



## Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™

TLP:WHITE

Alert ID : 16553645

Jun 07, 2024, 11:58 AM

This week, *Hacking Healthcare*™ examines a new report from the Cyberspace Solarium Commission 2.0 that assesses the state of healthcare cybersecurity in the U.S. and provides recommendations for public and private sector alike. We briefly detail the contents of the report before digging into some of the notable takeaways in the action and analysis section.

Welcome back to *Hacking Healthcare*™

### **Cyberspace Solarium Commission 2.0 Report Highlights Health-ISAC and Illustrates Healthcare Cybersecurity Maturity Challenge**

Continuing the work of the influential Cyberspace Solarium Commission (CSC), the CSC 2.0 project has recently released a report detailing challenges facing the healthcare and public health (HPH) sector alongside 13 recommendations for improvements. Let's review the issues they've highlighted and ways in which they believe they might be addressed.

#### What Is the CSC and the CSC 2.0 Project?

The CSC was "established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019."<sup>[i]</sup> It led to the creation of a bipartisan group of Congress members and private sector experts who came together to develop a seminal report aimed at "develop[ing] a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences."<sup>[ii]</sup> The report itself is a thorough 182-page document consisting of over 80 recommendations across six distinct pillars.<sup>[iii]</sup>

While the CSC and its works have been impactful for helping to guide U.S. cyber policy over the years, it was not meant to last forever. As such, while the original CSC as outlined by the John S. McCain National Defense Authorization Act for Fiscal Year 2019 has been sunset, the CSC 2.0 project has taken the reins to "preserve their legacy and continue their work."<sup>[iv]</sup>

#### CSC 2.0 Healthcare Report

The report opens with an overview of some of the well-known cyber challenges the HPH sector faces, some specific challenges to rural and small HPH entities, and some of the current government efforts to

address these challenges. Additionally, the scene-setting section of the report champions the value of industry-led collaboration, where the efforts of Health-ISAC and Health Sector Coordinating Council (HSCC) are highlighted.

Citing a number of recent high-profile cyberattacks against U.S.-based healthcare organizations since 2021, the report “provides 13 recommendations directed at the executive branch, Congress, and the healthcare sector to guide the sector into a safer, more resilient future.”[\[v\]](#)

At a high level, the recommendations are:

#### **Executive Branch**

1. Develop New, Long-Term Sector-Specific Cybersecurity Objectives
2. Work With Industry to Identify, Prioritize, and Secure Life-Saving Services
3. Iteratively Update HHS’s Cybersecurity Performance Goals (CPGs)
4. Accelerate the CPG Compliance Incentivization Program’s Timeline
5. Create a Rural Hospital Cybersecurity Workforce Development Strategy
6. Reassess Systemically Important Entities List

#### **Congress**

7. Ensure Sector Risk Management Agency (SRMA) Resources and Organizational Structure Are Optimally Efficient
8. Increase Funding for HHS’s SRMA Capabilities
9. Fund HHS’s CPG Resourcing and Incentive Program
10. Direct and Resource HHS to Establish a Rural vCISO Pilot Program

#### **Industry**

11. Spend More on Cybersecurity
12. Provide Cyber Hygiene Training to All Employees
13. Develop Regional Contingency Plans for Healthcare Providers

While these are more thoroughly developed in the full report, we dig deeper into some of the notable aspects in the Action & Analysis section below.

#### *Action & Analysis*

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

Upcoming International Hearings/Meetings:

- EU

No relevant meetings at this time

- US

No relevant meetings at this time

- Rest of World

No relevant meetings at this time

[i] <https://www.solarium.gov/>

[ii] <https://www.solarium.gov/>

[iii] CSC Final Report.pdf

[iv] <https://cybersolarium.org/>

[v] <https://cybersolarium.org/csc-2-0-reports/healthcare-cybersecurity-needs-a-check-up/>

[vi] <https://cybersolarium.org/wp-content/uploads/2024/06/csc2.0-healthcare-cybersecurity-needs-a-check-up-report.pdf>

#### Report Source(s)

Health-ISAC

#### Release Date

Jun 07, 2024, 11:59 PM

---

#### Reference | References

[solarium](#)

[Google Threat Horizons Report](#)

[cybersolarium](#)

[cybersolarium](#)

[cybersolarium](#)

#### Tags

Cyberspace Solarium Commission, CPGs, Hacking Healthcare

---

**TLP:WHITE:** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

#### For Questions and/or Comments:

Please email us at [contact@h-isac.org](mailto:contact@h-isac.org)

#### 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 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC's annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC's 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).

### **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](mailto:membership@h-isac.org) for access to Cyware.

### **For Questions or Comments:**

Please email us at [toc@h-isac.org](mailto:toc@h-isac.org)