Health Sector Coordinating Council
Cybersecurity Working Group

HSCC Cybersecurity Working Group

Q2 2023 Progress Report

June 30, 2023

Chairman's Forward

Erik Decker
Industry Co-Chair
HSCC Cybersecurity Working Group

Star-date Q2-2023, Chairman's Log: Let us reflect on the fact that the HSCC Cybersecurity Working Group published fully 6 resources in the second quarter, and we are on track to have published over 5 years at least 27 cybersecurity best practices and recommendations for the health sector by the end of 2023. That is an extraordinary library of content that now must find its way to implementation across the sector by the stakeholders that need it most.

Indeed, the leadership of the HSCC Cybersecurity Working Group recognizes that there is no shortage of resources available to the sector, but moreso a shortage of awareness and intention across the majority of the industry. We are now contemplating new initiatives toward mobilization and action. With the help of our Outreach and Awareness Task Group we are turning our focus to driving adoption of those publications and measuring meaningful progress as an industry.

This pivot is driven not just by our tempo of publications – 3 of which this year are joint HHS/HSCC publications, but by the increasing maturity of the partnership between HSCC, HHS and DHS CISA. We are seeing an encouraging momentum shift at HHS with senior-level support and reorganization focused on a coordinated strategy and engagement with the sector council. This includes substantial investments across HHS ASPR, 405d and HC3, and new senior ASPR leadership in Deputy Assistant Secretary Brian Mazenac. And of course, a shout-out to our steady and energetic government co-chairs of the CWG – Suzanne Schwartz of FDA, Julie Chua in OCIO, and Bob Bastani at ASPR.

And this pivot will be further accelerated as we come to closure over the next few months with our Five-Year Strategic Plan. We have a strong cadre of senior health sector leaders across the subsectors identifying and prioritizing the major healthcare trends that implicate cyber threats and how we should be prepared. We expect to have a final or near-final draft for review at the November All-Hands meeting in Salt Lake City hosted by Intermountain Health.

So, the first two quarters were very busy, but it is now up to us over the next two quarters and into next year for the industry to harvest the fruits of our labors.

##

Q2 2023 MEMBERSHIP

Membership by the Numbers

As of June 30, 2023

- 415 organizational Industry members, including:
  - 47 Industry association members
  - 56 non-voting Advisor companies
- Government organizations include 11 federal agencies, 3 state agencies, 2 city agencies, and 2 Canadian
- Total representing personnel: 922

Subsector Distribution

- Direct Patient Care: **40.2%**
- Health Information Technology: **7.0%**
- Health Plans and Payers: **5.1%**
- Mass fatality and Management Services: **0**
- Medical Materials: **9.2%**
- Laboratories, Blood, Pharmaceuticals: **6.5%**
- Public Health: **6.3%**
- Cross-sector: **8.0%**
- Government (Fed, State, County, Local): **4.3%**
- Advisors: **13.5%**

Q2 2023 ACTIVITIES

Q2 Activities

- Spring All-Hands hosted by Medtronic April 25-26
  - 180 attendees in person (110) and virtual (70), industry and government executives, including HHS Deputy Secretary's office
- Six new publications (3 joint-seal by HHS and HSCC)
- 1 new task group established (Manufacturing Operational Technology)
- 2 successful task groups published their work and disbanded (Legacy Medtech and Workforce)
- 82 Task Group work sessions
- 57member-prospect orientations

Governance

Health Sector Coordinating Council
Cybersecurity Working Group

2023 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

Jonathan Bagnall Head of Cybersecurity, Digital Service & Solutions – Medical Technology, (CE), Fresenius Medical Care

Dr. Adrian Mayers, Vice President, Chief Security Officer, Premera Blue Cross

Sanjeev Sah, Vice President, Chief Security Officer, Centura Health

2023 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

Objectives

Cybersecurity Objectives

CWG Task Groups formed 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

Active Task Groups

Health Sector Coordinating Council
Cybersecurity Working Group

Task Groups 2023

- **405(d) HEALTH INDUSTRY CYBERSECURITY PRACTICES (HICP)**

Ongoing enhancement of 405(d) HICP resources

- **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

- **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 ; second publication on enterprise incident response plan imminent

- **MEASUREMENT**

Developing methodology for health sector specific cybersecurity performance goals.

- **POLICY**

Activates as needed for policy proposals and response

- **MEDTECH CONTRACT LANGUAGE**

Updating Model Contract for Cybersecurity MC2) first published March 2022

- **MEDTECH SECURITY DEVELOPMENT (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 on preparing, receiving and acting on medical device vulnerabilities communications. First publication on patient awareness released April 2022. Second version on HDO preparedness in process.

- **OPERATIONAL TECHNOLOGY MANUFACTURING SECURITY**

Develop best practices guide for securing OT manufacturing networks for healthcare manufacturing subsectors.

- **OUTREACH & AWARENESS**

Develop tools and strategies for enhancing visibility and messaging the imperative of healthcare cybersecurity, HSCC CWG and its resources.

- **PRIVACY-SECURITY COLLABORATION**

Facilitate the interdependence of security and privacy risk to confidentiality, integrity, and availability of entity systems, data, etc., in patient safety and care.

- **PUBLIC HEALTH**

Identify strategies for strengthening the cybersecurity and resilience of SLTT public health agencies with the support of private sector and academic organizations.

- **RISK ASSESSMENT**

Published with HHS the NIST Cyber Framework Implementation guide; follow-on marketing and effort to measure adoption

- **SUPPLY CHAIN / THIRD PARTY CYBERSECURITY**

Results of pending survey on critical supplier risk management will inform subsequent development of related best practices.

Publications and Visibility

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC CYBERSECURITY WORKING GROUP
Guidance Publications, 2019-2023

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

- **July 2023** — Coordinated Healthcare Incident Response Plan
- **April 2023** — Health Industry Cybersecurity Recommendations for Government Policy and Programs
- **April 2023** — Hospital Cyber Resiliency Landscape Analysis (HSCC/HHS Joint)
- **April 2023** — health Industry Considerations for Prioritized Recognized Cybersecurity Practices
- **April 2023** — Health Industry Cybersecurity Practices 2023 (HSCC/HHS Joint)
- **April 2023** — Cybersecurity for the Clinician Video Training Series
- **March 2023** — Health Industry NIST Cybersecurity Framework Implementation Guide (Joint HSCC/HHS)
- **March 2023** — Health Industry Cybersecurity – Managing Legacy Technology Security
- **February 2023** — Health Industry Cybersecurity-Artificial Intelligence Machine Learning
- **May 2022** — Operational Continuity-Cyber Incident Checklist
- **April 2022** — MedTech Vulnerability Communications Toolkit

Health Sector Coordinating Council
Cybersecurity Working Group

HSCC CYBERSECURITY WORKING GROUP
Guidance Publications, 2019-2023

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

- **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 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
- **January 2019** — Health Industry Cybersecurity Practices

Publications on Deck

- (Joint HHS-HSCC) Operational Continuity-Cyber Incident – Q3
- Medical Device and Health I.T. Joint Security Plan v2 (JSP2) – Q3

Health Sector Coordinating Council
Cybersecurity Working Group

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	• HSCC Recommendations for Government Cyber Policy and Programs • NIST CSF Healthcare Implementation Guide • Operational Continuity-Cyber Incident Checklist • Health Industry Cybersecurity Supply Chain Risk Management Guide • Health Industry Cybersecurity Practices (HICP) • Health Industry Cybersecurity Practices (HICP)	April 2023 March 2023 May 2022 September 2020 April 2023 December 2018
2. Increase the security and resilience of medical devices and health IT	• Health Industry Cybersecurity-Managing Legacy Technology Security • Health Industry Cybersecurity-Artificial Intelligence Machine Learning • Medtech Vulnerability Communications Toolkit • Model Contract Language for Medtech Cybersecurity (MC^2) • Health Industry Cybersecurity – Securing Telehealth and Telemedicine • Health Industry Cybersecurity Supply Chain Risk Management Guide) • Management Checklist for Teleworking Surge During COVID-19 Response • Medical Device and Health I.T. Joint Security Plan (JSP) • Health Industry Cybersecurity Practices (HICP) • Health Industry Cybersecurity Practices (HICP)	March 2023 February 2033 April 2022 March 2022 April 2021 September 2020 March 2020 January 2019 April 2023 December 2018
3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities	• Cybersecurity for the Clinician Video Training Series • HSCC Recommendations for Government Cyber Policy and Programs • Health Industry Cybersecurity Workforce Development Guide	March 2023 April 2023 June 2019

Health Sector Coordinating Council
Cybersecurity Working Group

Addressing the Health Care Industry Cybersecurity Task Force Recommendations

HCIC IMPERATIVES	CWG DELIVERABLES	DATE
4. Increase healthcare industry readiness through improved cybersecurity awareness and education	• Cybersecurity for the Clinician Video Training Series • HSCC Recommendations for Government Cyber Policy and Programs • Cybersecurity for the Clinician Video Training Series • NIST CSF Healthcare Implementation Guide • Health Industry Cybersecurity-Managing Legacy Technology Security • Health Industry Cybersecurity-Artificial Intelligence Machine Learning • Operational Continuity-Cyber Incident Checklist • Medtech Vulnerability Communications Toolkit • Health Sector Return to Work Guidance • Cybersecurity Tactical Crisis Response Guide • HICP, HIC Workforce, HIC-MISO, JSP, HIC-SCRiM	April 2023 March 2023 March 2023 March 2023 February 2023 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	• Coordinated Healthcare Incident Response Plan • NIST CSF Healthcare Implementation Guide • Operational Continuity-Cyber Incident Checklist • Health Sector Return to Work Guidance • Cybersecurity Tactical Crisis Response Guide • Cybersecurity Information Sharing Best Practices • Health Industry Cybersecurity Matrix of Information Sharing Organizations	July 2023 March 2023 May 2022 June 2020 May 2020 March 2020 September 2019

2023 Priority:
Five Year Strategic Plan

Health Sector Cybersecurity Five-Year Strategic Plan

Five years after publication of 2017 HHS-Health Care Industry Cybersecurity Task Force report found healthcare cybersecurity to be in "critical condition":

- Identify the HCIC recommendations that the HSCC Cybersecurity Working Group publications have addressed, and which remain a priority for CWG and sector attention;
- Assess how identified healthcare industry trends over the next five years may present continued or emerging cybersecurity challenges to the sector;
- Recommend how the industry and government should prepare for those changes, with a measurable vision of what "Stable Condition" looks like in 2029; and
- Prescribe specific initiatives and tactics that the CWG and government must do as a public-private partnership to motivate and facilitate achievement of those preparedness objectives.

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

Morgan Shuey

Member Support Intern

Morgan.Shuey@HealthSectorCouncil.org