ANNOUNCEMENTS

HHS Releases New Voluntary Performance Goals to Enhance Cybersecurity Across the Health Sector and Gateway for Cybersecurity Resources

TLP:WHITE

Jan 30, 2024

On January 24, 2024, the U.S. Department of Health and Human Services (HHS), through the Administration for Strategic Preparedness and Response (ASPR), released voluntary health care specific cybersecurity performance goals (CPGs) and a new gateway website to help Health Care and Public Health (HPH) sector organizations implement these high-impact cybersecurity practices and ease access to the plethora of cybersecurity resources HHS and other federal partners offer.

As outlined in the recent HHS Health Care Sector Cybersecurity concept paper, HHS is publishing the CPGs to help healthcare organizations, and healthcare delivery organizations in particular, prioritize the implementation of high-impact cybersecurity practices. The HPH CPGs are designed to protect the healthcare sector from cyberattacks better, improve response when events occur, and minimize residual risk. HPH CPGs include both essential goals to outline minimum foundational practices for cybersecurity performance and enhanced goals to encourage the adoption of more advanced practices.

The HPH CPGs provide layered protection at different points of weakness in an organization's technology environment, which is crucial to increase cyber resilience and ultimately protect patient safety. Layered defense provides redundancy so if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way.

Both the essential and enhanced goals were informed by common industry cybersecurity frameworks, best practices, and strategies (e.g., Health Industry Cybersecurity Practices, NIST Cybersecurity Framework, and the National Cybersecurity Strategy and Implementation Plan), and are designed to directly address common attack vectors against U.S. domestic hospitals as identified in the 2023 Hospital Cyber Resiliency Landscape Analysis. As an example, according to the Landscape Analysis, 80% of cyber-attacks are identity-based (e.g., social engineering), compromising legitimate credentials to move laterally within organizations. Several essential CPGs, including implementing basic cybersecurity training, implementing email security measures, and revoking credentials for departing workforce members, are relatively lower-cost, high-yield actions to protect organizations from identity-based attacks. The more intensive enhanced goals like network segmentation prevent threat actors from moving laterally within organizations when they are compromised.

More information on these CPGs and HHS' cybersecurity work can be found here.

Reference(s)	HHS, HHS

Release Date
Jan 24, 2024 (UTC)

Incident Date
Jan 31, 2024 (UTC)

Alert ID e8891935

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags ASPR, HHS

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

HHS 405(d)
The 405(d) Program aims to develop consensus-based best practices and methodologies to strengthen the healthcare & public health (HPH) sector's cybersecurity posture against cyber threats. After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group developed Health Industry Cybersecurity Practice: Managing Threat and Protecting Patients, its first official Task Group product. The 405(d) Program and Task Group actively continues to develop new products to help further strengthen our sector.

For Questions and/or Comments
Please email us at contact@h-isac.org

Share Threat Intel
For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP "Share Threat Intel" Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Knowledge Base
Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

Download Health-ISAC's Information Sharing App.

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