybersecurity and Healthcare
It has been a whirlwind few months for the U.S. government. The Trump Administration has made or attempted to make seismic changes to the organization, mission, and process of the U.S. government, including to the entities that oversee cybersecurity and the health sector. While there has been a heavy focus on reorganization, reprioritization, and downsizing, there is a sense that things are heading into a new phase. Let's explore where we are, and where we may be heading.

Government Cybersecurity Capacity

The government's overall cybersecurity capacity, including to support the health sector, appears to have been impacted. The Trump Administration has proposed cutting nearly $500 million from the Cybersecurity and Infrastructure

Security Agency (CISA) budget alongside roughly 30% of CISA personnel, according to their FY 2026 budget proposal.[i]

Eric Geller's analysis notes that that $216 million, roughly 18% of the current funding, would be cut from "CISA's Cybersecurity Division, which leads efforts to protect government networks and help defend critical infrastructure."[ii]That same reporting suggests a 30% cut to the budget of "the Integrated Operations Division, which coordinates CISA's distribution of support and services to companies and local governments across the country", as well as "$62.2 million, 62% of current funding," from CISA's Stakeholder Engagement Division and "$97.4 million, a 73% reduction" from the National Risk Management Center.[iii]The proposed cuts would also affect nearly 1,100 positions and the Joint Cyber Defense Collaborative (JCDC).

While CISA has been the focus of the Trump Administration cuts and reorganization has not stopped there.

The National Security Council (NSC), which has historically employed a number of experts in cybersecurity related positions, has been drastically reduced. Reporting at the end of May highlighted cuts to roughly half of the NSC's staff, and cyber related positions have been significantly reduced.[iv] The Department of Health and Human Services has also seen significant personnel cuts and reorganization, alongside major funding cuts being proposed by the Trump Administration.

Leadership and Cyber Policy Priorities

The Trump Administration has yet to confirm a new Director for CISA or a National Cyber Director. The slower approach to nominating and confirming these positions has appeared to take on a heightened sense of urgency given the significant shakeups of senior personnel. It is perhaps for this reason that an attempt to get Trump's nominees, Sean Cairncross for National Cyber Director and Sean Plankey for CISA Director, in front of the Senate for a confirmation hearing was hastily arranged this past Thursday.

While an unfortunate logistical issue between either the Federal Bureau of Investigation (FBI) or the Department of Homeland Security (DHS)/CISA appears to have led to Plankey being pulled from the hearing, Cairncross was vetted and did lay out some priorities for his role with the Office of the National Cyber Director.
In his written testimony, Cairncross outlined the following:[v]

- He believes that broad public-private multi-stakeholder processes are key to effective cybersecurity

- The Office of the National Cyber Director (ONCD)[vi] needed to become what was envisioned when it was created, as the central cyber policy hub of the U.S. government
- Government policy "must" promote information exchange and engage cross-sectorally
- There needs to be a streamlining of federal cyber regulations and compliance burdens - one that moves away from "a checklist that increases costs and slows incident preparedness or response effectiveness"

Furthermore, during questioning, he also stated the following:[vii]

- He was committed to working to extend the Cybersecurity Information Sharing Act of 2015 (CISA 2015)
- He was interested in working on the issue of state and local cybersecurity grants
- It was time for the U.S. government to impose costs on malicious cyber actors and create strategic dilemmas for them
- China was the single biggest cyber threat
- He was very interested in working with Congress and the private sector to gain a better understanding of cybersecurity threats and risks facing the health sector, particularly those facing rural hospitals

Advisory Boards and Committees

The Trump Administration's move to end the various cyber advisory boards and committees has been met with a mixture of approval from those seeking reform or cost-savings, and disapproval from those worried the lack of these forums for public-private collaboration or governmental review is ultimately harmful.

Since their effective dissolution, little has happened to reconstitute these boards and committees and the proposed cuts to JCDC funding mentioned above do not appear to bode well for at least some of them. This has sparked at least four Senate democrats to publicly call on DHS to reinstate the Cyber Safety Review Board (CSRB), which had previously released comprehensive reports on Log4j, Lapsus$, and the Microsoft Exchange Online intrusion.[viii]

Action & Analysis

Included with Health-ISAC Membership

[i]https://www.dhs.gov/sites/default/files/2025-05/25_0530_cisa_fy26-congressional-budget-justification.pdf
[ii] https://www.cybersecuritydive.com/news/cisa-trump-2026-budget-proposal/749539/
[iii] https://www.cybersecuritydive.com/news/cisa-trump-2026-budget-proposal/749539/
[iv] https://www.politico.com/news/2025/05/23/trump-national-security-council-00368787
[v] https://www.hsgac.senate.gov/wp-content/uploads/Prepared-Statement-Cairncross-2025-06-05.pdf
[vi] The ONCD advises the President of the United States on cybersecurity policy and strategy and was established by Congress in 2021. The ONCD is housed within the Executive Office of the President.
[vii] https://www.hsgac.senate.gov/hearings/nominations-10/
[viii]https://www.warner.senate.gov/public/_cache/files/b/b/bbf743ed-a62b-4ddd-acbd-9efbb1b57e59/8F69B96E6BE00A94BA8DBDD3B9443CF17A885D52A40748B7A5000FDFFD217870.quill---letter-l27283---250521.warner-noem-csrb-reappointment---version-3---05-29-2025-02-29-pm.pdf

Reference(s)	dhs, senate, senate, politico, senate, cybersecuritydive
Report Source(s)	Health-ISAC

Alert ID 3ea5605d

View Alert

Share Feedback
was this helpful? |

Tags CISA 2015, ONCD, Hacking Healthcare, Trump administration, CISA

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

Download Health-ISAC's Information Sharing App.

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