Healthcare & Public Health
Sector Coordinating Council

PUBLIC PRIVATE PARTNERSHIP

CYBERSECURITY WORKING GROUP

Industry Annual Report

2018

Message From the Chair

Terry Rice

- *Chief Information Security Officer (CISO), Merck & Co.*
- *HSCC CWG Executive Committee Chair*

Collective Intent

In the end, we will be measured not by the number of white papers, letters, guidelines, or best practices that we produce, but by how we collectively implement them toward measurable improvements to our security posture as an interconnected, interdependent industry. That depends on all of you to work within your organizations to adopt HSCC recommendations and to be HSCC ambassadors to your peer organizations. While working to promote and ensure information security for a global pharmaceutical company, I know that in cyber security we are never truly done. Our adversaries are more adaptive and cunning than ever before. But I believe we are writing prescriptions for better cyber health in this sector, and hopefully, in the not-too-distant future, we'll be able to report that we are in "stable condition."

I am pleased to bring you the HSCC Cybersecurity Working Group 2018 annual report! I think you will agree that 2018 was an eventful year for improving the healthcare industry's cybersecurity preparedness. In 2017, the landmark report by the Health Care Industry Cyber Security Task Force diagnosed the industry's cyber health to be in "critical condition." While this grim news was neither surprising nor a disputed conclusion, it exemplified our entire group's justification for existing and operating with excellency.

To meet the ever-growing demand for cybersecurity coordination in our sector, the Cybersecurity Working Group of the Healthcare and Public Health Sector Coordinating Council (HSCC) began an aggressive recruitment campaign to organize around addressing the report's many recommendations early in 2018. We grew from 60 organizations a year ago, primarily representing the direct patient care subsector, to 200 organizations today, representing direct patient care, pharmaceuticals, medical technology and health I.T., plans and payers, and public health.

We established several new task groups to deliver on specific Task Force recommendations, recruited volunteers to lead and contribute to the task groups, and set objectives and schedules for their work. Backed by a newly-revised charter with clear governance and process rules, the energy and momentum behind those efforts yielded two major toolkits for hospital cybersecurity best practices and medical technology security; policy letters to HHS calling for cybersecurity exemptions to Stark Law and anti-kickback rules; and several works in progress that will see conclusion in 2019.

But with all we have taken on and accomplished, it is clear to us how much more we have left to do. This is why I am particularly proud of and humbled by our participating member's cooperation and unwavering support. Representing all of our member subsectors, the 9 member Executive Committee, elected by the general membership, will strengthen our thought leadership and resource support, guide us through our strategic planning and program oversight throughout 2019, and serve as primary sector liaisons to our government partners in HHS, FDA, DHS and others.

This partnership with government is essential. When industry works together with government on projects of mutual concern we operate as the Joint Cybersecurity Working Group. This means we strive to produce resources and recommendations that both government and industry can support and implement. This 2018 industry annual report will highlight many of the private sector and joint accomplishments of the Cybersecurity Working Group.

While the daily onslaught of cyber attacks on our industry will continue unabated and challenge our readiness, I feel more confident going into 2019 with your unyielding vigilance coupled with a structure and process that galvanizes our collective efforts with industry-developed tools, collaborative spirit, and constructive government-industry partnership.

Thank you to all who have served this industry in 2018. The dedication of all the task group leaders and the many volunteers who have contributed is inspiring. But there is no time for rest. For those who have not yet joined task groups, or have participated sporadically, please don't sit on the sidelines. We need you. Let us accelerate our work in 2019. Please contact me, any of our Executive Committee members, or our Executive Director Greg Garcia to get more involved.

-Terry Rice

VP IT Risk Management & Security
Chief Information Security Officer
Merck & Co.

Operational Goals for 2019

We will be working toward a number of measurable objectives for the Cybersecurity Working Group:

- Strengthened "culture of leadership" in the CWG, in which more members step up to take the reins and contribute thought leadership and resources
- Expanded cross-sector representation of the largest subsector stakeholders
- Increased membership and participation of senior executive decision-makers
- Task Group work products distributed and endorsed by relevant national industry associations and adopted by market movers; and
- Mechanisms for measuring adoption, implementation and results across relevant sub-sectors

From the Government Coordinating Council Chairs

Overview of Healthcare and Public Health Sector Public-Private Partnership Efforts to Improve Sector Cybersecurity in 2018

Cybersecurity is a critical area of focus and an important component in maintaining U.S. health security and resilience. The healthcare industry remains among the highest in cyber data breaches and is, increasingly, a cyberattack target. That is why in 2018, private industry and the federal government collaborated on unprecedented steps to improve the output of actionable cybersecurity-related products and activities. Through the outstanding contributions of the public-private Joint Cybersecurity Working Group and other partners, the healthcare and public health sector developed mitigation strategies and products to address the sector's cybersecurity risks and improve the industry's preparedness to respond to cybersecurity threats.

Such collaboration is fundamental to the U.S. Department of Health and Human Services' (HHS) charge to protecting our nation's healthcare and public health sector's critical infrastructure against hazards such as terrorism, infectious disease outbreaks, natural disasters, and cyber attacks. As noted by the Department of Homeland Security, "Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between the public and private sectors is essential to increasing resilience of the nation's healthcare and public health critical infrastructure."

To help protect our healthcare and public health critical infrastructure, HHS facilitates and collaborates with a public-private partnership between the private sector and government coordinating councils. We view this collaboration as essential to successful delivery of care.

With the momentum already built, 2019 stands to be even more impactful in raising awareness of cybersecurity threats and best practices for the healthcare industry. Thank you for your hard work in 2018 and for your continued commitment to the security of the nation's health system.

Sincerely,

Suzanne B Schwartz, MD, MBA

Associate Director for Science & Strategic Partnerships

Center for Devices & Radiological Health
US Food & Drug Administration (FDA)
US Department of Health and Human Services (HHS)

Bob Bastani, CISSP, CISM, CRISC

Supervisory IT Specialist, Healthcare and Public Health Sector Cyber Security Leader

Critical Infrastructure Protection
Office of the Assistant Secretary for Preparedness and Response (ASPR)
US Department of Health and Human Services (HHS)

HOW WE'VE GROWN
By the Numbers

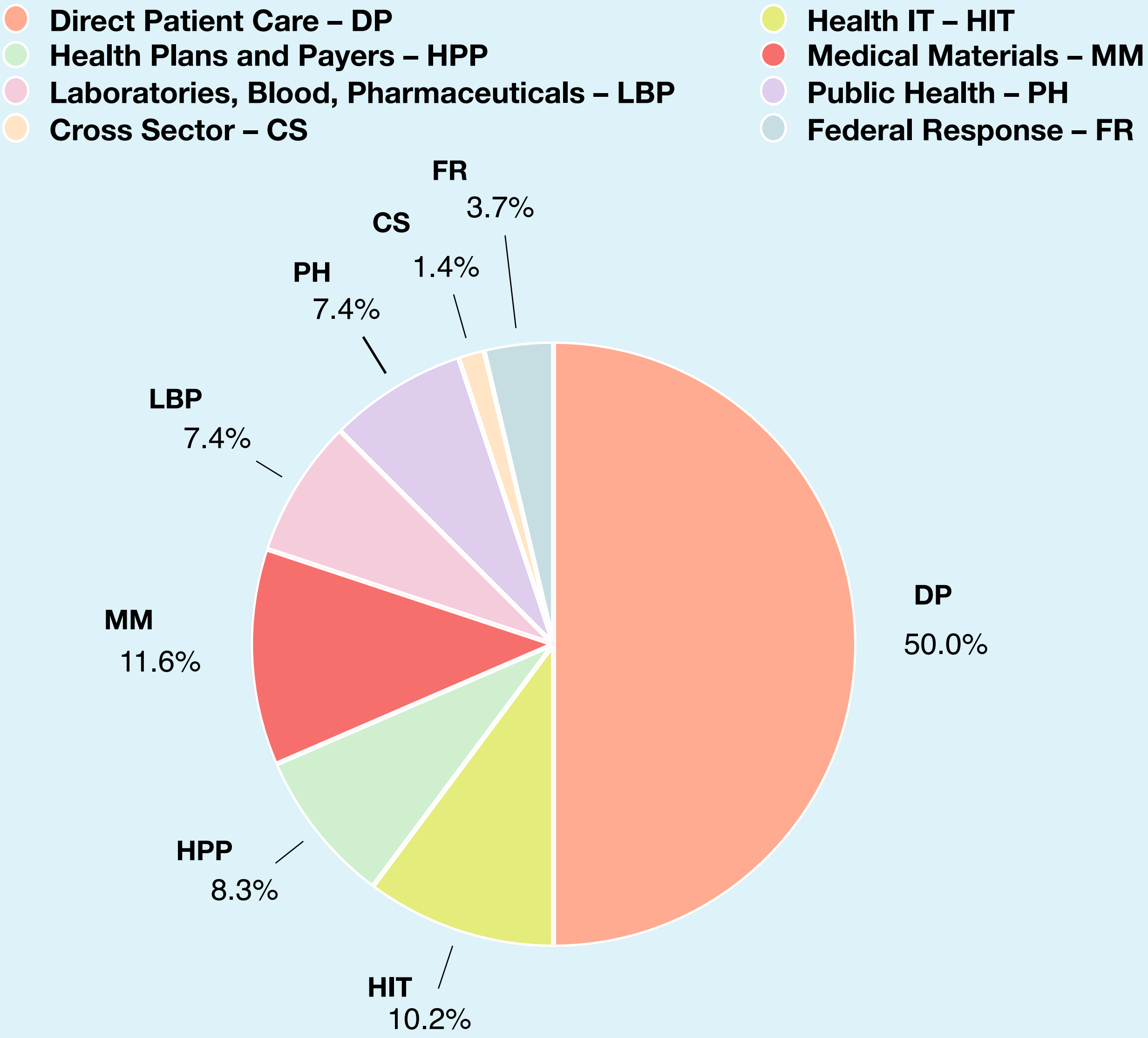
Membership

Since February 2018:

- Increase **from 60 to 200** voting organizational members
- **17** non-voting Advisors
- Industry association members increase **from 5 to 36**
- Private sector personnel members increase by 272, **from 58 up to 330**
- Government personnel at **56**, federally representing 7 agencies and 51 personnel, and one member each from 3 state agencies; 1 county and 1 city

Subsector Distribution

- Direct Patient Care: **108 (50%)**
- Health I.T.: **22 (10.2%)**
- Health Plans and Payers: **18 (8.3%)**
- Medical Materials: **25 (11.6%)**
- Laboratories, Blood, Pharmaceuticals: **16 (7.4%)**
- Public Health: **16 (7.4%)**
- Cross-sector: **3 (1.4%)**
- Federal Response (Government): **8 (3.7%)**



WHAT WE'VE DONE
A Progress Assessment

The Compass for Our Journey

In June 2017, a Congressionally-created, HHS-appointed blue-ribbon panel of experts making up the Health Care Industry Cybersecurity (HCIC) Task Force released a report that proposed recommendations for improving the cybersecurity posture of the sector. The HCIC recommendations were a call to action that formed the basis of the Cybersecurity Working Group agenda for 2018, and our establishment of 13 task groups dedicated to driving the implementation of those recommendations. The report organized its output into 6 Imperatives (below), which cascaded into 27 Recommendations and within them, 105 Action Items. The 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

These Imperatives include elements that HCIC designated to be "owned" by industry alone, government alone, or jointly as a public-private partnership. Clearly, the footprints of our industry members and the partnership are found throughout all 6 of the HCIC Imperatives, and our highlights below and in the Task Group wrap-ups illustrate how. In time, we can assure our Congressional colleagues and the members of the HCIC – many of whom are active in the CWG - that the health sector is accountable for our cybersecurity improvement and will continue to address these challenges with structured and collaborative energy.

Joint Cybersecurity Working Group Highlights

Two major deliverables for 2018 represent a great success of the healthcare private public partnership. Two task groups co-chaired by industry and government produced jointly developed cybersecurity resources for our health provider and medical technology stakeholders. These are:

- Publication of "Health Industry Cybersecurity Practices (HICP)", previously known as the "Section 405(d)" Initiative
- Publication of the Medical Technology and Health I.T. Joint Security Plan

The reception to these important toolkits has been welcomed and wide spread. In the coming months the partnership will be driving awareness, adoption, and implementation as broadly as possible across the stakeholder community.

In addition, our collaboration routines and special engagements between industry and government partners cultivated strong working relationships and mutual goals. The following are several examples of the JCWG in action.

- 35 weekly sync-up and planning calls since March between government and industry leadership (CWG Co-Chairs, Executive Director, ASPR, FDA, OIC)
- 90 Task Group working calls
- In-office planning meetings with:
  - HHS ASPR Bob Kadlec
  - HHS Deputy Secretary Chief of Staff
  - DHS CS&C A/S Jeanette Manfra
  - HHS ASPR D/AS Ed Gabriel
- "DHS 101" webinar on DHS available cybersecurity services
- DHS National Risk Management Center Discussion on Healthcare Technology Risk Management Assessment

Cybersecurity Working Group (Industry) Highlights

In some cases the Health Sector Coordinating Council deals with issues that are specific to industry and do not require government involvement or where government involvement would not be appropriate. This includes industry recommendations about public policy and activities around our internal operational tools and decision making process. For example, our policy task group was very active this year responding to requests for comment by HHS on various issues:

- October 26 advisory letter to OIG on EHR reporting and anti-kickback cyber exception
- October 17 advisory letter on cyber transparency in EHR Reporting Program
- August 24 advisory letter from industry SCC to CMS on Stark Law exception

The Cybersecurity Working Group developed clear structures for governance and communications, in the form of:

- Charter revision with clear governance and membership criteria (industry SCC charter only)
- SCC industry election of first 9-member Executive Committee
- Website launched - www.HealthSectorCouncil.org

SAVE THE DATES – 2019 ALL-HANDS JCWG MEETINGS

APRIL 2-4, 2019	San Diego, CA	Hosted by Becton Dickinson
OCTOBER, Date TBD	Austin, TX	Hosted by University of Texas, Austin

Some of our most fruitful and interactive work occurs during our semi-annual “All-Hands” in-person meetings. Our 2018 meetings on June 29 in Washington, DC and October 9 in Nashville were attended by more than 100 member-representatives at each event, with a networking reception, task group report-outs, feedback refinement and ratification, guest speakers, and, in October, a tabletop exercise that tested our response capabilities against a blended incident of a pandemic flu coupled with a ransomware cyber attack.

For more information, see the meeting reports for June 29 and October 9. If your infosec policy prohibits Google share, please request copies from Business Operations Coordinator, Omar Tisza at Omar.Tisza@HealthSectorCouncil.org

New Leadership will Drive the Industry Agenda for the HSCC CWG

In December, the industry members of the Cybersecurity Working Group elected our first executive committee*. The EC will serve the HSCC CWG by:

1) Electing the CWG Chair and Vice Chair;
2) Developing proposals to the general membership for the Council’s strategic and tactical objectives;
3) Adjudicating concerns or disagreements within the membership; and
4) Serving as liaisons to our government partners and the public as appropriate.

Please welcome them!

* The CWG Charter provides for staggered Executive Committee member terms according to vote counts in the general election. Given the Charter’s stipulation for a 9-member EC, the 3 candidates with the most votes are to serve 3 years, the middle three – 2 years, and the lower 3 a 1-year term. Based on its high numerical representation in the membership, the Direct Patient Care Subsector was assigned 2 EC seats and the other subsectors represented on the CWG – Health IT; Plans & Payers; Medical Materials; Pharma, Labs and Blood; Public Health; and Cross Sector - each occupies 1 seat. At this time, there is no Mass Fatality Services Subsector representation in the CWG membership. Because no other subsector could be proportionally justified to occupy two seats, we added to the top 8 an “At-Large” position, which goes to the individual who receives the most votes after the top 8, regardless of subsector representation.

HSCC CYBERSECURITY WORKING GROUP 2019 EXECUTIVE COMMITTEE

Chair & Vice Chair

NAME	AFFILIATION	ROLE	SUBSECTOR	END OF TERM
CHAIR: TERRY RICE	MERCK & CO.	CISO	PHARMA, LABS & BLOOD	December 2020
VICE CHAIR: THERESA MEADOWS	COOK CHILDREN'S HEALTH CARE SYSTEM	SVP & CISO	DIRECT PATIENT CARE	December 2020

DIRECT PATIENT CARE

NAME	AFFILIATION	ROLE	END OF TERM
ERIK DECKER	UNIVERSITY OF CHICAGO MEDICAL CENTER	CHIEF INFORMATION SECURITY OFFICER	December 2021
THERESA MEADOWS	COOK CHILDREN’S HEALTHCARE SYSTEM	SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER	December 2020

HEALTH INFORMATION TECHNOLOGY

NAME	AFFILIATION	ROLE	END OF TERM
TOM LEARY	HEALTHCARE INFORMATION & MANAGEMENT SYSTEMS SOCIETY (HIMSS)	VICE PRESIDENT, GOVERNMENT RELATIONS	December 2020

HEALTH PLANS AND PAYERS

NAME	AFFILIATION	ROLE	END OF TERM
SEAN MURPHY	PREMERA	CHIEF INFORMATION SECURITY OFFICER	December 2019

MEDICAL MATERIALS

NAME	AFFILIATION	ROLE	END OF TERM
ASHLEY WOYAK	BAXTER	BUSINESS INFORMATION SECURITY OFFICER	December 2019

LABS, BLOOD, AND PHARMACEUTICALS

NAME	AFFILIATION	ROLE	END OF TERM
GREG BARNES	AMGEN	CHIEF INFORMATION SECURITY OFFICER	December 2021

PUBLIC HEALTH

NAME	AFFILIATION	ROLE	END OF TERM
SRI BHARADWAJ	UC IRVINE HEALTH	CHIEF INFORMATION SECURITY OFFICER	December 2020

CROSS SECTOR

NAME	AFFILIATION	ROLE	END OF TERM
DENISE ANDERSON	HEALTH ISAC	PRESIDENT	December 2021

AT-LARGE

NAME	AFFILIATION	ROLE	END OF TERM
MARILYN ZIGMUND LUKE	AMERICA’S HEALTH INSURANCE PLANS	VICE PRESIDENT	December 2019

The HSCC Cybersecurity Working Group Charter

Pathway to Sector Leadership

In October of 2018, the CWG industry membership approved revisions to our charter to clarify how we will govern ourselves as a volunteer collaborative organization. An ad hoc task group* was established to answer fundamental governance questions:

1) Eligibility criteria for membership;
2) Leadership election process and term lengths;
3) Approval process for HSCC documents and recommendations; and
4) Dispute resolution procedures.

It is important to point out that this is a new charter; we did not attempt in its drafting to anticipate and address every governance detail or potential aberration, but to set a general direction that we can later refine after some experience. Any voting member in good standing may petition the leadership for a charter revision, which will be considered and decided upon at the discretion of the leadership.

<u>* Ad Hoc Charter Task Group</u>
Erik Decker, Chief Information Security Officer, UCMC
Laura Hoffman, Assistant Director, Federal Affairs, AMA
Lee Kim, Director, Privacy & Security HIMSS North America
Erin Richardson, Vice President & Assistant General Counsel, FAH
Todd Spangler, Director, Public Policy & Government Relations, BD

Here are some Charter highlights:

Voting Membership Eligibility–"Regular Member"
- A "Covered entity" or "Business associate" under HIPAA
- Company whose technology is regulated by FDA
- Trade association representing any of the above
- One vote per organization

Leadership Selection
- Executive Committee (slate of 7-9 cross-subsector) elected by majority vote of full CWG membership – candidates from TG leads and general membership
- Chair and Vice Chair elected by majority vote of Executive Committee

Leadership Terms
- Executive Committee: 3 years staggered
- Chair & Vice Chair: 2 years each, once renewable for 1 year, staggered.

Non-Voting Advisors
- Vendors, consultants or other organizations not meeting the above criteria are not eligible voting members but may participate at the invitation of leadership

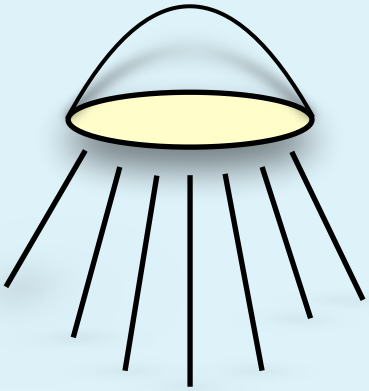
Governance
- TG Leaders determine appropriate document approval procedures for their TG
- CWG Leaders decide whether TG document is to be approved by vote or consensus; if by vote, majority rules
- Approved CWG deliverable presumed as full parent SCC recommendation, as SCC charter defers to working group governance
- Dissension: Members in minority against CWG-approved deliverable may petition CWG leadership for qualifying language in approved deliverable; resolution subject to Leadership discretion
- Charter in effect until leadership approves motion for amendment

Major Deliverables for 2018

Two major work products regarding medical technology security and hospital cyber best practices were concluded in 2018, with back to back release at the end of 2018 and beginning of 2019. These complementary guidelines meet two key Imperatives identified in the 2017 Task Force recommendations and are now set for an aggressive adoption and implementation drive over the course of 2019.

- The publication "**Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients**" is the culmination of 2 years' work of the "Section 405(d)" Task Group, co-chaired by Erik Decker, CISO of University of Chicago Medical Center, and Julie Chua from the HHS Office of the CIO. The result – details below - is a scalable toolkit of the top ten cybersecurity best practices that hospital systems should deploy.

- The **Medical Technology and Health I.T. Joint Security Plan**, a set of product security best practices for medical device and HIT companies, was developed over the course of 18 months by stakeholders in the Medtech, Health IT and Direct Patient care Subsectors, and co-chaired by Rob Suarez, BD's Director of Product Security, and Kevin McDonald, Mayo Clinic's Director of Clinical Information Security.



Spotlight on...

Health Industry Cybersecurity Practices

The Health Sector Coordinating Council (HSCC), in partnership with the U.S. Department of Health and Human Services, released the "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients" publication. The four-volume publication seeks to raise awareness for executives, health care practitioners, providers, and health delivery organizations, such as hospitals. It is applicable to health organizations of all types and sizes across the industry.

This industry-led effort was in response to a mandate of the Cybersecurity Act of 2015 Section 405(d), to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the healthcare industry. The publication marks the culmination of a two-year effort that brought together more than 150 cybersecurity and healthcare experts from industry and the government, and co-chaired by Erik Decker, CISO of University of Chicago Medical Center, and Julie Chua from the HHS Office of the CIO. The consensus-based document was developed and released under the auspices of the HSCC Joint Cybersecurity Working Group, a public-private partnership to enhance healthcare and public health cyber and critical infrastructure security and resilience.

The publication consists of four volumes:

1. The Main document of the publication explores the five most relevant and current threats to the industry and recommends 10 Cybersecurity Practices to help mitigate these threats.

2. Technical Volume 1 discusses these 10 cybersecurity practices for small healthcare organizations. It is intended for IT and IT security professionals.

3. Technical Volume 2 discusses these 10 cybersecurity practices for medium and large healthcare organizations. It is intended for IT and IT security professionals

4. Resources and Templates provides additional resources and materials that organizations can leverage to develop policies and procedures as well as assess their own cybersecurity posture, through a Cybersecurity Practices Assessment Toolkit.

For more information on this effort and to download a copy of the publication, please visit the HSCC CWG website or the 405(d) website at www.phe.gov/405d.

MedTech & HIT Joint Security Plan

The "Medical Technology and Health I.T. Joint Security Plan (JSP)", a set of product security best practices for medical device and HIT companies, was developed over the course of 18 months by stakeholders in the Medtech, Health IT and Direct Patient Care subsectors. The initiative was co-chaired by Rob Suarez, BD's Director of Product Security, Kevin McDonald, Mayo Clinic's Director of Clinical Information Security, and Aftin Ross, FDA. The JSP is a voluntary framework and integrated security plan for medical devices and health IT which seeks to address challenges associated with legacy products, secure development lifecycle practices, security and vulnerability communications to stakeholders, incident response coordination, and cybersecurity maturity assessment for continuous improvement. It is important to note that this plan is not a standard. Rather it establishes the basis for transparent and public commitment to adopting quality cybersecurity practices and achieving cybersecurity maturity across medical device and healthcare IT vendors as well as healthcare providers.

Working with HHS on Better Cybersecurity

Since the start of the 2018 summer, the Department of Health and Human Services (HHS) has queried the healthcare industry about how its regulatory structure can be improved to ensure better patient care, including how policy can encourage and incentivize better cybersecurity as an element of patient safety. The Health Sector Coordinating Council – the conduit through which these efforts can be brought to attention- has raised its hand to respond to these HHS requests, most recently in three significant policy letters on varied topics that include the Anti-kickback statute and Electronic Health Record (EHR) Reporting Program.

The CWG Policy Task Group (TG-2) – led by Theresa Meadows, CIO of Cook Children's Health System, Mari Savickis, VP of CHiME, and Carl Anderson, General Counsel for HITRUST – took the lead in developing a sector response to these RFI's. The resulting letters to HHS are summarized and linked below.

- On August 24, 2018 we responded to the Centers for Medicare and Medicaid Services (CMS) RFI regarding the Physician Self-Referral Law. Based on the recommendations of Health Care Industry Cybersecurity Industry (HCIC) Task Force Report, we recommended CMS create a Stark exception that allows for the donation or subsidizing of cybersecurity technology and services to help improve the cybersecurity posture of providers, better protect patient information, improve patient safety, and help fortify our sector from growing global threats.

- On October 17, 2018 we responded to an RFI on the Electronic Health Record (EHR) Reporting Program established under Section 4002 of the 21st Century Cures Act. In it, we urged ONC to focus on more transparency around electronic health record (EHR) vendors' cybersecurity posture and recommended a set of items to better inform a purchaser of the vendors security posture.

- On October 26, 2018 we responded to an HHS RFI about the OIG Anti-kickback statute. We recommended CMS create a Stark exception that allows for the donation or subsidizing of cybersecurity technology and services to help improve the cybersecurity posture of providers, better protect patient information, improve patient safety, and help fortify our sector from growing global threats.

Recognizing our HHS Partners' Support and Leadership

It bears repeating that much of our progress toward strengthening the security and resiliency of the sector cannot be achieved without the partnership of key personnel with the Department of Health and Human Services and the Food and Drug Administration. In 2018, we saw increasing levels of HHS engagement with the Sector Coordinating Council, as the Council itself became a more organized and robust partner. Starting with our June 29 All-Hands meeting hosted in Washington DC at HHS Headquarters, Deputy Secretary Eric Hargan addressed the 100+ attendees by video after he was unexpectedly called away from attending in person. See his warmly-received message here.

In addition, CWG leadership met during the year with other senior government partners to get acquainted and discuss mutual cybersecurity priorities and initiatives. We met with Department of Homeland Security Assistant Secretary for Cyber Security Jeanette Manfra (who spoke at our February organizing meeting and the June 29 all-hands); HHS Assistant Secretary for Preparedness and Response (ASPR) Bob Kadlec; and Associate Deputy Secretary Will Brady.

ASPR Kadlec and ADS Brady were particularly engaged in how we can manage the partnership on specific issues.

For example, some points ASPR Kadlec raised with us included:

- Put additional emphasis on developing our regional presence and support
- Integrate cyber and physical capabilities into our disaster response approach. We took him up on that with our blended cyber/pandemic exercise in Nashville in October;
- Review how the 2015 Cybersecurity Act information sharing provisions are helping or hindering our ability to share information and respond to incidents in the health sector; and
- Provide advice to HHS about where the regulatory structure, including HIPAA, could be impeding our cyber security preparedness and response. Indeed, HHS's string of RFI's with variations on that question and our three written responses show movement toward evolved thinking about the nexus between healthcare, cybersecurity and patient safety.

Will Brady, in turn, focused our attention on some of the technology issues facing the sector, what role the government can play in assessing the benefits and helping manage the risks, and how to balance the complementary tasks of promotion and protection. Two areas in which he asked for sector advice were the "Internet of Medical Things" and artificial/automated intelligence (AI). We highlighted that our Telehealth and Future Gazing Task Groups were focused on those and other technology issues, and that DHS as well wants to work with the health sector on just such a technology risk assessment.

Lastly, Brady expressed what is now the common lament about lack of sufficient workforce capacity for cybersecurity, either at the cyber specialist level or in proper training for the front line clinical workforce. We were happy to share with him progress in our Workforce Task Group 3 and told him we will keep him updated on its results.

Finally, specific recognition goes to the key personnel in HHS who served throughout the year as our principal "Sector Specific Agency" liaisons, and with whom we maintained weekly coordination and planning calls throughout the year. That kind of routine is essential for cultivating personal relationships and ensuring either that we are aligned on our mutual objectives or understand why we are not and what alternatives are available. So, a big 2018 thank you! goes to:

ASPR
Steve Curren
Laura Wolf
Bob Bastani
Nickol Todd
Alysia Durant

CIO
Julie Chua

FDA
Suzanne Schwartz
Aftin Ross
Seth Carmody

Task Group Wrap up

The turning of a new year comes with an appreciation of the year that passed. As our anticipation is focused on the polished outputs of the CWG–the JSP and 405(d) efforts–we have generated substantial progress on many other lesser publicized, but nevertheless crucial fronts. This year saw a high influx of members and heightened interest in collaboration from key stakeholders throughout the healthcare industry and government. This is reflected in the developments and ongoing maturity of the Task Groups (TGs) within the CWG. With the sustained participation of our engaged membership, the celebration of our collective efforts, and the support of the government and industry partnerships that invigorate our work, the following is a 2018 wrap up of Task Group (TG) progress and objectives:

- **Risk Assessment TG-1A** continues to update version 1 of the Healthcare Sector Cybersecurity Framework Implementation Guide to version 2, including incorporation of changes stemming from the NIST Cybersecurity Framework version 1.1 release.

- **Medtech Security TG-1B**. With publication of the Joint Security Plan toolkit, the task now turns to driving awareness and adoption, taking feedback from implementation, and refining and updating the practices for a version 2.

- **Intellectual Property (IP) Data Protection TG-1C** focuses primarily on a stand-alone IP protection guidance document that can be scaled to large and small institutions. The goal is to establish best practices across the breadth of industries for protecting sensitive information, to include manufacturing formulations, trade secrets and intellectual property.

- **Supply Chain & Third Party Cyber Risk Management TG-1D** is developing a field-deployable toolkit enabling any size healthcare facility to understand cyber risk and structure a supply chain security and procurement process that demands appropriate security features when acquiring connected clinical products, software and services.

- **Telemedicine TG-1E** scans the landscape of cybersecurity threats in the use of telemedicine. This TG is working towards a whitepaper that outlines telemedicine cybersecurity concerns, policies and procedures to address them and barriers to implementation.

- **Hospital Best Practices TG-1F**. With publication of the Health Industry Cybersecurity Practices resource, the task now turns to driving awareness and adoption, taking feedback from implementation, and refining and updating the practices for a version 2.

- **Policy & Regulation TG-2** will continue to coordinate the CWG response to government requests for comment on proposed regulatory actions and legislation, and work with HHS and other agencies to consider streamlining a cyber regulatory structure that facilitates, rather than complicates, cybersecurity risk management in the health sector.

- **Workforce Development TG-3** published a blog on the HSCC website during October's National Cybersecurity Awareness Month, discussing tips for building a pipeline of qualified cyber professionals in healthcare. TG 3 also is working on a significant effort to introduce fundamental cyber security curriculum into medical, nursing and pharmacy schools to better prepare our frontline clinicians for the responsibilities they have to basic cyber hygiene in the clinical environment, and the linkage between cyber security and patient safety. This group is partnering with AMA and stakeholders in the academic community to drive this initiative.

- **Cross-Sector Engagement TG-4** seeks to build relationships and understand the cross-sector engagement and how this is conducted on a daily basis and during incidents. The goal is to gain an initial understanding of how other sectors operate and explain how the HPH Sector operates through a series of webinars. In 2018, the Communications Sector and the Electricity Subsector were hosted in HSCC CWG webinars to continue developing cross sector engagement.

- **Information Sharing TG-5** is working to develop guidance and awareness products to encourage the engagement, expansion, and usability of threat information sharing.

- **Future Gazing TG-6** catalogues future technologies that will either improve healthcare cybersecurity or present new risks. We are currently developing a whitepaper report that will brief all audiences in how these new technologies will affect their cybersecurity strategic planning.

- **Marketing TG-7** is another standing committee that manages outreach and communications for the CWG. We have created an HSCC-CWG website with information and resources, published blog posts, conducted webinars, and disseminated information through social media.

- **Exercises TG-8** seeks to develop tabletop exercises to test potential best practices and communications across sector. Establish a template for continuous improvement in the exercise cycle.

It is easy to forget that the arduous work of our membership is voluntary. Individuals willingly and gladly take on an added responsibility–on top of their highly demanding positions. Out on the horizon, 2019 will build on the successes of the TGs above and continue to be a catalyst for lasting change in this critical sector. **If you are not currently active in a task group, we urge you to consider getting involved on behalf of your organization. Please contact any of the co-chairs above or Greg Garcia, Executive Director, at** greg.garcia@HealthSectorCouncil.org.

Pop Quiz - In Case You're Asked:

"What is the Health Sector Coordinating Council Cyber Working Group?"

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of industry associations and their members addressing the most pressing security and resiliency challenges to the healthcare sector. It has been a platform for collaboration among healthcare industry leaders and the government under the National Infrastructure Protection Plan for more than a decade. Specifically, your organization is part of an interdependent ecosystem that is facing increasingly sophisticated operational and cybersecurity threats, and vulnerabilities that can cascade across the value chain of the healthcare sector, ultimately affecting patient safety, security and privacy. It is our collective responsibility to deliver industry-wide policy and operational solutions to this shared challenge. Many organizations are stepping up to this responsibility by joining the HSCC and its Cybersecurity Working Group (CWG). All healthcare sector stakeholders who have expertise and resources to contribute are encouraged to do the same.

About the HSCC – The responsibility of all Sector Coordinating Councils (SCC) is captured in three iterations of a Presidential Executive Order dating to 1998, the most recent update being Presidential Policy Directive 21 in 2013, which calls on 16 critical industry sectors to self-organize – in partnership with the government - around the mission to protect essential assets and services from existential threats, both physical/operational and cyber. Every critical industry sector, including healthcare, financial services, electricity, emergency services, communications, water, transportation, and others, has been stepping up to this mission. We do this with two essential functions: the day-to-day operational protection, threat analysis and incident response of the Health Information Sharing and Analysis Center (H-ISAC) and related information sharing and analysis organizations, and the longer-term strategic and policy-oriented mission of the HSCC. Under the executive order, the HSCC is recognized as the private industry partner to the Department of Health and Human Services, which looks to us – in a non-regulatory, partnership posture – to help develop policy and operational improvements that enable our sector to better protect against and respond to threats, vulnerabilities and incidents. For more information, see our website at https://healthsectorcouncil.org/health-sector-council-cyber-working-group-introduction-2/ or go to our share drive for a powerpoint primer, or request it from greg.garcia@HealthSectorCouncil.org.

Healthcare Sector Coordinating Council

Joint Cybersecurity Working Group – Organizational Members

as of January 10, 2019

PRIVATE SECTOR – VOTING MEMBERS

1. Abbott Laboratories
2. AbbVie Pharmaceutical
3. Acurity
4. Advanced Medical Technology Association
5. Advocate Aurora Health
6. Aetna

Type to enter text

7. Aetna Global Security
8. Albany Medical Center
9. Alberta Health Services
10. Alexion Pharmaceuticals
11. Allergan plc
12. Alliance for Quality Medical Device Servicing
13. American Health Information Management Association
14. American Hospital Association
15. American Medical Association
16. American Medical Informatics Association
17. America's Health Insurance Plans
18. Amgen Inc.
19. Anthem
20. Arkansas Children's
21. Ascension (Health System)
22. Association for Executives in Healthcare Information Security
23. Association for the Advancement of Medical Instrumentation
24. Association of Public Health Laboratories
25. Aurora Health Care
26. Avera Health
27. B. Braun Medical
28. Baxter Healthcare Corporation
29. Baylor Scott & White Health
30. BD (Becton, Dickinson, and Company)
31. Beebe Healthcare
32. Biologics Modular
33. Blanchard Valley Health System
34. Blue Cross & Blue Shield of Rhode Island
35. Blue Cross Blue Shield Association (BCBSA)
36. Boston Scientific Corporation
37. Burgess Group
38. Cambia Health Solutions
39. Cardinal Health
40. CareCentrix
41. CareTech Solutions
42. Cedars-Sinai Health System
43. Centene Corporation
44. Cerner Corporation
45. CGH Medical Center/FBI Infragard Sector Chief
46. Children's Healthcare of Atlanta
47. Children's National Health System
48. College of Healthcare Information Management Executives (CHIME)
49. Christiana Care Health System
50. CHRISTUS Health
51. ClearDATA Networks
52. Clearwater Compliance
53. Clinica Sierra Vista
54. Coalfire
55. Coastal Bend Regional Advisory Council
56. Community Health IT
57. Community Hospital
58. Connected Health Initiative
59. Cook Children's Health Care System
60. Cooperative Exchange
61. Corvesta, Inc.
62. Covenant Health
63. CVS Health
64. Cyber Tygr, LLC
65. CynergisTek, Inc.
66. Diabetes Technology Society
67. Dignity Health
68. Edwards
69. Electronic Health Records Association
70. Electronic Healthcare Network
71. Eli Lilly & Company
72. Encompass Health
73. Ensemble Health Partners
74. Excela Health
75. Federation of American Hospitals
76. Flowing Springs Home Care
77. GE Healthcare
78. Geisinger
79. GlaxoSmithKline
80. Greater New York Hospital Association
81. Gundersen Health System
82. HCA Healthcare
83. Health Information Sharing and Analysis Center
84. Health Management Systems, Inc.
85. Health Promotion Consultants
86. Health Tek
87. Healthcare Administrative Technology Association
88. Healthcare Association of New York State
89. Healthcare Ready
90. HealthTrust
91. Hebrew Senior Life
92. Hennepin Healthcare
93. Henry County Hospital
94. Highlands Regional Medical Center
95. HIMSS
96. HITRUST

97. HMS
98. Holy Redeemer Health System
99. Horizon Blue Cross Blue Shield of New Jersey
100. Hospital Sisters Health System
101. Humana Inc.
102. Indiana University Health
103. Ingine
104. Intermountain Healthcare
105. International Association of Certified ISAOs
106. Jackson Health System
107. Johns Hopkins All Children's Hospital
108. Johns Hopkins University Applied Physics Laboratory
109. Johnson & Johnson
110. Juniper Health Inc.
111. Kaiser Permanente
112. Kuakini Health System
113. Madonna Rehabilitation Hospital
114. Marshfield Clinic Health System
115. Mary Lanning Healthcare
116. Masonicare
117. Massachusetts General Hospital/ Harvard Medical School
118. Mayo Clinic Health System
119. Medical Device Innovation Safety and Security Consortium
120. Medical Device Manufacturers Association
121. Medical Imaging Technology Association
122. Medical University of South Carolina
123. Medtronic
124. Memorial Sloan-Kettering Cancer Center
125. Merck
126. Meridian Behavioral Health Center
127. Methodist Le Bonheur Healthcare
128. Midland Memorial Hospital
129. Moffitt Cancer Center
130. Monmouth Ocean Hospital Service Corporation
131. Munroe Regional Medical Center
132. Natick VNA/Century Health Systems
133. National Committee for Quality Assurance
134. Natividad Medical Center
135. Nemours Children's Health System
136. New Jersey Hospital Association
137. New York University Langone Medical Center
138. NorthBay Healthcare
139. Northwell Health
140. Northwestern Medicine North Region
141. Novartis
142. Ohio Health
143. OurHealth
144. PAHCOM
145. Partners Healthcare / Mass. Gen. Hosp.
146. Pfizer
147. Pomerene Hospital
148. Premera
149. Premier Healthcare Alliance
150. ProMedica
151. Providence St. Joseph Health
152. Qualcomm Life
153. Quality Insights
154. Quest Diagnostics
155. Rady Children's Hospital
156. ResMed Corporation
157. Ridgecrest Regional Hospital
158. Royal Philips
159. Rush University Medical Center
160. Saint Luke's Health System
161. San Mateo County Health
162. Scottsdale Institute
163. Sensato
164. Sentara Healthcare
165. Sharp Healthcare
166. Shire
167. Shriner's Hospitals For Children
168. Siemens Healthineers
169. Southern Illinois Healthcare
170. Southwest Mississippi Regional Medical Center
171. Spectrum Health
172. St Lawrence Health System
173. Synergy Healthcare Services, LLC
174. Texas Biomedical Research Institute
175. Texas Children's Hospital
176. Texas Tech University Health Sciences Center El Paso
177. The Center for Medical Interoperability
178. The University of Texas, MD Anderson Cancer Center
179. Thermo Fisher Scientific
180. TIDI Products
181. Tift Regional Medical Center
182. Trinity Health
183. Tufts Health Plan
184. UAB Dept of Medicine
185. University of California Irvine Health
186. University of California Los Angeles Medical Center
187. University of Chicago Medicine
188. University of Colorado Health
189. University of Florida Health and Shands Hospital
190. University of Rochester Medical Center
191. University of Illinois (Chicago) Hospital
192. University of South Dakota Nursing School
193. University of Texas at Austin, School of Public Health
194. University of Texas Medical Branch Galveston
195. University of Washington Medicine
196. Varian Medical Systems
197. Village Care of New York
198. Vizient
199. Wake Forest Baptist Health
200. WellStar Health
201. WestCare Foundation
202. Workgroup for Electronic Data Interchange

PRIVATE SECTOR NON-VOTING ADVISORS

1. Assura, Inc.
2. Booz Allen Hamilton
3. Comply Assistant
4. Condition Zebra
5. Crowe LLP
6. Cynergistek
7. InfoArch Consulting,Inc
8. KPMG
9. KWMD LLC
10. Medical Device Innovation Consortium
11. MITRE
12. Muntz and Company LLC
13. Nova Leah
14. Pepper Hamilton LLP
15. PWC
16. Sublett Consulting, LLC
17. Symantec
18. The Fulcrum Group, Inc.
19. West Monroe Partners
20. UL LLC
21. ZingBox
22. Frechette

GOVERNMENT

1. Colorado Office of IT, Office of Information Security, CISO
2. District of Columbia Department of Health Care Finance
3. Health Canada
4. National Association of County and City Health Officials
5. State of New Jersey Homeland Security
6. The City of New York Department of Health and Mental Hygiene
7. U.S. Air Force Surgeon General
8. U.S. Department of Commerce National Institute of Standards & Technology
9. U.S. Department of Defense
10. U.S. Department of Health and Human Services
11. U.S. Department of Homeland Security
12. U.S. Department of Interior
13. U.S. Department of State
14. U.S. Food and Drug Administration