



Healthcare & Public Health
Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

HSCC Cybersecurity Working Group

Q3 2022 Progress Report

October 1, 2022

Chairman's Forward



Erik Decker
Industry Co-Chair
HSCC Cybersecurity
Working Group

We drove more progress and membership growth in the third quarter of 2022. Much of our attention has been focused on the next 5 years of our work plan to strengthen cybersecurity across the healthcare ecosystem. The National Cyber Director, Chris Inglis, challenged the HPH Sector and HHS not to get complacent, even with the 15 publications we have so far prescribed for the sector over the last 5 years to answer the many recommendations of the 2017 Health Care Industry Cybersecurity (HCIC) Task Force. The June meeting at the White House has been a rallying point for our strategic planning process. The outputs of this strategic planning effort will continue to drive the substantive priorities and organizational structure of our Cybersecurity Working Group. We must assess how well the sector is adopting those and other sound cyber practices, and what continuing and emerging challenges are ahead of us. To develop a strategic plan with clear goals and measures of success, our Five-Year Plan Task Group and a supporting cast of executives and subject matter experts will help us determine:

- What has changed in healthcare over the **last** five years?
- What projected trends in healthcare over the **next** 5 years present continuing or emerging cybersecurity implications?
- What operational or public policy challenges or opportunities might these projected healthcare cybersecurity implications present and how should we address them?
- What healthcare cybersecurity goals must we meet in 5 years and what can we do as a collaborative organization, through programs, communications, legislated or regulatory policy incentives, etc., to encourage intended achievement across the sector?

This initiative is underway now. Work continues with HHS leadership to make this a joint initiative, so we will be in full swing in 2023. In the meantime, look to the near future for upcoming publications on HICP 2022, Artificial Intelligence, a Healthcare Implementation Guide for the NIST Cybersecurity Framework, and guidance to HDO's and MDM's for the shared challenge of managing the cybersecurity of legacy medical devices.

Let's stay on it!

Membership

CWG Membership by the Numbers

As of September 30, 2022

- 325 voting organizational members
 - + 7 members over Q2 (2%)
- 41 non-voting Advisor companies
- 45 Industry Association members
- Government organizations include 10 federal agencies, 2 state agencies, 2 city agencies, and 2 Canadian
- Total representing personnel: 788
 - +25 personnel over Q2 (3%)

Membership Subsector Distribution

- Direct Patient Care: **38%**
- Health Information Technology: **9.25%**
- Health Plans and Payers: **4.75%**
- Mass Fatality and Management Services: **0**
- Medical Materials: **10%**
- Laboratories, Blood, Pharmaceuticals: **5.75%**
- Public Health: **4%**
- Cross-sector: **8%**
- Government (Fed, State, County, Local): **10%**
- Advisors: **10.25%**

Initiatives

Task Groups 2022

- **FIVE-YEAR PLAN / HCIC TASK FORCE UPDATE**
 - 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 PLAYBOOK**
 - 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
- **MEASUREMENT**
 - Measurement Task Group with scope TBD: e.g., a) measurement methodology; b) measure sector adoption of cybersecurity frameworks such as NIST CSF, HSCC HICP; c), measuring sector-wide security performance; and/or d) measuring patient impact from a cyber event.
- **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.
- **MEDTECH CYBERSECURITY JOINT SECURITY PLAN UPDATE (JSP2)**
 - First published in January 2019, the Medical Device and Health IT Joint Security Plan will be updated to reflect ongoing developments in medical device security and to integrate subsequent work products soon to be published on legacy device security, model cybersecurity contract language for medical technology, and vulnerability communications standardization
- **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.
- **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
- **EMERGING TECHNOLOGY CYBERSECURITY**
 - Assess emerging technologies used in healthcare may present cybersecurity risks. First publication pending on artificial intelligence. Next assessment on how to protect/encrypt systems, data and identity against malicious use of quantum computing
- **SUPPLY CHAIN**
 - Results of pending survey on critical supplier risk management will inform subsequent development of related best practices.
- **RISK ASSESSMENT**
 - Finalized NIST Cyber Framework Implementation guide; under review by HHS for co-branding
- **INTERNATIONAL**
 - Hosting webinars on health-cyber international coordination
- **WORKFORCE DEVELOPMENT**
 - Preparing series of cybersecurity training videos for clinicians and healthcare students; Reviewing potential production companies for cost and outside funding opportunities
- **POLICY**
 - Activates as needed for policy proposals and response

Publications

HSCC CYBERSECURITY WORKING GROUP

2019-2022 Guidance Publications

SEE: <https://healthsectorcouncil.org/hsc-cc-publications>

- April 2022 [Operational Continuity Cyber Incident \(OCCI\)](#)
- April 2022 [MedTech Vulnerability Communications Toolkit \(MVCT\)](#)
- March 2022 [Model Contract-Language for Medtech Cybersecurity \(MC2\)](#)
- June 2021 [Letter to President Biden on Healthcare Cybersecurity Strategy](#)
- 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 \(HICP\)](#)

Publications on Deck

- White Paper on Artificial Intelligence Applications and Cyber Risks in Healthcare – Q3 2022
- Health Industry NIST Cybersecurity Framework Implementation Guide – Q3 2022
- Legacy Medical Device Cybersecurity Management Guide – Q4 2022

Visibility

Q3 Public Foot-Print:

All Publications

- Total views to-date: **214,315**
- Total downloads to-date: **4813**
(2.25% of total views)

Webpage Views

- *Total Q3 Page Views: 15,090*
15% decrease from Q2 2022
- *Unique Page Views: 13,577*
9% decrease from Q2 2022

Press Mentions

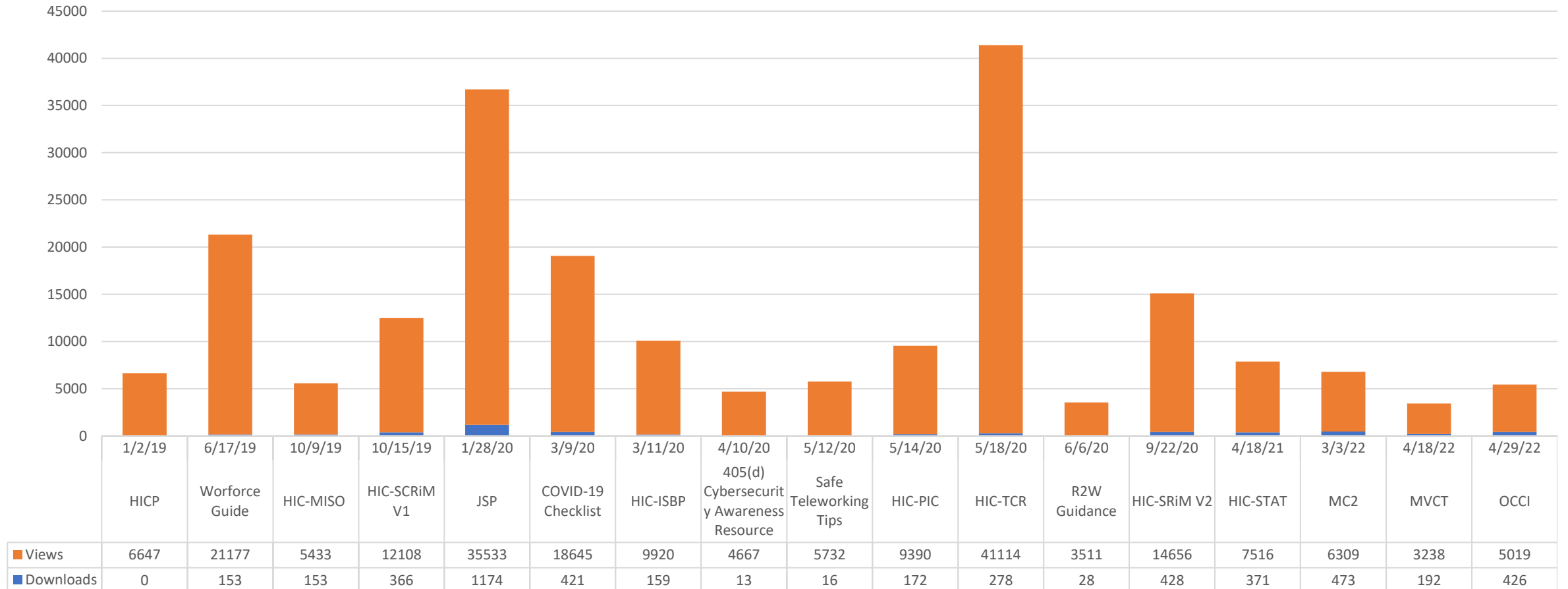
- 7 Press Mentions

Social Media Followers (since account opening October 2018)

- LinkedIn: 638
7% increase from Q2 2022
- Twitter: 195
4% increase from Q2 2022

View and Download Statistics of HSCC Recommendations

*Numbers began tabulating after May 2019 installation of download plugin**



Leadership 2022

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.

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
Office of the Assistant Secretary for Preparedness & Response
U.S. Department of Health and Human Services**

HEALTH SECTOR COORDINATING COUNCIL

Cybersecurity Working Group



Greg Garcia

Executive Director

Greg.Garcia@HealthSectorCouncil.org



Allison Burke

Program Operations Lead

Allison.Burke@HealthSectorCouncil.org