

30 November 2022

Senator Mark Warner
U.S. Senate
703 Hart Bldg.
Washington, DC 20510

Ref: “Cybersecurity is Patient Safety”

Dear Senator Warner,

The TIC Council Americas is pleased to provide comment on “Cybersecurity is Patient Safety” Policy Options in the Health Care Sector. Independent third-party testing, inspection, and certification (“TIC”) organizations play a critical role in confirming the compliance of products, systems, and services to US regulations, industry requirements, and international standards.

Our members support all efforts to address cybersecurity in connected infrastructure¹, systems, components, devices and software and look forward to our ongoing engagement and discussion on this topic.

Using a combination of cybersecurity standards, evaluation, and certification will improve systems security and risk management, through metrics, measurements, and benchmarks that support acquisition requirements. Conformity assessment is a reasonable and responsible model for addressing the challenges of acquisition and cybersecurity and improving cybersecurity posture throughout our health care systems. And trusted, independent third-party conformity assessment is a cost-effective policy solution as it provides the highest level of confidence and helps government leverage private-sector resources.

For your consideration, we have included responses to questions posted in your request for comment and look forward to engaging with you and other stakeholders to identify solutions to protect our health care systems and infrastructure.


TIC Council is a global association representing over 90 international independent third-party testing, inspection, certification, and verification organizations. Testing, Inspection and Certification (TIC) companies cater to a diverse range of industry sectors and a variety of standards and legislation. The industry represents an estimated one million employees across the world with annual sales of approximately USD 200 billion.

Should you have any questions, please don't hesitate to contact Karin Athanas at +1 240 762 8069 / kathanas@tic-council.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'Hanane Taidi'.

Hanane Taidi
Director General
TIC Council

A handwritten signature in black ink, appearing to read 'Karin Athanas'.

Karin Athanas
Executive Director
TIC Council Americas
kathanas@tic-council.org

¹ https://www.tic-council.org/application/files/5915/5775/4670/IFIA_One_Pager_IoT_and_Cybersecurity.pdf

Question Responses

Section 1.1, Page 11 – Healthcare Cybersecurity Leadership Within the Federal Government.

1. Is the U.S. Department of Health and Human Services succeeding in its role as the Sector Risk Management Agency for health care and is HHS the most appropriate SRMA?
2. What is the current status of coordination between HHS and CISA? How could that coordination be improved?
3. Should the 405(d) Program continue to be the “hub” of HHS and federal government partnership with industry?
 - a. What other agencies should be part of such an effort, and how should they coordinate?
 - b. Does the 405(d) Program need additional resources to ensure it can continue to develop and disseminate its work? How do we effectively measure the efficacy of 405(d) in order to evaluate what is the appropriate level of additional resources?

Response: Whether it be in healthcare, food, manufacturing, or another industry, cybersecurity requires the coordination of multiple stakeholder and agencies to ensure that products and systems comply with cybersecurity best practices. A robust framework will provide beneficial policies to ensure the continued reliable operation of health care systems.² It is recommended that an advisory group which includes other agencies, stakeholders such as the TIC Council Americas, and others, work collaboratively to develop recommendations to protect the cybersecurity of health care systems.

Section 1.3, Page 14 – Health Care Specific Guidance from the National Institute of Standards and Technology

1. What should be included in a health care cybersecurity framework? Is sector-specific guidance from NIST for the health care sector necessary?
2. Is the current guidance from NIST sufficient? Has your organization or members of your organization implemented the recommendations in the Cybersecurity Framework? If not, why?
3. Has your organization implemented the health care-specific playbook developed by HSCC? If not, why?

Response: The NIST Critical infrastructure Cybersecurity framework provides guidance for industry in implementing cybersecurity practices; however, these recommendations are guidance and can be applied differently based on the industry and available resources. Where consistent application of guidance is difficult, an international standard such as IEC 62443, provides the additional structure and requirements needed to protect vulnerable systems. The IEC 62443, and other international standards, provide a robust application that aligns with the NIST National Framework for Improving Critical Infrastructure. Additional requirements such as those specific to Health Care would also be beneficial.

² “A Robust Cybersecurity Framework for Industrial Control Systems,” TIC Council Americas, https://www.tic-council.org/application/files/9316/2489/1094/2021_TIC_Council_Americas_position_paper_Cybersecurity_final.pdf

Section 1.4, Page 15 – Modernizing HIPAA to Address Cyber Threats

1. Is it appropriate to address both privacy and security within a single enforcement regime or are the risks, solutions, and institutional competencies sufficiently distinct to warrant separate regulatory regimes?
2. Where are the gaps in HIPAA currently, and how should it be expanded?
3. How should HIPAA regulations align with those of the Federal Trade Commission, such as the Health Breach Notification Rule?

Response: It can be difficult to enforce privacy and security in a single enforcement regime. Privacy and security needs will change overtime, requiring continual review and revision of the requirements to address emerging risks. By separating these issues, a broader application of cybersecurity to a wide range of high risk industries becomes possible.

Section 2.1, Page 21 – Establishing Minimum Cyber Hygiene Practices for Healthcare Organizations

1. How should Congress go about creating minimum cyber hygiene practices? Which federal agency should be responsible for development and implementation? What should be the incentives or penalties for compliance or noncompliance?
2. Regarding including these are part of a facility’s Medicare Conditions of Participation – if this is not the preferred framework, why not? What makes cybersecurity—which we’ve learned has patient safety risks— different from other critical patient safety protections that are currently required?

Response: As outlined in TIC Council document “Selecting Methods of Conformity for Regulatory Schemes,” the level of cyber hygiene practices required will depend on the level of risk, the availability of resources to perform pre and/or post market evaluations, and the level of penalties applied when an instance of noncompliance is identified. If the risk to patient safety and security is low, voluntary guidance may be appropriate. Where the risk is high, mandatory practices which are confirmed by an external body, such as the TIC industry, may be needed.³

Section 2.2, Page 22 – Addressing Insecure Legacy Systems

1. How should Congress help incentivize the alignment of the life cycles for medical equipment and the software that runs it?
2. What sorts of requirements should medical devices have to meet in order to be eligible for reimbursement under a “cash for clunkers” style program? Does such an approach pose an unacceptable moral hazard?
3. Should providers have a “right to repair” medical equipment by contracting with third-party providers?
4. Should medical equipment manufacturers be required to update their products for a certain length of time?

³ “Selecting Methods of Conformity for Regulatory Schemes,” TIC Council Americas, https://www.tic-council.org/application/files/9515/8694/5697/2018_Feb_13_Revised_-_Selecting_Methods_of_Conformity_for_Regulatory_Schemes.pdf

5. Is medical equipment becoming more modular, meaning that parts can be swapped out and replaced? Is the market for health IT moving towards alternative procurement models, such as device leasing, that address these risks?

Response: Software updates to IoT capable devices have the capability of protecting those devices from emerging cybersecurity risks. However, they may also compromise safety mechanisms and introduce unknown hazards. It is important that manufacturers maintain the software of equipment for the life of the equipment and that equipment owners replace equipment when equipment reaches its end of life. Additionally, when a software patch is issued, that the software be evaluated before and after patch to identify potential risks and vulnerabilities.⁴ Third-party TIC organizations support equipment users and manufacturers by evaluating product updates and products after update to confirm that products continue to comply with requirements for secure performance.

Section 2.3, Page 24 – Software Bill of Materials

1. Should a single agency or group be in charge of SBOM requirements?
2. Are health IT risks sufficiently grave or unique to warrant an accelerated or heightened SBOM approach from other commercial IT products? Should SBOM requirement be applied retroactively?
3. Should SBOM creation, publication, and sharing be mandatory or voluntary?

Response: The TIC Council Americas participated in the development of the SBOM through the NTIA stakeholder group and subsequently participated in stakeholder calls as CISA finalized recommendations and test cases for application of SBOM in industry settings. The SBOM has great promise in providing transparency as to the software used in the development of products and systems. However, it is equally critical that the authenticity and traceability of SBOMs be confirmed prior to product release.

⁴ “Strong Cybersecurity Protections Support a Safe and Secure Product Infrastructure,” TIC Council Americas, https://www.tic-council.org/application/files/3216/4873/6765/Americas_Position_on_Cybersecurity_for_Consumer_Products_-_March_2022.pdf