HITRUST®

6175 Main Street
Suite 400
Frisco, TX 75034

855.HITRUST
(855-448-7878)
www.HITRUSTAlliance.net

June 6, 2024

VIA Hand Delivery and Email

House Energy & Commerce Committee
House Oversight & Accountability Committee
House Veteran Affairs Committee
House Ways & Means Committee
House Budget Committee

Senate Appropriations Committee
Senate Budget Committee
Senate Finance Committee
Senate Health Education Labor & Pensions Committee
Senate Veterans Affairs Committee

Dear Senators and Representatives:

I am writing to you on behalf of HITRUST[1], a leading provider of cybersecurity and information security assurances, to share our perspectives as you evaluate recommendations to avoid or minimize a repeat of the recent ransomware attacks that have impacted healthcare organizations, including Change Healthcare and Ascension Health. As a longstanding leader in information security and cybersecurity risk management[2] with 17 years of practical experience and demonstrable results in the health industry, HITRUST feels compelled to offer our perspective to the current discourse surrounding these incidents so that legislative, regulatory and policy makers have relevant information relating to the role standards and related assurances play in addressing information security and cybersecurity risks.

We commend the efforts of Congress and regulatory bodies to address the cybersecurity challenges that continue to threaten US critical infrastructure, including healthcare. However, we caution against reactionary measures that focus on additional or mandatory information security standards and regulatory requirements without better understanding the assurance framework[3] needed to ensure their relevance, implementation, operation, and maturity. The health industry is not lacking in cybersecurity and information security standards but is lacking in ensuring the standards are relevant to the current and emerging cyber threats and that there are appropriate

[1] See https://www.hitrustalliance.net.

[2] The Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Survey identified the NIST Cybersecurity Framework and HITRUST CSF as the two most widely used cybersecurity frameworks in the healthcare industry. See the 2018 HIMSS Cybersecurity Survey. Chicago: HIMSS North America. Available from https://www.himss.org/sites/hde/files/d7/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

[3] See https://hitrustalliance.net/the-hitrust-assurance-program.

and reliable mechanisms to define, measure, and report on their implementation and effectiveness.

A key element of any solution must be to ensure that relevant controls are embodied in standards and frameworks and that they are implemented and operating properly to deliver effective risk mitigation. Relevant standards **with** reliable assurances provide confidence and transparency that the appropriate controls are implemented and operating effectively. The current and unsustainable approach is comparable to adding more stringent accounting standards to define internal control requirements without the underlying and complementary need for robust audits.

Our primary recommendation is to shift the focus from creating or mandating additional standards to ensuring that existing frameworks allow for selection of relevant controls that are threat-adaptive[4], and that compliance outcomes, where needed, are only earned through robust assurance programs[5]. Specifically, we ask Congress and regulatory bodies to consider the following key points:

1. **Strong Assurance Programs:** Assurance programs should be leveraged to validate that controls are not only in place, but also effective and operationally mature. In addition, assurance systems must be transparent, scalable, consistent, accurate, and efficient—essential for trust and integrity.
2. **Continuous Improvement:** Standards and frameworks must be kept relevant to the risk and evolving cyber threat landscape, where controls are constantly evaluated and enhanced to meet current and emerging cyber threats. Regulatory standards are updated infrequently and are insufficient to maintain pace with cyber threats; thus, using approaches that adapt actively as threats evolve is essential.
3. **Measurable Outcomes:** The industry needs consistent, transparent, and accurate models[6] to measure and benchmark the effectiveness of controls. As the adage goes, "if it is

[4] HITRUST Enhances Cyber Threat Adaptive Engine Using Microsoft Azure OpenAI Service and Microsoft Defender Threat Intelligence. See https://hitrustalliance.net/press-releases/hitrust-enhances-cyber-threat-adaptive-engine-using-microsoft.
[5] See https://hitrustalliance.net/assessments-and-certifications.
[6] See the HITRUST Control Maturity Scoring Rubric available at https://23257256.fs1.hubspotusercontent-na1.net/hubfs/23257256/Download%20Center%20%2B%20Partner%20Content/HITRUST-CSF-Control-Maturity-Scoring-Rubrics.pdf.

important, you need to measure it." This allows for continuous optimization and better risk management.

4. **Support for Control Selection and Tailoring for all levels of Inherent Risk:** All entities with an internet presence are susceptible to cyber attacks. The industry therefore needs an approach that begins with a specific set of good security hygiene and/or best/leading practices applicable to all organizations. Tailoring[7] of additional control selections on top of those practices allows support for additional requirements and outcomes based on inherent risk and the approach needed to provide cyber security and resiliency for different size and classes of organizations. This model works because the eventual set of requirements are all backed and validated by the same transparent, consistent, accurate and efficient assurance system. This is especially important to the resilience of the healthcare system and other critical infrastructure industries where a subset of companies is the largest and most critical to the mission of the industry. This approach permits regulatory consistency without the 'one size fits all' approach that is inherently suboptimal due to differences in organizational complexity and maturity.

5. **Support for Healthcare Diversity through Inheritance and Shared Responsibility:** Smaller healthcare organizations and systems supporting rural or underserved communities need the same cybersecurity as larger organizations with more resources. As small and large organizations heavily rely on cloud service providers for technology and cybersecurity needs, the use of such systems can accelerate cybersecurity capability adoption for their customers—today, 85% of the requirements for a HITRUST assessment may be inherited by health industry companies from a HITRUST certified cloud service provider[8], such as Amazon AWS, Microsoft Azure, or Google Cloud. Making robust cybersecurity capabilities available to all healthcare industry organizations increases efficiency and reduces cost while streamlining security compliance.

[7] NIST defines tailoring as a process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. See NIST Online Glossary: Tailoring. Available from https://csrc.nist.gov/glossary/term/tailoring.

[8] See https://hitrustalliance.net/shared-responsibility-matrices.

6. **Improved Information Risk Management Drives Improvements in Cyber Insurance**: When security events happen, cyber insurance provides needed resources for incident response and system recovery. However, growing losses across cyber insurance products make obtaining, affording, and maintaining cyber insurance coverage increasingly challenging. Mature and robust information security assessments with relevant controls and assurance provide confidence to insurance underwriters[9] that relevant security controls are in place and operating effectively, reducing the likelihood and impact of a cyber event and associated losses. Assurance also reduces the complexity of the insurance application process and can often help manage the risk that the cost of cyber insurance may rise beyond what small and less mature entities can afford.
7. **Responding to New Risks such as AI:** Cyber threats are accelerating with the adoption of Artificial Intelligence, which relies heavily on sensitive and protected information. Appropriate security controls are necessary to harness AI's promise for health innovation, patient, and provider engagement. HITRUST and leading AI service providers are actively collaborating on AI risk management and security requirements[10], including an AI Assurance Program[11] built on our proven assurance model. including shared responsibility and inheritance of security controls available from leading AI service providers.
8. **Risk Management, Not Absolute Security:** It is critical to shift the culture and mindset from seeking absolute security to managing risks[12]. This involves applying relevant controls and using reliable assurance methodologies to reduce risks to acceptable levels, with remaining residual risks covered by cyber insurance. Regulation and policy making based on data-driven evidence of control implementation provided by assurance systems can enable powerful incentives for regulated entities that confidently demonstrate the maturity of their cybersecurity system in a provable manner.

[9] HITRUST and specialty insurance underwriter Trium announce availability of new cyber security insurance product for HITRUST-certified customers. See https://hitrustalliance.net/press-releases/hitrust-announces-availability-of-new-cyber-insurance-product.

[10] See https://hitrustalliance.net/ai-hub.

[11] HITRUST Releases the Industry's First AI Assurance Program. See https://hitrustalliance.net/press-releases/hitrust-releases-the-industrys-first-ai-assurance-program.

[12] See https://www.manula.com/manuals/hitrust/risk-management-handbook-exposure-draft/1.0/en/topic/executive-summary.

We know that the approach outlined in our recommendations can be effective as demonstrated and documented in HITRUST's latest *Trust Report*[13]—99.4% of our current certifications, which includes organizations of varying sizes in many industries including health, did not report a breach over the past two-year period while operating in one of the most aggressive cyber-attack environments in history. This is a testament to the significance of relevant controls and a strong assurance program—one that ensures that the appropriate security controls are validated through reliable testing to earn objective certification. The HITRUST framework is continually updated to address the evolving threat landscape and ensures that organizations can implement and maintain controls that are effective in mitigating information risk and updated in response to the changing threat landscape.

The healthcare industry already possesses the necessary standards, frameworks, and assurance programs to mitigate risks effectively—although additional focus is warranted to maintain relevance against a continually changing threat landscape—requiring adaptive approaches to keep pace with emerging cyber threats seeking to compromise companies. What is lacking is greater adoption of the approaches that are proven effective. HITRUST has long championed these concepts and implemented solutions for cyber threat adaptive control and assurance frameworks to support comprehensive information risk management, which emphasizes the implementation of relevant controls backed by proven and measurable operational maturity of sufficient strength.

HITRUST acknowledges the numerous public and private initiatives focused on defining security standards, frameworks, and approaches. Unfortunately, many of these initiatives are incomplete as they lack sufficient clarity of the security controls needed and / or are silent on the fundamental need for robust and reliable security assurance. Therefore, those initiatives, regardless of compliance expectations, do not solve the underlying cybersecurity problem and risk management challenges. As discussed above, proactive and proven approaches to security assurance are essential to risk management without regard to the standards and controls specified and required. Companies also often have duplicated or overlapping compliance

[13] See https://hitrustalliance.net/trust-report.

expectations requiring adherence with multiple standards and frameworks which detracts from investment in security operations due to the cost of compliance management.

Healthcare industry companies will continue to be frequent targets of criminals and nation states until we implement approaches that make information security validation and assurance an inherent part of cybersecurity programs. Compliance motivations alone do not solve the problem as the speed of changing cyber threats outpaces compliance systems. Only a proactive, threat-adaptive approach can ensure that relevant controls are in place and operating before entities are attacked.

We urge Congress, healthcare, and cybersecurity leaders in Government to consider these points as they look to enhance our nation's cybersecurity posture. Rather than introducing more standards, we ask for support for efforts that encourage adoption of proven capabilities already available in the private sector including reciprocity for approaches that are demonstrated to be effective.

HITRUST stands ready to support these efforts and to work with you to respond with urgency to the cybersecurity challenges facing our nation and the health sector. The safety of our citizens and the efficiency of the providers that care for them is vital to our nation.

Thank you for your attention to this critical matter. We look forward to continuing our dialogue and working together to strengthen our nation's cybersecurity infrastructure.

Sincerely,

Daniel Nutkis
Founder and Chief Executive Officer
HITRUST

CC: Secretary Xavier Becerra
Department of Health and Human Services

Director Jen Easterly
Cybersecurity and Infrastructure Security Agency