Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

RE: **Comments on CISA Cybersecurity Performance Goals - Common Baseline v2**

SUBMITTED BY: Health Sector Coordinating Council Cybersecurity Working Group

DATE: August 4, 2022

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the Critical Infrastructure Partnership Advisory Council framework to partner with and advise the government on the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver health services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is a standing working group of the HSCC, composed of more than 360 industry organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Summary Recommendations

The HSCC CWG thanks CISA for the opportunity to comment on its "*Cybersecurity Performance Goals - Common Baseline v2*".

The Common Baseline development process as outlined in its FAQ document and referenced in the next section of this letter envisions the next phase to include aligning the Cybersecurity Performance Goals (CPGs) to specific critical infrastructures. The CWG agrees with that process and accordingly we reinforce our expectation that CISA will:

- Leverage its cybersecurity thought leadership when promulgating the CPGs to the health sector by deferring explicitly to the cybersecurity control frameworks and performance measures developed by the HSCC/HHS partnership. One of these frameworks is statutorily recognized, and all are public-domain and targeted specifically at healthcare organizations. Our concern is that promoting both CISA-generalized CPG's and health-sector specific resources to our sector stakeholders is likely to cause confusion among under-resourced health entities seeking coherent assistance; and
- Coordinate with the HSCC and HHS, as envisioned in the Common Baseline FAQ, toward developing and surveying health sector cybersecurity performance measures that ensure alignment between our guidance and the CPG's as much as appropriate to minimize mixed messaging to our healthcare stakeholders.

Comments on CISA's CPG Process for the Benefit of the Health Sector

In pursuing our assessment, measurement, and planning objectives described above, the HSCC CWG is ready to work with HHS and CISA in the sector-specific CPG process outlined in the Common Baseline FAQ:

- "Once the Common Baseline (cross-sector Performance Goals) are complete, CISA will work with each Sector Risk Management Agency (SRMA) to begin development of sector-specific goals by:
    - Identifying any additional cybersecurity practices, not already included in the Common Baseline, needed to ensure the safe and reliable operation of sector-specific critical infrastructure.
    - Providing examples for evidence of implementation specific to infrastructure and entities in that sector; and
    - Mapping any existing requirements (e.g., regulations or security directives) to the Common Baseline and sector-specific objectives and/or evidence of implementation so stakeholders can see how their existing compliance practices fulfill certain objectives.

- CISA and SRMAs will use an iterative process to develop the sector-specific goals. CISA will engage several sectors at a time during a set of "sprints" with the aim to complete all sector-specific goals by end of CY2024."

We note, however, the Common Baseline Goals "Quick Guide" recommends that baseline measures should follow these specific principles: a) Binary (yes/no) measurements are preferred; and b) Scaled measurements, such as "the number of devices with MFA enabled", should be avoided.

Without addressing the specific controls or measures presented in CISA's Baseline Performance Goals, the HSCC CWG makes two observations. First, the use of "binary" measures potentially misses the complexities of multilayered enterprise architectures and policies, requiring an adjustable measurement process for anomalies and qualifications to yes/no answers. In our view, appropriate application of metrics can include binary when aggregated at a national level but less so at an enterprise level if meaningful performance metrics is the intent. In some sectors, specific products and systems may not meet the baseline performance goals due to the nature of their design, implementation, and complexities of regulations in the sector. Second, determining "scaled measurements" with common definitions can be difficult on a national level; but using a baseline performance measurement with numerators and denominators that are meaningful to an enterprise and their sector can inform both enterprise and sectoral performance at the national level.

By our read of the Common Baseline Controls List, many of the identified "measures" that accompany given controls appear to be controls themselves rather than measures. As the HSCC CWG begins a performance assessment process for the health sector, we will approach our measurement objectives using a combination of the following methods, in order of their implementation:

1. Structural measurement – measuring whether a security structure or application is in place. An example is whether there is a person responsible for cybersecurity.
2. Process measures - such as the application of the NIST Framework; i.e., whether there are processes in place to theoretically protect the entity.
3. Outcome measures - measuring whether the processes are working; e.g., the introduction of MFA has reduced the incidence of successful business email compromise by 80% over the previous year. Outcome measures are critical since just doing something may not result in protection. The field of healthcare is full of processes with little to no impact on patient outcomes or safety but continue to be followed. This is not just confined to cybersecurity.
4. Multilayered measurements – engaging the various components of a complex system, such as healthcare, requires different distilled measures weighed complementarily for accurate depiction. Our sector includes large health systems, pharmaceutical companies, and medical device manufacturers with well-resourced management and expertise to implement rigorous cyber risk and controls, and measure their effectiveness. Most healthcare, however, is delivered in the ambulatory setting, often with small practices, or by small hospitals and skilled nursing facilities functioning in the cybersecurity world at a much different level of expertise. A sector's measurement program must account for differences so "all boats rise."

The most essential principle of these measurements is they are done for the purpose of process improvement. This is what the HSCC will be addressing in the coming months, and we look forward to partnering with CISA and HHS as we move forward together.

Policy Guidance for Healthcare Cybersecurity Frameworks

We appreciate CISA's formidable mission to develop voluntary cybersecurity guidelines and performance measures applicable across all critical infrastructure sectors. While we recommend CPGs be tied to prioritized threats and risks, we support the broad objectives of the CPGs, described as:

- "A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
- "A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity
- "A combination of best practices for IT and OT owners, including a prioritized set of security controls.
- "Unique from other control frameworks as they consider not only the practices that address risk to individual entities, but also the aggregate risk to the nation."

The health sector and our government partners focus on these objectives in capturing the uniquely complex ecosystem of healthcare IT and OT infrastructure - including, but not limited to, direct patient care; medical materials and technology; pharmaceuticals, labs and blood; plans and payers; health IT; and public health.

As a policy platform, the **Cybersecurity Information Sharing Act of 2015 (CISA 2015)** launched a public-private cybersecurity program aligned notionally to the CPG principles, but specifically for the health sector, involving assessment, recommendations, and operationalization for healthcare cybersecurity. In response, the HSCC CWG has spearheaded a broad-based, growing strategy of partnering with government stakeholders, implementing Congressional intent and developing preparedness measures against the dangerous, multiplying and evolving cyber threats to the sector and the nation's patients.

Health Care Industry Cybersecurity Task Force

In **§405(c) of CISA 2015**, Congress directed HHS to establish a Health Care Industry Cybersecurity (HCIC) Task Force, which resulted in the appointment of two dozen healthcare and cybersecurity experts from industry and government. The one-year process of the HCIC Task Force culminated in a June 2017 report that diagnosed healthcare's cybersecurity to be in "critical condition," and prescribed six major imperatives and 105 action items for improving cybersecurity management across the healthcare industry and government. These recommendations primarily constitute the HSCC CWG program plan, to date resulting in the publication of 15 cybersecurity best sound practices and guidance documents developed by executive practitioners across the healthcare ecosystem, tailored to the specific needs of the health sector – *by the sector, for the sector*.

In April of 2022, CEOs of the organizations represented on the HSCC CWG Executive Committee met with White House National Cyber Director Chris Inglis to discuss in part how the sector can be assessed against the HCIC recommendations five years after its publication. The discussion concluded with a CWG commitment to review the HCIC report and assess:

1. How we have so far addressed the HCIC recommendations;
2. What remains to be done;
3. What new dynamics/emerging threats are at play; and
4. How this assessment informs an HCIC update with targeted goals and outcomes five years from now.

This process will reference our many resources as guidance and performance measures for our progress. We envision this initiative to be a joint effort between the sector, HHS, as well as CISA.

HHS 405(d) Program

A cornerstone joint publication by HHS and HSCC – known as the Health Industry Cybersecurity Practices (HICP) –

resulted from statutory mandate in **§405(d) of CISA 2015**, which anticipated the assessment of the 405(c) task force and directed the HHS Secretary to "establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, ***a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes to***:

A. "Serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;
B. "Support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;
C. "Are updated on a regular basis and applicable to a range of health care organizations; and
D. "Are consistent with—
    i. The standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act;
    ii. The security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996;
    iii. The provisions of the Health Information Technology for Economic and Clinical Health Act."

The 405(d) provision was implemented as a joint **405(d) Task Group** of the HSCC Cybersecurity Working Group and HHS, composed of more than 250 volunteer clinicians and health system leaders, healthcare cybersecurity executives, and policy experts from across the HSCC membership, HHS, NIST and DHS. The resulting HICP, two years in the making, provides scalable, voluntary cybersecurity principles and practices for use by providers of any size and ability. Key to the HICP's approach for scalable cybersecurity practices is a toolkit structure guiding stakeholders through ten functional cybersecurity practices aligned with the NIST Cybersecurity Framework, with ***suggested performance measures following each of the ten "Cybersecurity Practices."*** See the suggested metrics at the end of each cybersecurity practices chapter in Volume 2 of the HICP: https://405d.hhs.gov/Documents/tech-vol2-508.pdf.

Referencing our observation above about the need to tie CPG's to threats and risks, the 405(d) initiative enumerated prevailing threats against the national healthcare system, built 10 practices to mitigate those threats, and tailored specific, differentiated assistance for implementing those practices among small, medium and large sized organizations. We did this knowing no one-size-fits-all model works for our complex critical infrastructure.

The 405(d) task group continues to develop new cybersecurity resources, tools, and products to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the sector's evolving cybersecurity threats.

With almost 4 years of promoting and supplementing sectoral implementation of HICP practices, the HSCC is now: 1) developing a HICP version 2 in alignment with the Congressional mandate to keep the resource up to date, and 2) beginning to apply HICP performance measures to inform enterprise improvement and investment in cyber readiness. This process envisions partnering with HHS and CISA to aggregate performance data nationally, characterizing whether and how the sector improves its cybersecurity posture.

HICP Codified as Breach Mitigation Incentive

Statutory recognition of HICP's relevance to health sector cybersecurity and the public-private partnership which developed it is found in PL 116-321 (2021), directing HHS, when enforcing HIPAA following a data breach, to consider as a condition for mitigating fines or audit whether a breached entity has implemented "recognized security practices," to include the NIST Cybersecurity Framework and "approaches promulgated under §405(d)" of CISA 2015. This new policy endorses the implementation of cybersecurity tools and measurable performance goals developed jointly by industry and government as an incentive for the healthcare community to invest against cyber-attacks, associated patient impacts, and regulatory penalties.

HHS Risk Assessment Tool

Finally, the HHS Office of the National Coordinator and Office for Civil Rights recently updated the Security Risk Assessment (SRA) Tool. The SRA Tool is a software application designed to assist small to mid-sized organizations in meeting their responsibility to protect electronic protected health information (ePHI). The tool uses a step-by-step approach for helping organizations assess policies and procedures, track hardware assets and vendor relationships, and self-rate threats and vulnerabilities. This year the SRA tool includes new references to HICP, helping users understand threats posed to their organization and providing guidance on mitigation strategies. See: Security Risk Assessment Tool | HealthIT.gov.

Measuring Adoption and Effectiveness

As the above policy and organizational foundations indicate, the health sector's cybersecurity imperatives are being met head-on by a maturing public-private partnership supported by Congressional intent and regulatory objectives. This by no means suggests the sector's cybersecurity preparedness is where it needs to be, but we anticipate that a concerted industry-government campaign to drive awareness of tools available to the sector will accelerate necessary adoption and increase performance. Along with preparing an HCIC update and measuring enterprise and sector maturity against the HICP framework, over the next two years the HSCC will assess our progress against the suite of current and upcoming CWG resources that address many of the HCIC recommendations. A sampling of our available publications includes:

- **April 2022 –** Operational Continuity Cyber Incident (OCCI): OCCI is a checklist intended to provide a flexible template for operational staff and executive management to respond to and recover from an extended enterprise outage due to a serious cyber-attack. Its suggested operational structures and tasks can be modified or refined according to an organization's size, resources, complexity and capabilities.
- **April 2022 –** Medtech Vulnerability Communications Toolkit (MVCT): MVCT is a toolkit written to provide specific tools to medical device manufacturers and software developers for creating cybersecurity vulnerability communications related to their products or services. This toolkit focuses on vulnerability communications directed to non-security professionals, including clinicians, patients, users and other readers not familiar with cybersecurity and connected technologies. It is intended to help medical device manufacturers formulate and communicate vulnerability disclosures in ways all affected audiences, including nontechnical stakeholders, can understand.
- **March 2022 –** Model Contract-Language for Medtech Cybersecurity (MC^2): MC^2 is a reference for appropriate cybersecurity terms and conditions in contracts between Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) regarding the security, compliance, management, operation, services, and security of medical devices, solutions, and connections in a clinical environment. The FAQ's in this document supplement the MC^2.
- **April 2021 –** Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT): HIC-STAT identifies cyber risks and best practices associated with the use of telehealth and telemedicine, and summarizes the policy and regulatory underpinnings for telehealth/telemedicine cyber risk management. It is targeted for senior executives in healthcare and IT, telehealth service and product companies, and regulators.
- **September 2020 –** Health Industry Cybersecurity Supply Chain Risk Management Guide – Version 2 (HIC-SCRiM-v2): The HIC-SCRiM is a toolkit for small to mid-sized healthcare institutions to better ensure the security of the products and services they procure through an enterprise supply chain cybersecurity risk management program.

- **May 2020 –** Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC): The HIC-PIC is a white paper with guidance for how healthcare organizations can protect trade secrets, medical research and other innovation capital from cyber theft.
- **March 2020 –** Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP): The HIC-ISBP is a best practice guide for how healthcare organizations can set up and manage cyber threat information sharing programs for their enterprise.
- **June 2019 –** Health Industry Cybersecurity Workforce Guide: The HIC Workforce Guide is a tool kit for recruiting and retaining skilled cybersecurity workforce in the healthcare sector.
- **January 2019 –** Health Industry Cybersecurity Practices (HICP): The HICP is a four-volume publication seeking to raise awareness on managing cyberthreats and safeguarding patient safety for executives, health care practitioners, providers, and health delivery organizations, such as hospitals.
- **January 2019 –** Medical Device and Health IT Joint Security Plan (JSP): The JSP is a total product lifecycle reference guide for developing, deploying and supporting cyber secure technology solutions in the health care environment.

In the pipeline for publication later this year are guidance documents addressing: 1) the cybersecurity management of aging medical devices reaching “legacy” status, which constitute some of the higher risk medical technologies deployed in a clinical environment; 2) a health sector implementation guide for NIST CSF informative references; 3) a healthcare-specific playbook for cyber incident response and business continuity; 4) an update to the Medical Device Joint Security Plan; and 5) the update to HICP.

Concluding Recommendation

As the CISA public comment process for Baseline Performance Goals transitions to the next phase when CISA turns to sector-specific consultations, and joint work efforts result in CISA’s promulgation of the critical infrastructure performance goals, we recommend the agency support unity of messaging and publicly recognize and advocate to the health sector, in coordination with HHS and HSCC, the cybersecurity practices promulgated under the health sector public-private partnership. This partnership process has leveraged a policy and process platform for collaborative development of evolving cybersecurity controls, measures and accountability for health sector cybersecurity. Unity of effort in support of this platform will ensure its success.

Thank you for the opportunity to comment.

Sincerely,

Greg Garcia
Executive Director
Health Sector Coordinating Council Cybersecurity Working Group