Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare ○ TLP:WHITE Alert ID : b0e18f42 Feb 27, 2023, 09:48 AM

This week, Hacking Healthcare assesses the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC) 2023 planning agenda. We break down the issue areas that they plan on addressing and the kind of impact that they may have on the healthcare sector.
Welcome back to *Hacking Healthcare*.

CISA's JCDC Releases 2023 Planning Agenda

At the end of January, the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC) released their 2023 Planning Agenda, which highlights the group's specific areas of interest that they plan on addressing in 2023.[i] While some may have expected healthcare to be featured more prominently, the action items listed have the potential to make a beneficial impact on the sector.

For those who may have trouble keeping up with all the various government initiatives, the JCDC is a U.S. public-private cybersecurity organization that leverages new authorities granted by Congress in the 2021 National Defense Authorization Act to "unify cyber defenders from organizations worldwide."[ii] This mission includes attempting to increase collaboration to yield benefits in addressing cyber vulnerabilities, while also proactively thinking about potential cyber risks that may manifest in the future, and how to best combat them. In practice, this mission has manifested in guidance, toolkits, international support of U.S. allies, threat and vulnerability amplification, and attempts at general information sharing improvements.

The 2023 agenda is built around the overall goal of bringing the government and private sector together to develop and execute cyber defense plans that achieve specific risk reduction goals and enable focused collaboration. The three areas of focus this year are: systemic risk, collective cyber response, and high-risk communities, all elements of the cyber ecosystem that can be abused by malicious actors to achieve widespread impacts.[iii]

In the 2023 agenda, the JCDC plans to convene partners for the following efforts:[iv]

- Understand and mitigate risks potentially posed by open-source software (OSS) used in industrial control systems

- Advance cybersecurity and reduce supply chain risk for small and medium critical infrastructure entities through collaboration with remote monitoring and management, managed service providers, and managed security service providers

- Deepen operational collaboration and integration with the Energy Sector and identify approaches to enhance security and resilience of edge devices for the water sector

In addition, the "JCDC will lead an effort to update the National Cyber Incident Response Plan, in close coordination with the Federal Bureau of Investigation and other partners, which will include articulating specific roles for non-federal entities in organizing and executing national incident response activities."[v] The JCDC will also "lead collaborative planning efforts with non-government organizations, government, and industry stakeholders to develop a cyber defense plan for civil society organizations that are at high risk of being targeted by foreign state actors."[vi]

The JCDC expects to begin planning efforts related to OSS and scaling cybersecurity to support small and midsize critical infrastructure in the next few weeks.[vii]. They plan on addressing the rest of their agenda throughout the year while attempting to remain flexible in order to respond to current events.

Action & Analysis

Included with H-ISAC Membership

Wrap-up

Overall, we are cautiously optimistic that CISA and the JCDC will provide some tangible benefit to the healthcare sector over the course of the year, although we do hope that they will look for more opportunities to engage productively with the healthcare sector given its limited representation and the limited resources of its organizations.

Congress

Tuesday, February 7th:

- No relevant hearings

Wednesday, January 8th:

- No relevant hearings

Thursday, January 29th:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

- No relevant meetings

[i] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[ii] https://www.cisa.gov/jcdc
[iii] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[iv] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[v] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[vi] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[vii] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[viii] https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/
[ix] https://www.cisa.gov/uscert/ncirp
[x] https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
[xi] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[xii] https://healthitsecurity.com/news/white-house-sets-sights-on-new-healthcare-cybersecurity-standards
[xiii] https://healthitsecurity.com/news/white-house-sets-sights-on-new-healthcare-cybersecurity-standards
[xiv] https://www.cisa.gov/blog/2023/01/26/jcdc-focused-persistent-collaboration-and-staying-ahead-cyber-risk-2023
[xv] https://www.census.gov/library/stories/2020/10/health-care-still-largest-united-states-employer.html

Reference | References

CISA
Health-ISAC DDoS Whitepaper
Whitehouse
Health IT Security
CISA
CISA
census
CISA

Report Source(s)

Health-ISAC

Tags

JCDC, Hacking Healthcare, CISA, Collaboration

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Written by John Banghart, who 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.

John can be reached at jbanghart@h-isac.org and jfbanghart@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 for access to Cyware.