Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Sector Publishes Guidance on Supply Chain Cybersecurity Risk Management

Washington, DC – October 15, 2019 - The Healthcare and Public Health Sector Coordinating Council (HSCC) today published a toolkit for small to mid-sized healthcare institutions to better ensure the security of the products and services they procure through an enterprise supply chain cybersecurity risk management program. The "Health Industry Cybersecurity Supplier Risk Management (HIC-SCRiM)" toolkit is intended to provide actionable guidance and practical tools to help organizations of limited scale or resources to manage the cybersecurity risks they face through their dependencies within the health system supply chain.

"By enabling these organizations to ensure secure products and services from their suppliers, we will leverage market forces to raise the bar across the healthcare supply chain to the benefit of all." said Greg Garcia, HSCC Executive Director of its Cyber Security Working Group.

The toolkit is aligned to the new Supply Chain requirements within the 2018 update to the NIST Cyber Security Framework, and provides concrete guidance on process and governance, as well as practical tools such as contractual language for different supplier relationship types, risk assessment and supplier inventory templates and policy examples. Co-chaired by Darren Vianueva of Trinity Health and Chris van Schijndel of Johnson & Johnson, the Supply Chain Security task group that developed the toolkit is made up of more than twenty supply chain and cybersecurity professionals from a broad spectrum of health sector organizations.

While it is primarily written for small and medium sized organizations, the guide also makes a call to action for large healthcare organizations, associations and consultancies to raise awareness and encourage adoption across the sector.

To access and download a copy of the HIC-SCRiM, go to https://HealthSectorCouncil.org/HIC-SCRiM .

This is the 5th best practices guidance published by the HSCC in 2019. Previous HSCC Joint Cybersecurity Working Group resources published this year include:

- Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO) – September: https://healthsectorcouncil.org/hic-miso/
- Health Industry Cybersecurity Workforce Development Guide (HIC-Work) - June: https://healthsectorcouncil.org/workforce-guide/
- Health Industry Cybersecurity Medical Device Joint Security Plan (HIC-JSP) - January: https://healthsectorcouncil.org/the-joint-security-plan/
- Health Industry Cybersecurity Practices (HICP) - January: https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/

About the Healthcare and Public Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG). The HSCC is an industry-driven public private partnership of health companies and providers developing collaborative solutions to mitigate threats to critical healthcare infrastructure. It is one of 16 critical infrastructure sectors organized to partner with the government under Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. The HSCC Joint Cybersecurity Working Group (JCWG) includes more than 200 medical device and health IT companies, direct patient care entities, plans and payers, labs, blood and pharmaceutical companies, and several government partners. The JCWG industry chair is Terence (Terry) Rice, Vice President, IT Risk Management and Chief Information Security Officer for Merck & Co.

For more information: Greg Garcia, HSCC Cybersecurity Working Group Executive Director: Greg.Garcia@HealthSectorCouncil.org or visit us online at https://healthsectorcouncil.org

##