Summary - HITRUST's Response

RFI - Opportunities and Obstacles to Harmonizing Cybersecurity Regulations

The Office of Acting National Cyber Director Kemba E. Walden issued a Request for Information (RFI) related to the Opportunities and Obstacles to Harmonizing Cybersecurity Regulations. Responses were to be submitted by October 31, 2023. HITRUST submitted its response to this RFI. The following represents HITRUST's recommendation to the challenge of harmonization of cybersecurity regulations.

Why is HITRUST well-qualified to respond?

HITRUST was founded in 2007 as a cybersecurity and data privacy standards organization. Since that time, we have worked in close collaboration with privacy, information security, and risk management leaders from public and private sectors to develop, maintain, and provide broad access to our widely adopted, common risk and compliance management framework, the HITRUST CSF, and other assessment and assurance methodologies and mechanisms that are part of the HITRUST Assurance Program. We champion programs that safeguard sensitive information and manage information risks for healthcare and public health (HPH) and other industries throughout the third-party supply chain in the U.S. and globally.

Harmonization is fundamental to HITRUST. We work closely with public and private sectors to provide an integrated approach to address multiple frameworks, standards, legislative and regulatory requirements. The resulting robust assurance mechanism ensures appropriate implementation. The HITRUST CSF is continuously updated with more than 40 authoritative sources, including National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, NIST SP 800-171, International Standards Organization and International Electrotechnical Commission (ISO/IEC) Standard 27001 (ISO/IEC 27001), and Health Insurance Portability and Accountability Act (HIPAA) security requirements.

HITRUST was asked by the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) to develop sector-specific guidance in 2015 for the implementation of the NIST CSF. HITRUST also chaired the development of the most recent version of the HPH sector guidance, published by the Department of Health and Human Services (HHS) in March of 2023. The update expands the scope of the original document to address the use of any NIST Framework for Improving Critical Infrastructure Cybersecurity, Informative References such as ISO/IEC 2700 and NIST SP 800-53, and the HITRUST CSF to help specify a reasonable and appropriate set of cybersecurity controls.

HITRUST is the only cybersecurity certification body approved for Qualified Health Information Networks under the Trusted Exchange Framework and Common Agreement (TEFCA). The HITRUST r2 Validated Assessment is the only cybersecurity certification approved under TEFCA.

The Health Third Party Trust (Health3PT), an initiative focused on solving challenges in third-party risk management (TPRM) and led by a council comprised of the nation's leading healthcare organizations, recently selected HITRUST assessments using the HITRUST CSF and the HITRUST Assurance Program as essential tools to increase trust for the industry and with third-party suppliers.

Key Takeaways of HITRUST's Response

Consistent cybersecurity outcomes require true harmonization, including reciprocity and assurances.

Based on our experience supporting, reviewing, and certifying thousands of security assessments for healthcare and other critical infrastructure sectors, HITRUST agrees that the voluntary securing of critical infrastructure has had measurable benefits. However, these have not been consistent across or within all critical infrastructure sectors. The need is for more than just standards and regulations. These are, of course, necessary for achieving desired results. We believe adequate, consistent cybersecurity outcomes can only be achieved where results are measured and evaluated. We suggest minimizing the creation of additional regulatory mandates. Instead, we encourage proper harmonization, which should include a focus on reciprocity and accountability with existing regulations across industries and incorporating private sector assurances that deliver transparency, reliability, and high-quality outcomes.

More regulation alone does not solve the challenges in cybersecurity.

HITRUST cautions that there is risk in mandating new, different cybersecurity requirements for the widely diverse industries in the private sector. Without adequately considering how new regulations apply across industries, they could produce no aggregate benefit or even introduce harm by focusing resources on compliance over security outcomes. There is no 'one size fits all' approach to cybersecurity, and organizations need flexibility to adapt appropriately. Unique business cases will arise based on an organization's size, resources, business environment, legal obligations, threats, and use and integration of third-party technologies and services such as cloud services and generative AI. Industry-specific threats, such as those to medical devices, payment card devices, or access to treasury functions, will also drive unique needs.

Additionally, for any approach to mandatory or voluntary standards to work, they must be both flexible and prescriptive enough to help all types of organizations build cybersecurity programs that

- deliver far more than a 'check the box' model for compliance
- generate prescriptive policy, procedure, and implementation expectations
- specify evidence required to achieve and exceed the required outcomes
- identify a scoring model
- provide the testing and assurance system necessary to independently demonstrate effective maturity implementation

Effective approaches to harmonizing regulation will be best served if accepted best practices are aligned with reliable assurances.

Given the common occurrence of breaches in organizations thought to have had appropriate controls in place, the need for reliable assurances cannot be overstated. HITRUST recommended in our response that ensuing regulations require the use and acceptance of highly reliable cybersecurity assessment and certification programs from the private sector. Where properly implemented, these will demonstrate that practices — or controls — are comprehensive in breadth and depth. They will ensure that all reasonably anticipated threats for the applicable contexts are addressed, risks are managed appropriately, and compliance requirements are addressed properly. They will ensure that controls are fully implemented, actively monitored, and constantly managed so that they can be relied upon to operate effectively and as intended in an evolving threat environment. And they will ensure that the information provided is trustworthy. Trustworthiness requires that it comes from independent and high-quality sources, including practitioners and professional services firms, and that the assessment and reporting methods are likewise independent and high-quality.

By leveraging the concept of reliability when mandating assurance requirements, regulators should be able to determine with a high degree of confidence how organizations are implementing cybersecurity frameworks and standards, including those provided by the NIST Cybersecurity Framework's Informative References. They must know whether their implementations are reasonable and appropriate to an organization's risk and predisposing conditions. And they must be aware if it can be reasonably determined that their implementations have been in place for a requisite period of time.

Reciprocity, including reliance on private sector assurances, will be critical to effective harmonization.

HITRUST suggests that public and private partnerships will improve cybersecurity as public standards take hold across industries and private sector investments fuel harmonization and unification of standards. As acceptance of constantly updated, reliable, and transparent assurance mechanisms demonstrate effective cybersecurity, they will guide additional organizations and entities to adopt them, creating nationwide improvements organically.

Third-party assessors involved in cybersecurity assurances must be accredited through and adhere to an established quality system.

Third-party assessment systems that use trained and certified third-party assessors provide scale but will only add value if they operate within an accreditation and management system. The system must result in trained and qualified assessors and provable, validated, and consistent results. This requires monitoring and quality management processes to test and validate the work performed across multiple assessors and assessment organizations. Assurance reports should be based upon a provable and transparent system that ensures that issued reports align with expectations.

Reliance expectations require transparency, scalability, consistency, accuracy, and integrity.

HITRUST believes that only reliable reports should be used for cybersecurity reliance. The concept of assurance reliability based upon expected attributes, or outcomes, is critical for those who rely upon the assurances they receive. Both private sector companies and regulators can know with confidence that third-party assessors have consistently examined the cybersecurity outcomes targeted by an organization and that reliance on the resulting outcomes is appropriate. Key attributes are

- Transparency – Are controls incorporated, and is the assessment approach utilized, including the evaluation and scoring model, open and transparent to all stakeholders, including regulators? More specifically, will the report's recipient understand how the controls were selected, evaluated, and scored?
- Scalability – Is the approach used appropriate to the size and type of organization assessed? Does the tailoring of the Informative References follow accepted guidelines?
- Consistency – Are assessment results consistent, regardless of which third-party assessor organization professional or professional services firm was engaged? Does the process ensure that individuals performing the work evaluate and document their findings consistently?
- Accuracy – Do assessment results accurately reflect the state of controls implemented in an organization's environment? What mechanisms are in place to facilitate the accurate evaluation and scoring of implemented controls?
- Integrity – Are assessments conducted, and are results reported consistent with prescribed requirements for the assessment and reporting option? What processes are in place to ensure the assessor conducted the assessment faithfully and reported the results truthfully?

Conclusion

HITRUST, through over a decade of developing and harmonizing standards, creating and operating an assurance program, and reviewing tens of thousands of assessments, believes that any approach to harmonizing cybersecurity regulations – especially with the intent to mandate specific cybersecurity requirements and assurance mechanisms – should require the minimum necessary while providing maximum flexibility. However, it is essential to be clear that flexibility should not be equated with insufficient cybersecurity requirements, low assurance expectations, or self-governance systems that attest against internally established, opaque, or potentially lower control expectations.

Instead, HITRUST promotes more robust assurances demonstrating the outcomes required for our nation. This is possible using existing and recognized cybersecurity standards and frameworks, proven and reliable assurances from the private and public sectors, and formal reciprocity with reliable third-party approaches to assurance, including assessment, certification, and reporting. Such an approach will increase cybersecurity outcomes and improve scalability and subsequent adoption by the industry.

We thank the National Cyber Director, the President, and the Vice President for their leadership in this vital area. Regulatory harmonization and potential expansion of the cyber regulatory framework are complex and critical topics for our nation. HITRUST looks forward to engaging with others across our nation as we take on this crucial challenge.