Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

Health Sector Coordinating Council Cybersecurity Working Group

2022 Annual Report

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Chairman's Forward

Erik Decker
Industry Co-Chair
HSCC Cybersecurity Working Group

Since our Cybersecurity Working Group was reorganized in 2017 with the coordination of our Executive Director, Greg Garcia, we have been preparing for the coming cyber-storm. We have made tremendous progress in our critical infrastructure partnership, to the point where we now meet bi-weekly with our Federal partners; we have spun up 15 task groups to produce content our industry needs; our work products have been recognized by Congress and added into law; and we have the attention of the highest federal officials from HHS, the Office of the National Cybersecurity Director (ONCD), CISA and the National Security Council. We are, as they say, locked and loaded and ready to fire!

Here is what we did in 2022 to get us set for 2023: We:

- Increased our industry membership by 60 organizations, from 313 to 373, and launched four new task groups to meet identified challenges
- Published three major cybersecurity toolkits for incident response and business continuity; model cyber contract language for medical device purchase and management; and coherently communicating medtech vulnerabilities to patients; as well as an outreach and awareness checklist (members only) for our sector to use to advocate our work products
- Conducted two in person All-Hands sessions hosted by Abbott and Kaiser Permanente, attended by more than 400 members in person and virtually
- Concluded the production of an 8-part video clinician training series called "Cybersecurity for the Clinician" to be released in the Spring or early Summer
- Attended a White House Healthcare Cybersecurity Summit with our Executive Committee's CEOs at the invitation of Chris Inglis, the National Cyber Director.

All of these efforts are, of course, *inputs* to the mission but not *outcomes* with performance measures of cyber improvement. This will take time, but it is on our watch.

Here is what we have planned and what we need your help with in 2023:

- **Five Year Plan –** Our number one priority for the year will be to update the Health Care Industry Cybersecurity Task Force recommendations in partnership with HHS. This document will continue to serve as our group's compass and prepare us for the challenges of 2028.
- Helping to get us to that plan, we'll see the following in the first half of 2023:
  - Comments to Senator Warner (D-VA) healthcare cyber policy options paper
  - Joint HSCC/HHS publication of the NIST CSF Implementation Guide
  - Publication of the Managing Legacy Technology cybersecurity guide
  - HICP 2023 (Health Industry Cybersecurity Practices, version 2)
  - JSP2 (Medical Device and Health I.T. Joint Security Plan, version 2)
  - A forward-looking overview of potential cyber risks from the use of artificial intelligence
  - Publication of an Enterprise Incident Response Plan stemming from a cyber attack
  - Release of the free "Cybersecurity for the Clinician" video training series (1 CME credit!)

And that is only the first half of the year. As always, it is all hands on deck. We need your continued commitments to our collective security. It is a challenge not just for each of our enterprises but for the sector as a whole. As National Cyber Director Chris Inglis has challenged us, we must set up the system in such a way that: "*You have to beat all of us to beat one of us*." We can rise to that challenge.

ACTIVITY HIGHLIGHTS DURING THE YEAR

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

2022 ANNUAL REPORT ACTIVITY HIGHLIGHTS

- Increased our industry membership by 60 organizations, from 313 to 373, and launched four new task groups to meet identified challenges
- Published three major cybersecurity toolkits for incident response and business continuity; model cyber contract language for medical device purchase and management; and coherently communicating medtech vulnerabilities to patients; as well as an outreach and awareness checklist (members only) for our sector to use to advocate our work products
- Conducted 250+ virtual task group sessions and two in-person All-Hands sessions hosted by Abbott and Kaiser Permanente, attended by more than 400 members in person and virtually
- Held ~30+ Friday morning SCC/GCC coordinating sessions
- Concluded the production of an 8-part video clinician training series called “Cybersecurity for the Clinician” to be released in the Spring or early Summer
- Elected 3 Executive Committee members representing Medical Technology, Plans & Payers, and At-Large
- Featured our many work products and task group leaders in a dedicated series of 10 podcasts hosted by “Outcomes Rocket”, as well at least 46 press features and 30+ HSCC public appearances
- Attended a White House hosted Healthcare Cybersecurity Summit with our Executive Committee’s CEOS at the invitation of Chris Inglis, the National Cyber Director

MEMBERSHIP

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

CWG Membership by the Numbers

Since January 2022 –60 new industry members, 19% increase

- 373 organizational Industry members, including:
  - 45 Industry association members
  - 44 non-voting Advisor companies
- Government organizations include 10 federal agencies, 2 state agencies, 2 city agencies, and 2 Canadian
- Total representing personnel: 799

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

2022 Subsector Distribution

- Direct Patient Care: **41%**
- Health Information Technology: **10.4%**
- Health Plans and Payers: **5%**
- Mass fatality and Management Services: **0**
- Medical Materials: **9.1%**
- Laboratories, Blood, Pharmaceuticals: **6.8%**
- Public Health: **3.9%**
- Cross-sector: **8.9%**
- Government (Fed, State, County, Local): **4.1%**
- Advisors: **11.5%**

IMPLEMENTATION OF OBJECTIVES

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Cybersecurity Objectives

Continued Operation of CWG Task Groups to implement the

2017 Healthcare Industry Cyber Security Task Force Imperatives:

1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.
2. Increase the security and resilience of medical devices and health IT
3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities
4. Increase healthcare industry readiness through improved cybersecurity awareness and education
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks and exposure
6. Improve information sharing of industry threats, risks, and mitigations

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Task Groups 2022

- **405(d) HEALTH INDUSTRY CYBERSECURITY PRACTICES**
  - Joint Industry/HHS Task Group (from §405(d) of the Cybersecurity Act of 2015) created the HICP (Health Industry Cybersecurity Practices) and is developing supporting collateral material and timely cyber events, marketing and partnerships
- **5-YEAR PLAN**
  - Update the Health Care Industry Task Force (HCIC) recommendations as a five-year plan reflecting emerging threat scenarios in a rapidly evolving healthcare system
- **EMERGING TECHNOLOGY CYBERSECURITY**
  - Assess emerging technologies used in healthcare that may present cybersecurity risks.
- **INCIDENT RESPONSE - BUSINESS CONTINUITY**
  - Develop a healthcare cyber incident response and business continuity plan aligned with existing physical incident response protocols. First publication on emergency management after extended cyber-related outage released April 2022
- **INTERNATIONAL**
  - Hosting webinars on health-cyber international coordination
- **LEGACY MEDTECH SECURITY**
  - Providing guidance for Medical Device manufacturers, services and health delivery organizations about managing cybersecurity
- **MEASUREMENT**
  - Developing methodology for health sector specific cybersecurity performance goals.
- **POLICY**
  - Activates as needed for policy proposals and response
- **MEDTECH CYBERSECURITY JOINT SECURITY PLAN UPDATE (JSP2)**
  - Published Medical Device and Health IT Joint Security Plan (JSP); and benchmarking report. Developing updated JSP2.
- **MEDTECH VULNERABILITY COMMUNICATIONS**
  - Provide guidance to differing stakeholders (MDMs, HDO's, clinicians, patients) on preparing, receiving and acting on medical device vulnerabilities. First publication on patient awareness released April 2022. Second version on HDO preparedness.
- **MODEL CONTRACT LANGUAGE**
  - Monitoring implementation of its published Model Contract for Cybersecurity (MC2)
- **OUTREACH & AWARENESS**
  - Focused, resourced and creative attention on leveraging government, industry associations and other stakeholders to build national health sector awareness and adoption of HSCC cybersecurity resources, NIST CSF, etc.
- **RISK ASSESSMENT**
  - Finalized NIST Cyber Framework Implementation guide; under review by HHS for co-branding
- **SUPPLY CHAIN**
  - Results of pending survey on critical supplier risk management will inform subsequent development of related best practices.
- **WORKFORCE DEVELOPMENT**
  - Preparing series of cybersecurity training videos for clinicians and healthcare students; Reviewing potential production companies for cost and outside funding opportunities

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HSCC CYBERSECURITY WORKING GROUP
Guidance Publications, 2019-2022

SEE: https://healthsectorcouncil.org/hscc-publications

- **December 2022** — Publications Marketing Checklist (*members only*)
- **May 2022** — Operational Continuity-Cyber Incident Checklist
- **April 2022** — MedTech Vulnerability Communications Toolkit
- **March 2022** — Model Contract-Language for Medtech Cybersecurity
- **April 2021** — Health Industry Cybersecurity – Securing Telehealth and Telemedicine
- **September 2020** — Health Industry Cybersecurity Supply Chain Risk Management
- **June 2020** — Health Sector Return-to-Work (R2W) Guidance
- **May 2020** — Health Industry Cybersecurity Tactical Crisis Response
- **May 2020** — Health Industry Cybersecurity Protection of Innovation Capital
- **March 2020** — Health Industry Cybersecurity Information Sharing Best Practices
- **March 2020** — Management Checklist for Teleworking Surge During COVID-19
- **October 2019** — Health Industry Cybersecurity Matrix of Information Sharing Organizations
- **June 2019** — Health Industry Cybersecurity Workforce Guide
- **January 2019** — Medical Device and Health IT Joint Security Plan (JSP)
- **January 2019** — Health Industry Cybersecurity Practices (HICP)

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Addressing the Health Care Industry Cybersecurity Task Force Recommendations

HCIC IMPERATIVES	CWG DELIVERABLES	DATE DELIVERED
1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity	• Operational Continuity-Cyber Incident Checklist • Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) • Health Industry Cybersecurity Practices (HICP)	May 2022 September 2020 December 2018
2. Increase the security and resilience of medical devices and health IT	• Medtech Vulnerability Communications Toolkit • Model Contract Language for Medtech Cybersecurity (MC^2) • Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT) • Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) • Management Checklist for Teleworking Surge During COVID-19 Response • Medical Device and Health I.T. Joint Security Plan (JSP) • Health Industry Cybersecurity Practices (HICP)	April 2022 March 2022 April 2021 September 2020 March 2020 January 2019 December 2018
3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities	• Health Industry Cybersecurity Workforce Development Guide (HIC-Workforce)	June 2019

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Addressing the Health Care Industry Cybersecurity Task Force Recommendations

HCIC IMPERATIVES	CWG DELIVERABLES	DATE DELIVERED
4. Increase healthcare industry readiness through improved cybersecurity awareness and education	• Publications Marketing Checklist (*members only*) • Operational Continuity-Cyber Incident Checklist • Medtech Vulnerability Communications Toolkit • Health Sector Return to Work Guidance • Health Industry Cybersecurity Tactical Crisis Response Guide • HSCC Multimedia Promotions for National Cyber Security Awareness Month (blogs, podcast, webinars) • HICP, HIC Workforce, HIC-MISO, JSP, HIC-SCRiM	December 2022 May 2022 April 2022 June 2020 May 2020 October 2019 2019-2020
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks and exposure	• Health Industry Cybersecurity Intellectual Property Protection Guide	May 2020
6. Improve information sharing of industry threats, risks, and mitigations	• Operational Continuity-Cyber Incident Checklist • Health Sector Return to Work Guidance • Health Industry Cybersecurity Tactical Crisis Response Guide • Health Industry Cybersecurity Information Sharing Best Practices • Health Industry Cybersecurity Matrix of Information	May 2022 June 2020 May 2020 March 2020 September 2019

GOVERNANCE

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

2022 Executive Committee

CHAIR: Erik **Decker, VP - Chief Information Security Officer, Intermountain Healthcare**

VICE CHAIR: Chris Tyberg, Chief Information Security Officer, Abbott

Julian Goldman, MD, Medical Director, Biomedical Engineering, Mass General Brigham

Samantha Jacques, Vice President Corporate Clinical Engineering, McLaren Healthcare

Leslie A. Saxon, MD, Executive Director, USC Center for Body Computing

Janet Scott, Vice President, Business Technology Risk Management and CISO, Organon

Leanne Field, PhD, M.S. Clinical Professor & Founding Director, Public Health Program, The University of Texas at Austin

Denise Anderson, President & CEO, Health Information Sharing & Analysis Center

Michael McNeil, Senior Vice President, Global CISO, McKesson

Marilyn Zigmund Luke, Vice President, America's Health Insurance Plans

Mark Jarrett, Senior Health Advisor, Northwell Health.

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

2022 Government Co-Chairs

Suzanne Schwartz
Director
Office of Strategic Partnerships & Technology Innovation
Center for Devices and Radiological Health
U.S. Food and Drug Administration

Julie Chua
Director, GRC Division
HHS Office of the Chief Information Officer

Bob Bastani
Senior Cyber Security Advisor
Security, Intel, and Information Management Division
Administration for Strategic Preparedness and Response
U.S. Department of Health and Human Services

HEALTH SECTOR COORDINATING COUNCIL
Joint Cybersecurity Working Group

Greg Garcia
Executive Director
Greg.Garcia@HealthSectorCouncil.org

Allison Burke
Member Engagement Project Manager
Allison.Burke@HealthSectorCouncil.org

https://HealthSectorCouncil.org