Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Health Sector Publishes Guide for Cybersecurity Workforce Development

Washington, D.C., June 17, 2019 – Today, the Healthcare and Public Health Sector Coordinating Council (HSCC) released a tool kit for recruiting and retaining skilled cybersecurity workforce in the healthcare sector. The "Healthcare Industry Cybersecurity Workforce Guide: Recruiting and Retaining Skilled Cybersecurity Talent" addresses the growing need for cybersecurity talent in the health sector as cyber threats and vulnerabilities continue to grow.

The Workforce Guide helps hiring managers and Chief Information Security Officers think about cyber workforce development as a continuum, from: 1) Hiring students, to 2) Transitioning IT staff to cybersecurity responsibilities; 3) Developing and managing professional development programs for executive-track cybersecurity personnel; and 4) Outsourcing critical functions not otherwise resourced within the enterprise.

"Attracting and retaining cybersecurity talent is a major challenge in all industry sectors," said Greg Garcia, Executive Director for Cybersecurity of the HSCC. "But as medical and wearable healthcare technology become more connected, patient safety will increasingly rely on cyber safety, and a skilled workforce is essential to finding that balance."

A task force established in 2016 by the U.S. Department of Health and Human Services – the Health Care Industry Cybersecurity Task Force - reported in June 2017 that healthcare cybersecurity is in "critical condition" and cited the lack of a capable cybersecurity workforce. The task force identified six key imperatives to address the challenges, including developing the necessary healthcare workforce capacity to prioritize and ensure cybersecurity awareness and technical capabilities.

According to a 2018 survey by the Poneman Institute - *State of Cybersecurity in Healthcare Organizations in 2018*, 79 percent of respondents said it is difficult to recruit IT security personnel. And only half (51 percent) of respondents said their organizations have a Chief Information Security Officer.

Another survey by the American Medical Association found that 83% of physician practices have experienced some form of cybersecurity attack. And the majority of physicians surveyed (55%) said they are very or extremely concerned about future cyber attacks on their practice.

The HIC Workforce Guide was developed by members of the Health Sector Coordinating Council's Cybersecurity Working Group, referring to a range of best practices they found useful in maintaining a strong cybersecurity talent base. The guide is aimed particularly at small to mid-sized health delivery organizations and companies who don't have extensive resources for security but need a place to start. For a copy of the white paper, see https://healthsectorcouncil.org/workforce-guide.

###

About the Healthcare and Public Health Sector Coordinating Council (HSCC)
The HSCC is an industry-driven public private partnership of healthcare 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 Workforce Task Group developed this resource for the sector, and is co-chaired by Brandyn Blunt of Trinity Health and Marian Merritt of the National Initiative for Cybersecurity Education within the National Institute Standards and Technology.

For more information about the HSCC Joint Cybersecurity Working Group visit www.HealthSector.Council.org or contact Executive Director Greg Garcia at Greg.Garcia@HealthSectorCouncil.org