Health Sector Coordinating Council
Cybersecurity Working Group

Health Sector Coordinating Council Cybersecurity Working Group

2023 Annual Report

Erik Decker
Industry Co-Chair
HSCC Cybersecurity Working Group

2023 marked a turning point in the arc of the Health Sector Coordinating Council Working Group, with the progress of our engagement with government, the development of the 5-Year Cybersecurity Strategic Plan and the pivot from content development to mobilization. Below is a list of just some of our successes.

Strategic Initiatives

- Ever strengthening partnership with the government, developing joint resources, providing specifically requested policy and sector assistance advice stemming from the joint Hospital Landscape Analysis and Cyber Performance Goals, and maintaining our regular cadence of Friday leadership meetings to coordinate and plan.
- Near completion of our 5-Year Health Industry Cybersecurity Strategic Plan, to be published February 27.
- Congressional testimony and numerous legislative staff consultations
- Heavily attended All-Hands meetings in Minneapolis and Salt Lake City, and more than 300 working meetings collectively by our 12 task groups

Membership

- An increase to 425 organizations represented by almost 1000 personnel, with an average of 2.5 new-member orientations per week, all from word-of-mouth recommendations and interest

2023 Publications

- CHIRP – Coordinated Healthcare Incident Response Plan (IRBC)
- Government Recommendations (AdHoc Policy)
- Considerations for Recognized Security Practices (AdHoc Policy)
- HICP 2023 (A joint industry/HHS sealed product through 405d)
- Landscape Analysis (A joint industry/HHS sealed product through 405d)
- Cybersecurity for the Clinician Video Training Series (Workforce)
- HSCC-HHS NIST Framework Implementation Guide (Risk Assessment)
- HIC-MaLTS – "Managing Legacy Technology Security" (Medtech Legacy Security)
- HIC-AIM – "Artificial Intelligence-Machine Learning" (Emerging Technology Security)
- PubMarCh – "HSCC Publications Marketing Checklist"(Outreach and Awareness)

In the queue for Q1 2024:
- **Coordinated Privacy-Security Compliance (Privacy-Security TG)**
- **Operational Continuity-Cyber Incident – (An updated joint industry/HHS sealed product through 405d)**
- **Medical Device and Health I.T. Joint Security Plan v2 (JSP2 TG)**
- **MC² – "Model Contract-language for Cybersecurity" (Model Contract TG)**

I assure you as we step into 2024 the momentum will pick up even more, as we mobilize sector adoption and implementation of our many resources and the Strategic Plan. We know that the need for cybersecurity in healthcare is never waning so we will continue to rally behind the mobilizing words of the former National Cyber Director, Chris Inglis. We must set up our healthcare system such that "*You must beat all of us to beat one of us*".

MEMBERSHIP

CWG Membership by the Numbers

Since January 2023 –

- Added 52 industry organizations, to 425 members (*14% increase over 2022*); total includes:
    - 52 Industry association members
    - 58 non-voting Advisor companies
    - 19 Government organizations (11 federal agencies, 4 state agencies, 2 city agencies, and 2 Canadian agencies)
- Total member personnel: 967
- ***600% member organization increase from 60 since 2018***

2023 Subsector Distribution

- Direct Patient Care: **40.9%**

- Health Information Technology: **6.6%**

- Health Plans and Payers: **5.4%**

- Mass fatality and Management Services: **0**

- Medical Materials: **9.7%**

- Laboratories, Blood, Pharmaceuticals: **5.9%**

- Public Health: **5.4%**

- Cross-sector: **8%**

- Government (Fed, State, County, Local): **4.5%**

- Advisors: **13.6%**

IMPLEMENTATION OF OBJECTIVES

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

Health Sector Coordinating Council
Cybersecurity Working Group

- **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

![Health Sector Coordinating Council Cybersecurity Working Group]

HSCC Publications, 2019-2023

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

2023

- *Updated* Health Industry Cybersecurity Information Sharing Best Practices
- *Updated* Health Industry Cybersecurity Matrix of Information Sharing Organizations
- Coordinated Healthcare Incident Response Plan
- Recommended Government Policy & Programs
- Hospital Cyber Landscape Analysis (Joint HSCC/HHS)
- Prioritized Recognized Cybersecurity Practices
- Health Industry Cybersecurity Practices 2023 (Joint)
- Cybersecurity for Clinician Video Training Series
- Health Industry NIST CSF Implementation Guide (Joint)
- Managing Legacy Technology Security
- Artificial Intelligence Machine Learning

2022

- Operational Continuity-Cyber Incident Checklist
- MedTech Vulnerability Communications Toolkit
- Model Contract-Language for Medtech Cybersecurity
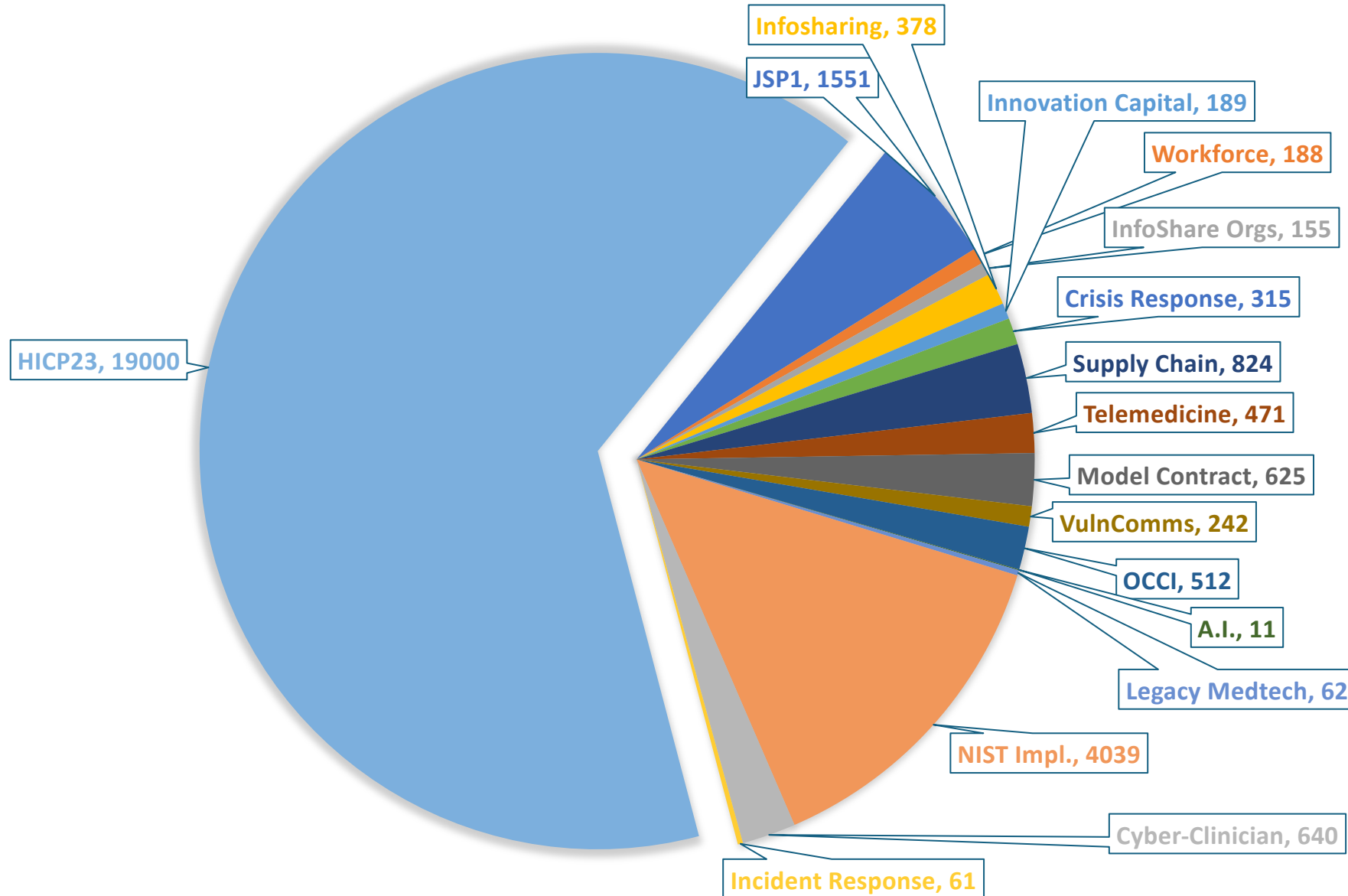
2021

- Securing Telehealth and Telemedicine

2020

- Supply Chain Risk Management
- Health Sector Return-to-Work Guidance
- Tactical Crisis Response
- Protection of Innovation Capital
- Information Sharing Best Practices
- Checklist for Teleworking Surge During COVID-19

2019

- Matrix of Information Sharing Organizations
- Workforce Guide
- Medical Device and Health IT Joint Security Plan
- Health Industry Cybersecurity Practices (Joint HSCC/HHS)

Downloads of HSCC Cybersecurity Best Practices

Pie chart: Downloads of HSCC Cybersecurity Best Practices

- HICP23, 19000
- JSP1, 1551
- Infosharing, 378
- Innovation Capital, 189
- Workforce, 188
- InfoShare Orgs, 155
- Crisis Response, 315
- Supply Chain, 824
- Telemedicine, 471
- Model Contract, 625
- VulnComms, 242
- OCCI, 512
- A.I., 11
- Legacy Medtech, 62
- NIST Impl., 4039
- Cyber-Clinician, 640
- Incident Response, 61

Health Sector Coordinating Council
Cybersecurity Working Group

All Publications

- Total views to-date: **278,000+**

- Total downloads to-date: **95,000+** (5.27% of total views)

- Video Training: **30,000+ views**

Webpage Views

- Total Page Views: 91,248
  64% increase from 2021

- Unique Page Views: 43,245
  17% increase from 2021

Public Recognition

- 57 Press Mentions and Features

Social Media Followers (since account opening October 2018)

- LinkedIn: 1,425
  73% increase from 2022
- X (formerly Twitter): 282
  33% increase from 2022

GOVERNANCE

Health Sector Coordinating Council
Cybersecurity Working Group

Cybersecurity Working Group
New 2024 Executive Committee

CHAIR: Erik Decker, VP, CISO, Intermountain Healthcare
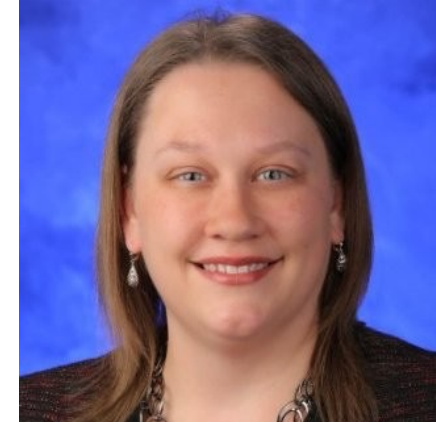
VICE CHAIR: Chris Tyberg, CISO, Abbott

AT-LARGE: Sanjeev Sah, Vice President, CSO, CommonSpirit Healthcare

CROSS SECTOR: Bobby Rao, Global CISO, Fresenius Medical Care

DIRECT PATIENT CARE: Julian Goldman, MD, Medical Director, Biomedical Engineering Mass General Brigham

DIRECT PATIENT CARE: Samantha Jacques, VP Corporate Clinical Engineering, McLaren Healthcare

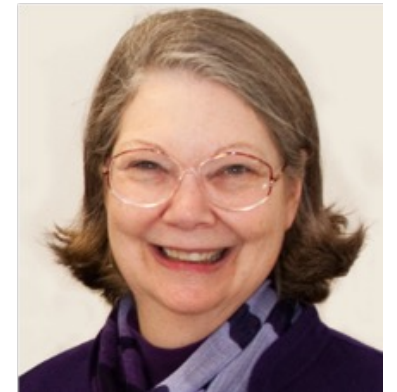**HEALTH IT:** Jennifer Stoll, Executive Vice President External Affairs, OCHIN, Inc.

MEDICAL TECHNOLOGY: Chris Reed, VP Product Security, Medtronic

PLANS-PAYER: Adrian M. Mayers, Dr.BA, VP & CISO, Premera Blue Cross

PHARMA-LAB-BLOOD: Janet Scott, VP, Business Technology Risk Management and CISO, Organon

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

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

HEALTH SECTOR COORDINATING COUNCIL
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