



This week, Health-ISAC®'s Hacking Healthcare® examines how President Trump's first two weeks have impacted U.S. cyber and technology policy. In particular, the Action and Analysis section examines how the regulatory freeze may impact the Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) and the HIPAA Security Rule NPRM, what a new AI policy might mean for AI in healthcare, and how the dismissal of various cyber advisory committees and boards may have negative effects.

Welcome back to Hacking Healthcare®.

## **Trump Administration Review**

The first week and a half of the Trump administration has provided no shortage of topics for conversation. This week, we wanted to highlight a few particular actions that were taken that could have an effect on healthcare and cybersecurity. In particular, the regulatory freeze, a new approach to artificial intelligence (AI) policy, and uncertainty over some of the many cyber advisory boards.

### Regulatory Freeze

As expected, the Trump administration promptly instructed all executive departments and agencies to halt in-progress regulatory work.[i] This included:

1. Instructing executive departments and agencies to “not propose or issue any rule in any manner, including by sending a rule to the Office of the Federal Register”[ii] until appropriate, Trump vetted personnel reviewed and approved it.[iii]
2. Instructing executive departments and agencies to “Immediately withdraw any rules that have been sent to the [Office of the Federal Register] but not published in the Federal Register.”[iv]
3. Instructing executive departments and agencies to “consider postponing for 60 days from the date of this memorandum the effective date for any rules that have been published in the Federal Register, or any rules that have been issued in any manner but have not taken effect, for the purpose of reviewing any questions of fact, law, and policy that the rules may raise.”[v] In addition, departments or agencies were told to consider opening a comment period to allow for “comments about issues of fact, law, and policy” while also instructing them to “consider further delaying, or publishing for notice and comment, proposed rules further delaying such rules beyond the 60-day period.”[vi]

## AI Policy

The Trump administration inherited AI policies from the Biden administration, including Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, which established a “government-wide effort to guide responsible artificial intelligence (AI) development and deployment”[vii] and Executive Order 14141, Advancing United States Leadership in Artificial Intelligence Infrastructure, which included ensuring the development of domestic AI infrastructure.

Since the transition, the Trump administration has rescinded Executive Order 14110, left 14141 unchanged as of this writing, and published an as-of-yet unnumbered executive order, Removing Barriers To American Leadership In Artificial Intelligence.[viii] The new executive order seeks to remove barriers to innovation, which, in this case, appears to refer to the Biden-era policy’s emphasis on minimizing bias and the potential for unintended harm. In addition, the new executive order seeks to create a new AI action plan within 180 days, complete a review of the policies and actions resulting from the rescinded Biden executive order, and revise them to better align with the Trump administration’s policies.

## Advisory Boards/Committees

The Trump administration has effectively ended the work of Department of Homeland Security (DHS) advisory committees, at least temporarily. All members of these committees are reported to have been dismissed if they had not already resigned.[ix] This was described as part of a “commitment to eliminating the misuse of resources and ensuring that DHS activities prioritize our national security.”[x]

Included in the purge was the Cyber Safety Review Board (CSRB), which had previously published reports on the 2023 Microsoft Exchange Online intrusion, the cyber threat group Lapsus\$, and the Log4j event. The CSRB was in the process of investigating Chinese hacks in the telecommunications sector. It has been reported that the Artificial Intelligence Safety and Security Board, the Critical Infrastructure Partnership Advisory Council, the National Security Telecommunications Advisory Committee, the National Infrastructure Advisory Council, and the Secret Service’s Cyber Investigations Advisory Board were all also affected.[xi]

## *Action & Analysis*

### ***\*Included with Health-ISAC Membership\****

[i] <https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/>

[ii] <https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/>

[iii] With some carve outs for OMB to address particular issues (e.g. emergency situations)

[iv] <https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/>

[v] <https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/>

[vi] <https://www.whitehouse.gov/presidential-actions/2025/01/regulatory-freeze-pending-review/>

[vii] <https://crsreports.congress.gov/product/pdf/R/R47843>

[viii] <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>

[ix] <https://therecord.media/trump-dhs-removal-private-sector-members-advisory-boards>

[x] <https://www.documentcloud.org/documents/25500093-dhs-advisory-boards-termination-letter/>

[xi] <https://bsky.app/profile/ericjgeller.com/post/3lgbpqmxeok2f>

[xii] Hacking Healthcare addressed the HIPAA Security Rule NPRM specifically a few weeks ago. That content can be found here: <https://health-isac.org/health-isac-hacking-healthcare-1-10-2025/>

[xiii] <https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements>

[xiv] <https://bsky.app/profile/ericjgeller.com/post/3lgbpqmxeok2f>

## Report Source(s)

Health-ISAC

## Release Date

Feb 02, 2025, 11:00 PM

---

**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](mailto:jbanghart@h-isac.org) and [jfbanghart@venable.com](mailto:jfbanghart@venable.com).

Tim can be reached at [tmcgiff@venable.com](mailto:tmcgiff@venable.com).

### **Turn off Categories:**

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" [here](#).

### **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](mailto: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](mailto:toc@h-isac.org)