Statement from the College of Healthcare Information Management Executives

Senate Committee on Health, Education, Labor and Pensions
Executive Session: S. 1199, S. 1173, and S.1895
124 Dirksen Senate Office Building
June 26, 2019

The College of Healthcare Information Management Executives (CHIME) is pleased to offer a statement in support of S. 1895 §502(b) as included in the Manager's Amendment. As senior health information technology leaders, we welcome the opportunity to share our perspectives on how technology impacts healthcare costs and if harnessed correctly, will both improve outcomes and increase efficiency within the healthcare system.

CHIME is a professional organization that represents more than 2,900 Chief Information Officers (CIOs) and other senior healthcare IT leaders. CHIME enables its members and business partners to collaborate, exchange ideas, develop professionally and advocate for the effective use of information management to improve the health and care in the communities they serve. CHIME members are responsible for the selection and implementation of clinical and business systems that are facilitating healthcare transformation through technology. Our members represent some of the earliest and most prolific adopters of electronic health records (EHRs) and other health IT resources for clinicians and patients. Our mission is, "To advance and serve healthcare leaders and the industry improving health and care globally through the utilization of knowledge and technology."

Section 502 - Recognition of security practices

The Committee's direction to the Office for Civil Rights (OCR) to acknowledge the attempts of healthcare providers to follow good cybersecurity practices is commendable. Healthcare organizations are constantly under attack from bad actors determined to disrupt their operations or unlawfully release patient data that are well-resourced, often much better than our health systems. Organizations acting in good faith and applying best practices still face the probability of cyberattacks and thus breaches. Therefore, recognizing an organization's effort to improve their cyber posture is important and can be more effective that unduly punitive approaches. CHIME has long supported the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the Health Care Industry Cybersecurity Practices (HICP), and the ongoing efforts of the 405(d) work group established by the Cybersecurity Act of 2015.

CHIME encourages the Committee to ensure that proprietary solutions are not endorsed or included in OCR's assessment of cybersecurity programs over publicly available practices like those outlined by the NIST CSF or HICP. The overall intent of the language in §502(b) is to allow providers, which may have varying degrees of financial means, to have a level playing field in showing that they are attempting to follow good cybersecurity practices that don't have a cost barrier to entry. As soon as there is the potential for OCR to include

proprietary or private-sector generated frameworks, certifications, etc., health systems run the risk that those with less resources will be unable to receive the same consideration yet may be making a good-faith effort in establishing a robust cybersecurity program. Allowing the inclusion of proprietary resources could further emergence of a digital divide between well-resourced organizations and those lesser-resourced organizations at a time when they are already struggling. We don't want to see a situation where the weak get weaker. Promoting the NIST CSF is a better approach, as it pulls everyone forward.

Congress has been widely hailed for its leadership in recognizing the contribution NIST is making to address the cybersecurity threats across all segments of critical infrastructure. Just last year, the 115th Congress affirmed its support for NIST's continued work in leading the development of solutions to the threats posed by cybersecurity in the reauthorization of the NIST Act P.L. 115-236. Section 2(c)(15) specifically endorses the inclusive, public-private partnership that supports the NIST CSF by mandating the agency to continue "on an ongoing bases, facilitate and support the development of a voluntary, consensus based, industry-led set of standards, guidelines, best practices, methodologies, procedures and processes to cost-effectively reduce cyber risks to critical infrastructure."

The mandate of Section 2(c)(15) aligns with the consensus recommendations of the Healthcare Industry Cybersecurity Task Force. The Task Force, mandated by the Cybersecurity Information Sharing Act of 2015, provided a report to Congress and established its first "Imperative" to "[d]efine and streamline leadership, governance, and expectations for health care industry cybersecurity." Recommendation 1.2 under that Imperative is "[e]stablish a consistent, consensus-based health care-specific Cybersecurity Framework."

This panel of leading experts drawn from across the public and private sectors of the healthcare industry went on to recommend that: "[t]he framework should build upon the minimum standard of security required by the NIST Cybersecurity Framework and the HIPAA Security Rule to promote a single lexicon for health care sector as well as standards, guidelines, and best practices. The complex environment requires certain basic standards that all stakeholders must meet and guidelines that allow flexibility for select issues. Without this framework, any of the countless constituents may pose a risk to the health care ecosystem."

Through the efforts of the CISA 405(d) working groups and task groups, this momentum has been carried forward in a public-private partnership to implement the Task Force's call that "*HHS and NIST must develop guidance about how to apply the framework to the health care sector"* and *Industry and government should partner to establish an evaluation mechanism and prioritized best practices to support the range of small to large organizations to consistently apply the NIST Cybersecurity Framework.*

NIST's approach to cybersecurity risk management is globally recognized and widely adopted. In collaboration with NIST, the OCR and the Office of the National Coordinator for Health Information Technology (ONC) have completed a crosswalk of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the NIST CSF. At a minimum, this is a further validation of the NIST Cybersecurity Framework, if not further declaration of it as a "standard of care."

We have a national standard and it is the NIST CSF. It has been adopted by every one of the Department of Homeland Security's Critical Infrastructure sectors with the exception of the Healthcare and Public Health Sector. The federal government has adopted it, too. While we appreciate the intent of "certification" by other groups, NIST has stated that they will not develop a certification program for the CSF. They have, however, indicated that they would work with private organizations and companies to develop "certification criteria" and work with them to keep "certification" up to date as the CSF expands and evolves. Developing, or even recognizing other programs and processes – especially proprietary ones which leverage the NIST CSF – is contrary to the idea of *streamlining* as called for in the Cybersecurity Task Force Report.