SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare ○ TLP:WHITE Alert ID : 7ed2ded0 Feb 01, 2024, 08:52 AM

This week, *Hacking Healthcare*™ examines the publication of healthcare specific cybersecurity performance goals (CPGs). We breakdown where this initiative has come from, what the CPGs are, how they might eventually be used, and what Health-ISAC members may wish to consider doing with them in the meantime.

Welcome back to *Hacking Healthcare*™.

HHS Publishes Healthcare Sector Cybersecurity Performance Goals

Last Wednesday, the U.S. Department of Health and Human Services (HHS)'s Administration for Strategic Preparedness and Responses (ASPR) announced the publication of "voluntary health care specific cybersecurity performance goals (CPGs)."[i] These healthcare and public health sector (HPH) specific CPGs were developed with the intention of improving the security and resiliency of healthcare sector entities and with an eye towards facilitating "new enforceable cybersecurity standards across HHS policies and programs that are informed by these CPGs."[ii] Let's examine the newly released HPH CPGs and the concurrently released *Healthcare and Public Health Sector Cybersecurity Gateway* website to assess the impact this new product may have.

HPH CPGs: Origin

For those of you having trouble remembering why HHS has expended the resources to help create healthcare specific CPGs, a brief refresher is in order. As part of the Biden administration's longstanding focus on elevating and maturing the government's cybersecurity policy, the White House has continually developed executive orders and actions on the issue. One of these, published back in Late July of 2021, was the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*.[iii]

That document identified the need for "baseline cybersecurity goals that are consistent across all critical infrastructure sectors, as well as a need for security controls for select critical infrastructure that is dependent on control systems."[iv] Ultimately, the task of developing a consistent baseline of "cybersecurity goals" fell to the Department of Homeland Security (DHS) and their Cybersecurity and Infrastructure Security Agency (CISA).

Published in October of 2022, the Cross-Sector Cybersecurity Performance Goals were touted as "A common set of protections that all critical infrastructure entities - from large to small - should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques."[v] As a follow-on action, and in recognition that every critical infrastructure sector has its own unique risks, threats, and implementation challenges, CISA was tasked with building out sector-specific CPGs.

HPH CPGs: Content

So, what can you expect from this new document?

Thankfully, the organization and length of the HPH CPGs are comprehensible and reasonable, even if it is a bit of a departure from its parent Cross-Sector CPGs. At 13 pages, the document doesn't overwhelm and stays high-level. After a quick introduction, the document breaks down into roughly 3 components.

The first component introduces ten "Essential" and ten "Enhanced" goals, with the former "setting a floor of safeguards," while the later "[helping] healthcare organizations mature their cybersecurity capabilities." Each goal is accompanied by a brief definition and are mapped to the Health Industry Cybersecurity Practices (HICP).

The goals themselves should largely be familiar to organizations that have used HICP or come across some of CISA's cyber hygiene initiatives.[vi] Essential Goals include MFA implementation, the use of strong encryption, and basic incident planning and preparedness. The more mature Enhanced Goals add items like cybersecurity testing, third party vulnerability disclosure, and asset inventory.

The second component, making up the bulk of the document, is a more technical appendix that provides additional detail on each goal, the general types of threats mitigated by each, and how those goals map to the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF), HICP, and NIST's publication *800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations*.

Lastly, the third component is a mapping of the HPH CPGs to the Cyber Defense Matrix in an attempt to illustrate how the HPH CPGs might be deployed and how they provide protection to an organization.

Health Sector Cybersecurity Gateway

Concurrently announced with the HPH CPGs was the *Healthcare and Public Health Sector Cybersecurity Gateway* website, which is hoped will "[Connect] the Healthcare and Public Health (HPH) Sector with specialized healthcare specific cybersecurity information & resources from across the U.S. Department of Health and Human Services and other federal agencies."[vii] As of this writing, the Gateway appears to link to the HPH CPGs, and has a partially interactive "wheel" that links users to a variety of HHS departments and offices.

Action & Analysis
Included with Health-ISAC Membership

Additional Information

As a reminder for members, the Health-ISAC regularly puts out more timely announcements of topical policy developments than we are capable of with Hacking Healthcare's weekly cadence. We would encourage you to keep an eye out for these as they are published on the Cyware platform.

For those interested in reading more, please see the Health-ISAC HPH CPG Announcement here: https://health-isac.cyware.com/webapp/user/myfeeds/e8891935

Congress

Tuesday, January 30

No relevant hearings

Wednesday, January 31

No relevant meetings

Thursday, February 1

No relevant meetings

International Hearings/Meetings

No relevant meetings

EU

[i] https://aspr.hhs.gov/newsroom/Pages/HHS-Releases-CPGs-and-Gateway-Website-Jan2024.aspx

[ii] https://aspr.hhs.gov/newsroom/Pages/HHS-Releases-CPGs-and-Gateway-Website-Jan2024.aspx

[iii] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[iv] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[v] https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[vi] https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe

[vii] https://hphcyber.hhs.gov/

[viii] https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

Report Source(s)

Health-ISAC

Reference | References

CISA

Whitehouse
TOC Spotlight Webinar - Citrix Slides Attachment
CISA
HHS
HHS
HHS

Tags

Cyber Performance Goals, CPGs, Best Practices, HICP, hygiene, Hacking Healthcare, HHS

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

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 and jfbanghart@venable.com.
- Tim can be reached at 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 for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org