HITRUST®

6175 Main Street
Suite 400
Frisco, TX 75034

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

October 25, 2023

Executive Office of the President
Office of the National Cyber Director
ATTN: Kemba E. Walden
Acting National Cyber Director
1650 Pennsylvania Avenue
Washington, DC 20504

RE: REQUEST FOR INFORMATION (RFI) ON CYBERSECURITY REGULATORY HARMONIZATION

VIA regulations.gov

Dear Director Walden:

Thank you for the opportunity to respond to your office's recent RFI on potential opportunities for—and obstacles to—harmonizing cybersecurity regulations. The following comments address those questions relevant to our experience as a globally recognized leader in information risk management and assurance reporting.

Support for Critical Infrastructure

Since our founding in 2007, HITRUST[1] has championed programs that safeguard sensitive information and manage information risk for organizations in the healthcare and public health (HPH) sector, other critical and non-critical industries, and throughout the third-party supply chain in both the U.S. and internationally. In collaboration with privacy, information security, and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted[2] common risk and compliance management framework, the HITRUST CSF,[3] as well as related assessment and assurance methodologies[4] incorporated into the HITRUST Assurance Program.[5]

[1] HITRUST (2023a). About HITRUST. Available from https://hitrustalliance.net/about-hitrust/.

[2] For example, 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.
For more information on HIMSS, see HIMSS (2023). About HIMSS. Available from https://www.himss.org/who-we-are.

[3] HITRUST (2023b). HITRUST CSF. Available from https://hitrustalliance.net/product-tool/hitrust-csf/.

[4] HITRUST (2023c). HITRUST Assessments. Available from https://hitrustalliance.net/product-tool/hitrust-assessments/.

[5] HITRUST (2023d). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.

Harmonization through Public and Private Industry Partnership

HITRUST has worked closely with the public and private sectors to provide an integrated approach to cybersecurity that can address multiple best practice frameworks, standards, and legislative and regulatory requirements while also providing a robust assurance mechanism to ensure appropriate implementation. This approach embraces harmonization, in both spirit and in fact, which requires an ongoing investment in risk management principles; risk-based control and safeguard identification, specification, and selection; and alignment of risk management and controls across many authoritative sources for cybersecurity. Mechanisms that allow a harmonized framework to be practically implemented, controls to be selected and specifically applied, and implementation maturity to be transparently scored are required for any framework to achieve the desired cybersecurity outcomes.

Specifically, the HITRUST CSF is continuously updated with more than 40 authoritative sources including National Institute of Standards and Technology (NIST)[6] Special Publication (SP) 800-53,[7] NIST SP 800-171,[8] International Standards Organization and International Electrotechnical Commission (ISO/IEC) Standard 27001 (ISO/IEC 27001),[9] and Health Insurance Portability and Accountability Act (HIPAA)[10] security requirements. In addition, the HITRUST Assurance Program provides a rigorous approach to maturity scoring, third-party assessment, and centralized quality assurance of each assessment conducted under the program.

Public and Private Industry Partnership in Practice

Due to our demonstrated leadership in healthcare cybersecurity and information risk management, HITRUST was asked by the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC)[11]

[6] NIST (2023a). About NIST. Available from https://www.nist.gov/about-nist.

[7] Joint Task Force, JTF (2020, Sep). Security and Privacy Controls for Information Systems and Organizations, Rev. 5 (NIST SP 800-53 r5). Gaithersburg, MD: NIST: Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[8] Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., and Guissanie, G. (2020, Feb). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Rev. 2 (NIST SP 800-171 r2). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[9] ISO/IEC (2022). Information Security, Cybersecurity And Privacy Protection - Information Security Management Systems – Requirements. Geneva: ISO/IEC. Available from https://webstore.ansi.org/standards/iso/isoiec270012022.

[10] Office of Civil Rights, OCR (2013, Mar 26). HIPAA Administrative Simplification Regulation Text: 45 CFR Parts 160, 162, and 164. Washington, DC: HHS. Available from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

[11] CISA (2022b). Sector Coordinating Councils. Available from https://www.cisa.gov/sector-coordinating-councils.

(HSCC) and Government Coordinating Council (GCC)[12] to develop sector-specific guidance[13] in 2015 for implementation of the NIST CSF. HITRUST also chaired the development[14] of the most recent version of the HPH sector guidance, published by the Department of Health and Human Services (HHS) in March of 2023.[15] The update expands the scope of the original document to address the use of any NIST Framework for Improving Critical Infrastructure Cybersecurity[16] (NIST Cybersecurity Framework) Informative Reference,[17] such as ISO/IEC 2700 and NIST SP 800-53, as well as the HITRUST CSF to help specify a reasonable and appropriate set of cybersecurity controls.

In addition, HITRUST is currently the only cybersecurity certification body and the HITRUST r2 Validated Assessment[18] the only cybersecurity certification currently approved for Qualified Health Information Networks under the Trusted Exchange Framework and Common Agreement[19] (TEFCA) program operated by the Office of the National Coordinator for Health Information Technology.[20] [21] And, HITRUST assessments using the HITRUST CSF and the HITRUST Assurance Program[22] were also recently selected by a council representing the nation's leading healthcare organizations through the Health 3rd Party Trust[23] (Health3PT) initiative seeking to ensure cybersecurity and third-party risk management

[12] CISA (2022c). Government Coordinating Councils. Available from https://www.cisa.gov/government-coordinating-councils.
[13] Joint HPH Cybersecurity Working Group (2016, May). *Healthcare Sector Cybersecurity Framework Implementation Guide*, Ver 1.1. Available from https://hitrustalliance.net/uploads/HPHCyberImplementationGuide.pdf.
[14] HHS (2023). HPH Sector Cybersecurity Framework Implementation Guide: Acknowledgements. Available from https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/Acknowledgements.aspx.
[15] HHS and HSCC Cybersecurity Working Group, CWG (2022, Mar). *HPH Cybersecurity Framework Implementation Guide, ver. 2.0*. Available from https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Documents/HPH-Sector-CSF-Implementation-Guide-508.pdf.
[16] NIST (2018, Apr 16). Framework for Improving Critical Infrastructure Cybersecurity, Ver. 1.1. Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[17] NIST (2023b). Informative References: What are they and how are they used? Available from https://www.nist.gov/cyberframework/online-learning/informative-references.
[18] HITRUST (2023e). HITRUST Risk-based, 2-Year (r2) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-risk-based-2-year-r2-validated-assessment/.
[19] Office of the National Coordinator for Health Information Technology, ONC (2022, Jan). *Common Agreement for Nationwide Health Information Interoperability*, v1. Available from https://rce.sequoiaproject.org/wp-content/uploads/2022/01/Common-Agreement-for-Nationwide-Health-Information-Interoperability-Version-1.pdf.
[20] Per Section 12.1.2 of the Common Agreement, QHINs must achieve and maintain third-party certification to an industry-recognized cybersecurity framework demonstrating compliance with all relevant security controls, as set forth in the Standard Operating Procedure (SOP): QHIN Security Requirements for the Protection of TI v1.1.
[21] The Sequoia Project (2022). QHIN Cybersecurity Certification. Available from https://rce.sequoiaproject.org/qhin-cybersecurity-certification/.
[22] HITRUST (2023f). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.
[23] HEALTH3PT (2023a). What is the Health 3rd Party Trust (HEALTH3PT) Initiative. Available from https://health3pt.org/about-us/.

through collecting assurances, identifying residual risks, and tracking and managing those identified risks across companies from all sectors serving the health industry.[24]

Consistent Outcomes Require Appropriate Assurance

Based on this 15+ years of experience supporting, reviewing, and certifying thousands of security assessments for healthcare and other critical infrastructure sectors, HITRUST agrees that—while voluntary approaches to securing critical infrastructure have resulted in marked improvement—such improvements have not proven consistent across all critical infrastructure sectors or even within them. Our experiences, and those of the hundreds of security assessors firms with whom we work, demonstrate that the issue is not the standards and regulations alone. We suggest that high-quality, robust and consistent assurance mechanisms are equally important, if not more important, to achieving adequate and consistent cybersecurity outcomes for all security regulations. Outcomes are only achieved where results are evaluated and measured.

We therefore suggest that additional regulation that would mandate more cybersecurity requirements be minimized and instead encourage the spirit of harmonization and a focus on reciprocity and accountability not only across existing regulations supporting different industries but with private sector assurance systems that can provably and transparently deliver high-quality and reliable outcomes. Such a partnership and approach will improve cybersecurity for our nation through the uptake of public standards across multiple industries, leverage of existing private sector investments to harmonize and unify those standards, and the acceptance of constantly updated, reliable, and transparent assurance mechanisms that guide and demonstrate effective cybersecurity.

[24] HEALTH3PT (2023b). HITRUST selected by Health3PT in Alignment with Recommended Practices. Available from https://info.health3pt.org/hitrust-assurance-program-selected-by-health3pt-in-alignment-with-recommended-practices/.

We also caution government on the extent to which ensuing regulations mandating new and different cybersecurity requirements will impact the incredibly diverse private sector entities without achieving the expected benefit of regulation. There is no 'one size fits all' approach to cybersecurity,[25] especially when such an approach restricts the ability of organizations to manage cyber risk in a way that is appropriate to their particular situation.

Responses to specific questions articulated in the RFI are provided below.

Questions for Respondents

Q1: Conflicting, mutually exclusive, or inconsistent regulations.

a. *Specific examples*: No comment.

b. *Timely updates*: While not opining on which federal or SLTT cybersecurity rules or enforceable guidance may impose conflicting, mutually exclusive, or inconsistent requirements (reference Q1.a), it is important to recognize the inherent latency in the maintenance of security rules and standards against the rate at which cyber threats and new risks evolve and emerge. HITRUST can cite many instances where existing standards and regulations take years before being updated to address changes in the cyber threat landscape. Examples include but are not necessarily limited to the NIST SP 800-53B[26] control baselines[27] and its many enhanced overlays[28] [29] such as the Centers for Medicare and Medicaid (CMS)[30] Acceptable Risk Safeguards

[25] For example, see Financial Industry Regulatory Authority, FINRA (2015, Feb). Report on Cybersecurity Practices. Washington, DC: Author, p. 38. Available from https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf.

[26] JTF (2020, Oct). Control Baselines for Information Systems and Organizations (NIST SP 800-53B). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

[27] NIST defines a security control baseline as the set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system. See NIST (2023c). NIST Online Glossary: Security Control Baseline

[28] NIST defines a security control overlay as a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. See NIST (2023d). NIST Online Glossary: Security Control Overlay. Available from https://csrc.nist.gov/glossary/term/security_control_overlay.

[29] NIST defines an enhanced overlay as an overlay that adds processes, controls, enhancements, and additional implementation guidance specific to the purpose of the overlay. See NIST (2023e). NIST Online Glossary: Enhanced Overlay. Available from https://csrc.nist.gov/glossary/term/enhanced_overlay.

[30] CMS (2023). About CMS. Available from https://www.cms.gov/about-cms/about-cms.

(ARS),[31] Minimum Acceptable Risk Standards for Exchanges (MARS-E),[32] and the Federal Risk and Authorization Management Program (FedRAMP).[33] This becomes even more pronounced where cyber threats evolve and shift quickly and requires an approach that can keep up with those new threats through multiple updates per year.

c. *Compliance*: In our experience, organizations subject to multiple regulatory requirements for cybersecurity either implement multiple stand-alone programs with duplicated costs or—in the case where multiple cybersecurity requirements are applicable to the same scope of implementation—integrate them manually through a governance, risk, and compliance (GRC) application or use an integrated framework such as the HITRUST CSF with the benefit of providing assurances for multiple regulations and requirements based on investment in a single assessment. The HITRUST 'assess once and report many' approach allows complementary requirements to be identified and harmonized where implementation specifics and standards vary between different sources of guidance and regulation.

d. *Costs*: The cost of maintaining and operating a complex system with multiple regulatory requirements can vary considerably depending on the approach taken. And, duplicated and disjointed regulatory requirements for similar or common controls impose additional costs for governance and validation with a commensurate reduction in the ongoing capital and operational budgets available to implement and sustain security controls. Said another way, such a system, at any scale, increases governance cost both in capital expense for duplicated capabilities and operational expense in work hours to manage the multiple expectations without a corresponding improvement in security outcomes. More importantly, even where large and complex companies have the resources to strive to meet multiple and disjointed requirements, duplicative systems dilute focus on operational outcomes which impedes the ability to prevent and respond to cybersecurity events.

[31] CMS (2022, Jun 29). CMS Acceptable Risk Safeguards (ARS), Ver. 5.1x. Baltimore, MD: Centers for Medicare & Medicaid Services. Available from https://www.cms.gov/files/document/acceptable-risk-safeguards-v51.xlsx.

[32] CMS (2021, Feb 23). Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite, Volume I: Harmonized Security and Privacy Framework, Ver. 2.2 (Doc. No. CMS_CIO-STD-SEC01-3.1). Baltimore, MD: Centers for Medicare & Medicaid Services. Available from https://www.cms.gov/files/document/mars-e-v2-2-vol-1final-signed08032021-1.pdf.

[33] FedRAMP (2023). About Us: Program Basics. Available from https://www.fedramp.gov/program-basics/.

e. *Redundancy*: No comment.

f. *Annual costs*: No comment.

g. *Resources*: No comment.

h. *Security Gaps*: No comment.

i. *Mitigating costs*: See comment in Q1.j below.

j. *Implementation*: Although cybersecurity maturity levels can vary widely within a specific industry, a recent study indicated regulated industries like finance and healthcare have, on average, more mature cybersecurity programs than their less regulated counterparts.[34] Unfortunately, the benefits identified in the study are limited – indicating that those regulated industries demonstrate maturity that is only slightly above the middle level which is just one level above 'ad hoc management.' As a result, some may conclude that our current regulatory approach has failed to materially improve the state of information security for those industries that are subject to them and may actually result in less security than would otherwise be possible due to the cost or inefficiency of regulatory governance.[35] To be most effective in both outcomes and costs, the private sector should be primarily responsible for cybersecurity with clearly identified accountability that security outcomes adhere to regulatory expectations using clear and transparent assurances. The government can support and encourage industry efforts by financially incentivizing companies that adopt certain cyber policies while potentially withholding funds from those who do not implement these policies.[36] Consistent with the approach taken by NIST and supported by complementary private sector efforts, we subsequently recommend regulations require a specific set of good security hygiene and / or best / leading practices applicable to most organizations as a common security control baseline

[34] Eiden, K., Kaplan, J., Kazimierski, B., Lewis, C., and Telford, K. (2021, Aug 4). Organizational cyber maturity: A survey of industries. Available from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries#/.

[35] Clinton, L. (2022, Jan 21). Regulation of Cybersecurity Has Been Tried and It Doesn't Work (Blog). Available from https://isalliance.org/regulation-of-cybersecurity-has-been-tried-and-it-doesnt-work/.

[36] Richard A. Clarke, R. and Robert K. Knake, Robert (2020). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats," New York: Penguin.

with support for further tailoring[37] [38] based on risk analysis for specific organizations.[39] This would avoid a 'one size fits all' approach that is inherently suboptimal due to differences in organizational complexity and maturity, [40] [41] [42] resulting in excessive costs for some organizations and less than optimal protection for others. To further improve an organization's return on security investment, regulations should also incentivize organizations to maintain their security program through the mitigation of fines and other penalties in the event of a breach[43] or through true 'safe harbor'[44] but only where such benefits are earned by recognized and provable assurances.

Q2: Use of Common Guidelines.

a. *Effectiveness*:

While the referenced Federal Financial Institutions Examination Council (FFIEC)[45] model may work for a single sector, HITRUST does not believe a single set of control requirements—harmonized or not—would be effective across multiple disparate sectors due to the diversity of both their respective business environment and their threat landscape. However, common guidelines can be effective if 'structured' and used appropriately. For example, in the Healthcare and Public Health Sector:

[37] 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 (2023f). NIST Online Glossary: Tailoring. Available from https://csrc.nist.gov/glossary/term/tailoring.

[38] See JTF (2020, Oct), pp. 5 – 14 for additional information on the use and tailoring of control baselines.

[39] Cline, B. (2017, Sep). Leveraging a Control-Based Framework to Simplify the Risk Analysis Process In the ISSA Journal 15(9), pp. 39 – 42. Available from https://mydigitalpublication.com/publication/?m=1336&i=436950&p=42&pp=1&ver=html5.

[40] Moraetes, G. (2018, Jan 26). Choosing the Right Security Framework to Fit Your Business. Security Intelligence. Available from https://securityintelligence.com/choosing-the-right-security-framework-to-fit-your-business/.

[41] Covington, R. (206, Apr 13). When it comes to security standards, one size doesn't fit all. CSO. Available from https://www.csoonline.com/article/555669/when-it-comes-to-security-standards-one-size-doesnt-fit-all.html.

[42] Lorenzin, L. (2019, Aug 5). Why Zero Trust is not a one-size-fits-all solution. FedTech. Available from https://fedtechmagazine.com/article/2019/08/why-zero-trust-not-one-size-fits-all-solution.

[43] One example of these types of mitigations is provided in what is colloquially referred to as the 'HIPAA Safe Harbor Act." See An Act To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, Pub. Law No. 116-321 (2021). Available from https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf.

[44] Safe harbor may be defined as a provision granting protection from liability or penalty if certain conditions are met. A safe harbor provision may be included in statutes or regulations to give peace of mind to good-faith actors who might otherwise violate the law on technicalities beyond their reasonable control. See Cornell Law School (2023). Legal Information Institute: Wex: Safe Harbor. Available from https://www.law.cornell.edu/wex/safe_harbor.

[45] FFIEC information security requirements are one of the many authoritative sources integrated and harmonized within the HITRUST CSF.

1. The NIST Cybersecurity Framework provides a comprehensive set of desired cybersecurity outcomes via the Framework Core Subcategories[46] while leaving it up to implementing organizations to determine the specific cybersecurity controls required to achieve those outcomes.

2. Then, the HPH sector provides additional guidance[47] on how the Framework Core Illustrative References[48] can be used to select additional controls, i.e., tailor the control baseline, to address any additional risk to an organization's sensitive information[49] (as addressed in Q1.j above).

Based on this approach, one could effectively mandate the 'core' good hygiene / best practice control baseline and the risk-based tailoring requirement while allowing the use of voluntary frameworks such as the NIST Cybersecurity Framework Core Informative References to tailor the baseline as needed.

b. *Challenges*: Expanding upon our response to Q2.a, the primary challenge to such an approach is the overall diversity of organizations to which it would necessarily apply. Examples include but certainly aren't limited to an organization's size, resources, business environment, legal obligations, threats (including industry-specific threats such as those to medical devices, payment card devices, or access to treasury functions), use and integration of third-party technologies and services (e.g., cloud services, generative AI), and other predisposing conditions.[50]

c. *Extensibility*: Adapting a model such as the one used by the FFIEC would require limiting the set of 'harmonized controls' to only those that are arguably universal across multiple sectors or

[46] NIST (2023g). Cybersecurity Framework Components: Framework Core. Available from https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components.

[47] HHS and HSCC CWG (2023, Mar). HPH Sector Cybersecurity Framework Implementation Guide, ver. 2.0. Available from https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx.

[48] NIST (2023h). Informative References: What are they, and how are they used? Available from https://www.nist.gov/cyberframework/online-learning/informative-references.

[49] HITRUST's approach to control framework-based risk analysis and control specification provides the foundation for HPH sector guidance on implementing the HITRUST CSF. See HHS and HSCC CWG (2022, Mar), pp. 7 – 8.

[50] JTF Transformation Initiative (2012, Sep). Guide for Conducting Risk Assessments, Rev. 1 (NIST SP 800-30 r1). Gaithersburg, MD: NIST, p. 32. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

organizational types. Cybersecurity outcomes would be better served if the model allows each organization to tailor the resulting baseline and address their particular situation. Extensive guidance on the tailoring process as well as the development of sector, sub-sector, and other types of target profiles[51] based on common risk factors[52] would facilitate the tailoring process in addition to providing additional consistency in control specification amongst organizations with similar inherent risk.[53] Additionally:

1. A more robust approach to obtaining and sharing reliable assurances beyond self-assessment,[54] including formal reciprocity between and amongst the independent providers of such assurances, would be needed to make an approach like the one used by FFIEC extensible; and
2. An automated means of sharing assurances between and amongst organizations and their stakeholders[55] would also be helpful.

d. *Appropriateness*: The model would be applicable to all sectors if aligned with our response to Q2.c.

[51] NIST (2018, Apr 16), p. 11.

[52] NIST defines risk factors as a characteristic used in a risk model as an input for determining the level of risk. See NIST (2023i). NIST Online Glossary: Risk Factor. Available from https://csrc.nist.gov/glossary/term/risk_factor.

[53] Risk models define the risk factors to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk factors are also used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition. See Cline, B. (2022, Jul), p. 16.

[54] HITRUST (2020). How Do I Know if an Assurance Report is Rely-Able? Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/How-Do-You-Know-if-a-CSF-Assurance-Report-is-Rely-able.pdf.

[55] Charest, K. (2021, Oct 21). HITRUST Results Distribution System (RDS) Adds Efficiency in Providing Information Assurances (Blog). Available from https://hitrustalliance.net/hitrust-results-distribution-system-rds-adds-efficiency-in-providing-information-assurances/.

e. *Application outside of examination-based compliance*: Compliance is not security.[56] [57] But it can be construed as the 'floor' from which security begins. And while examination-based compliance regimes may be applied to cybersecurity, the requirement for specific trained and experienced technical cybersecurity and audit expertise to achieve the depth of analysis needed to assess operational outcomes is a constraint for all industries. For any approach to mandatory or voluntary standards to work, they must be flexible and prescriptive enough to help organizations of all types use them to build a cybersecurity program that delivers far above a 'check the box' model for compliance; generates prescriptive policy, procedure and implementation expectations; specifies evidence required to achieve and exceed the required expectations; identifies a scoring model; and then the testing and assurance system necessary to demonstrate that cybersecurity maturity is effectively implemented. The approach described in our responses to this RFI supports both regulatory examination and cybersecurity outcomes.

f. *Opportunities for improvement*: Implementation and then oversight of a (i) tailoring process as described in our response to Q2.a and c, including the development and harmonization of sector-specific or similar target profiles, and (ii) assurance processes, especially in the areas of reliability and reciprocity, would provide significant opportunities for improvement over the FFIEC model and support for other industries.

[56] For example, see Dewing, F. (2019, 15 Aug). Compliance is Not Security: Why You Need Cybersecurity Chops in the Boardroom. Available from https://www.forbes.com/sites/theyec/2019/08/15/compliance-is-not-security-why-you-need-cybersecurity-chops-in-the-boardroom/?sh=64e7962339b8.

[57] Bailey, K. (2019, Jan 17). Why compliance does not equal security. Forbes. Available from https://www.forbes.com/sites/forbestechcouncil/2019/01/17/why-compliance-does-not-equal-security/.

g. *Self-assessment*: While useful as part of a broader assessment portfolio,[58] self-assessments typically provide a low level of assurance about the state of an organization's cybersecurity program relative to an independent or third-party assessment.[59] Self-assessments are subject to bias[60], including the tendency to overestimate performance[61], and a lack of expertise in critically scoring outcomes while conducting self-assessment. The ability for an internal or external stakeholder, including regulators, to rely upon the results and subsequent conclusions of an assessment is subsequently impacted by these issues and many others.[62]

HITRUST subsequently limits the use of self-assessments to organizations that present low inherent risk or as part of an iterative third-party assurance process for organizations with higher levels of risk.[63] Organizations that use the HITRUST Approach typically use HITRUST Readiness Assessments—which are self-assessments—to determine their current profile[64] and then identify the actions needed to obtain HITRUST certification as well as maintain awareness of the state of their cybersecurity programs on an ongoing basis.[65] HITRUST requires such self-assessments be based upon the same control framework so they may serve as a stepping stone to more robust forms of assurance with appropriate levels of independence and quality. Self-assessment can be a part of the overall model but cannot alone serve as the basis of the model.

h. *Common tools*: A common self-assessment tool such as the HITRUST Readiness Assessment mentioned in our response to Q2.g would help organizations on their journey towards demonstrating cybersecurity maturity and achieving regulatory requirements; however, it

[58] Cline, B. (2019, Nov 11). Understanding and improving the role of self-assessments in third-party risk management. HITRUST. Available from https://hitrustalliance.net/understanding-improving-role-self-assessments-third-party-risk-management/.

[59] Cline, B. (2022, Jul). HITRUST TPRM Qualification Process: Methodology Guide. Frisco, TX: HITRUST, pp. 21 – 26. Available from https://hitrustalliance.net/content/uploads/HITRUST-Third-Party-Risk-Management-Methodology.pdf.

[60] de Wit, J. and Meyer, C. (2022, May 1). Uncovering Cognitive Biases in Security Decision Making. In *Security Management* (May/Jun 2022). Available from https://www.asisonline.org/security-management-magazine/articles/2022/05/uncovering-cognitive-biases-in-security-decision-making/.

[61] de Wit, J., Pieters, W., and Van Gelder, P. (2023, Jul). Bas and noise in security risk assessments, an empirical study on the information position and confidence of security professionals. In *Security Journal*. Available from https://www.researchgate.net/publication/372162382_Bias_and_noise_in_security_risk_assessments_an_empirical_study_on_the_information_position_and_confidence_of_security_professionals.

[62] The reliability of an assessment or audit can be evaluated based on its suitability relative to the needs of a relying party, the rigor with which it is conducted, and its inherent impartiality or lack of bias. See Cline, B. (2022, Jul), pp. 22 – 23.

[63] Cline, B. (2022, Jul), p. 27.

[64] NIST (2018, Apr 16), p. 11.

[65] HITRUST (2016, Aug 3). HAA 2016-009: Intent of Readiness Assessments. Available from https://hitrustalliance.net/advisories-archive/.

would be a poor tool for the provision of assurances around one's compliance with those requirements to regulators and other third parties due to a self-assessment's inherently lower level of reliability for the reasons stated in our response to Q2.g.

Q3: Use of Existing Standards or Frameworks.

a. *Consistency and alignment*: The variability of cybersecurity requirements and standards, including how prescriptive or descriptive said standards may be, is an impediment to consistency and alignment. And, while any standard or framework can be mapped to another, there are invariably gaps in those mappings due to the way the controls are developed and written.[66] HITRUST has experienced this firsthand with more than 40 authoritative sources integrated within the HITRUST CSF.[67] Relationships between requirements across standards and frameworks are seldom one-to-one and are more often one-to-many, many-to-one, and even many-to-many. This is true even for some overlays of a NIST SP 800-53 control baseline such as NIST SP 800-171,[68] which can result in misalignment, complexity, and inconsistency of interpretation and subsequent implementation.

One way to help ensure alignment between and amongst the many standards and frameworks in use today is by taking a more formal approach to mapping requirements from multiple sources such as the one published and used by NIST in their Cybersecurity Framework Online Informative Reference (OLIR) program[69] and then identifying and leveraging accumulative and superseding dependencies between them for proper application.

   i. *Applicability*: See our response to Q3.a above.[70]

[66] Keller, N., Quinn, S., Scarfone, K., Smith, M., and Johnson, V. (2022, Dec). National Online Informative References (OLIR) Program: Overview, Benefits, and Use, Initial Public Draft (NIST IR 8278r1 ipd). Gaithersburg, MD: NIST, pp. 4 – 9. Available from https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8278r1.ipd.pdf.

[67] HITRUST (2022, Dec). Introduction to the HITRUST CSF, Ver. 11.0.0. Frisco, TX: Author, p. 9. Available from https://hitrustalliance.net/content/uploads/CSFv11.0.0_Introduction.pdf.

[68] Cline, B. (2023, Jul 6). Letter to R. Ross, NIST. Re: Call for Comments on Initial Public Draft: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations, p. 2. Available from https://csrc.nist.gov/csrc/media/projects/protecting-controlled-unclassified-information/Call-for-comments-July-2023/CUI_Call_HIITrust_July7_2023.pdf.

[69] Keller, N., Quinn, S., Scarfone, K., Smith, M., and Johnson, V. (2022, Dec).

[70] HITRUST (2022, Dec), p. 9.

ii. *Adoption*: Regulators have adopted multiple frameworks and standards at both the federal and state level. For example, see the colloquially described "HIPAA Safe Harbor Act"[71] at the federal level where the Office of Civil Rights has narrowly interpreted "Recognized Security Practices" to only two federally issued standards[72] and the "Ohio Safe Harbor Act"[73] at the state level where Ohio lists multiple public and private sector frameworks and approaches with varying levels of depth and coverage. These different approaches lead to inconsistency in approach for covered entities that are seeking to align themselves with multiple such laws and with regard to variability of expected outcomes. HITRUST regularly provides input to lawmakers and regulators through testimony,[74] responses to RFIs,[75] [76] and other such avenues whenever such opportunities arise. Examples of such input include many of the points made in our response to Q2.a – g around the need for flexible control standards, reliable assurance, and formal reciprocity.

b. *Conformity*: While federal and state laws address various frameworks and standards related to the specification and implementation of cybersecurity requirements, they generally fail to address how subsequent assurances around the implementation of those requirements should be conducted other than such assurances would be needed. Assuming a primary, if not the primary objective, of an assurance approach is to provide trustworthy information about an organization's ability to safeguard sensitive information and subsequently demonstrate the effectiveness of its controls to meet its compliance obligations, the degree of reliability of an

[71] An Act to amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, Pub. Law No. 116-321 (2021).

[72] See the pre-recorded video presentation for HIPAA covered entities and business associates (regulated entities) on "recognized security practices,". Department of Health and Human Services Office of Civil Rights. Available at https://youtu.be/e2wG7jUiRjE.

[73] Businesses Maintaining Recognized Cybersecurity Programs, Ohio Rev. Code, Title 13, Ch. 1354, § 1354.02. Available from https://codes.ohio.gov/ohio-revised-code/section-1354.02.

[74] Nutkis, D. (2017). Cybersecurity Regulation Harmonization: Hearings before the U.S. Senate Committee on Homeland Security & Governmental Affairs. Available from https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Nutkis-2017-06-21.pdf.

[75] Booker, R. (2022, Nov 30). Letter to Sen. M Warner. Re: Cybersecurity is Patient Safety – Policy Options in the Health Care Sector. Available from HITRUST upon request.

[76] Cline, B. (2022, May 18). Letter to L. Coffer, HHS/OCR. Re: HITECH Act 'recognized security practices' Request for Information – HHS-OCR-0945-AA04. Available from HITRUST upon request.

assurance approach should be the deciding factor in how much consideration it is given for any type of safe harbor provided by regulators.

Given the number of breaches that have and continue to occur in organizations purported to have had appropriate practices (controls) in place, the need for reliable assurances cannot be overstated. HITRUST strongly recommends that ensuing regulations require the use and acceptance of highly reliable cybersecurity assessment and certification programs available from the private sector as well as the public sector. Such methods generally consider whether:

(i) the practices (controls) are comprehensive in breadth and depth to ensure all reasonably anticipated threats for the applicable contexts are addressed, risks are managed appropriately, and compliance requirements are addressed appropriately;

(ii) the practices (controls) are fully implemented as well as monitored, and managed to ensure they operate and will continue to operate effectively, as intended, in an evolving threat environment; and

(iii) the information provided about the first and second areas are trustworthy, which generally involves considerations around the independence and overall quality of the practitioners, professional services firms, and assessment and reporting methods employed.

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; whether their implementations are reasonable and appropriate to the risk and predisposing conditions pertinent to an organization; and if it can be reasonably determined their implementations have been in place for a requisite period of time.[77]

[77] Cline, B. (2022, May 18), pp. 6 – 7.

c. *Additional opportunities*: No additional comment, as we believe the approach articulated in our responses to previous questions is the single best approach to harmonizing regulations around the implementation and assessment/certification of an organization's cybersecurity program.

Q4: Third-Party Frameworks:

a. *Current frameworks*: As discussed previously, we recommend the NIST Cybersecurity Framework and supporting Informative References such as NIST SP 800-53 and the HITRUST CSF using the risk-based approach described in current HPH sector implementation guidance.[78]

b. *Efficacy*: HITRUST has demonstrated the efficacy of this approach (see Q4.a) in addressing disparate cybersecurity requirements for organizations of various types and sizes across multiple industries over the past 15 years. The HITRUST CSF, which incorporates dozens of disparate frameworks and standards,[79] supports a model implementation of the NIST Cybersecurity Framework[80] and provides some of the most highly reliable assurances[81] available to the public and private sector.[82] [83]

Q5. Tiered Regulation.

a. *Adaptability*: A tiered model has been successfully demonstrated in the private sector through use of the HITRUST CSF by organizations of all types and sizes over the past 15 years.[84] The key to structuring such a standard is to require a baseline set of good hygiene and best practices common to most if not all organizations and tailoring the baseline by adding and modifying requirements based on specific (inherent) risk factors. See our response to Q2.c. A tiered regulatory model should also address the assurances required by regulators in a similar fashion. A one-size fits-all approach to assurance is neither cost-effective nor efficient, which is why organizations such as HITRUST and the Payment Card Industry (PCI) Security Standards Council

[78] HHS and HSCC CWG (2023, Mar).
[79] HITRUST (2022, Dec), p. 9.
[80] Joint HPH Cybersecurity Working Group (2016, May), p. 9.
[81] Cline, B. (2022, Jul), pp. 21 – 26.
[82] HITRUST (2018, May 22). HITRUST Provides NIST Cybersecurity Framework Certification. Available from https://hitrustalliance.net/press_release/hitrust-provides-nist-cybersecurity-framework-certification-2/.
[83] HITRUST (2023g). FAQs: Risk Management Frameworks: HITRUST & NIST. Available from https://hitrustalliance.net/faqs/hitrust-risk-management-framework/hitrust-and-the-nist-cybersecurity-framework/?id=2729.
[84] For example, see HIMSS (2018).

(SSC)[85] provide different types of assessments for organizations with varying levels of information risk.[86] [87]

b. *Extensibility*: See our response to Q2.c and Q5.a above.

Q6. Oversight.

a. *Agency engagement*: One example of overlapping (if not potentially conflicting) federal oversight was shown in a recent joint letter from the HHS Office of Civil Rights and the Federal Trade Commission on the "privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties".[88] HHS has the authority to regulate information under the HIPAA Security Rule[89] and the FTC has the authority to enforce data protection practices under the Federal Trade Commission Act.[90] Others undoubtably exist given how organizations often select multiple regulatory risk factors when tailoring the HITRUST CSF to a specific scope of implementation and assessment.

b. *Oversight*: No further comment.

c. *Awareness*: No further comment.

d. *Multiple oversight*:

i. *Primary agency*: In the example provided in Q6.a, we believe the FTC defers to HHS/OCR when violations of the HIPAA Security Rule occur.

ii. *Reciprocity*: HITRUST has found that, without a formal (and transparent) approach to reciprocity, regulators tend to view potential reciprocity on a case-by-case basis or at time of enforcement. The result is uncertainty if not confusion on the part of regulated

[85] PCI SSC (2023). About Us. Available from https://www.pcisecuritystandards.org/about_us/.
[86] HITRUST (2023c).
[87] PCI DSS (2015). Understanding the SAQs for PCI DSS Version 3. Available from https://docs-prv.pcisecuritystandards.org/SAQ%20(Assessment)/Instructions%20%26%20Guidance/Understanding_SAQs_PCI_DSS_v3.pdf.
[88] For example, see FTC (2023, Jul 20). FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies. Available from https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.
[89] OCR (2013, Mar 26).
[90] Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2012). Available from https://www.ftc.gov/section-5.

entities on what practices must be implemented, or even prioritized, and how assurances around their implementation must be provided to demonstrate compliance.

iii. *Barriers*: No further comment.

e. *Unintended consequences*: No comment.

f. *Annual cost*: No comment.

g. *Multiple agency*: No comment.

h. *Obstacles and inefficiencies*: See our response to Q6.d.ii.

i. *Cyber reciprocity*: We are not aware of any formal reciprocity agreements in this context beyond the example provided in Q7.f regarding the stated intent by the Cybersecurity Maturity Model Certification (CMMC) Accreditation Body to accept FedRAMP for cloud service providers in the Defense Industrial Base.[91]

j. *Non-cyber reciprocity*: No comment.

k. *Self-attestation*: See our response to Q2.a, c, g, and h.

l. *Burden reduction and process harmonization*: 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 that both results in trained and qualified assessors and provable, validated, and consistent results. This requires the use of monitoring and quality management processes to test and validate the work performed across multiple assessors and assessment organizations. HITRUST has a robust set of qualifications for third party assessors,[92] and only issues assurance reports that demonstrate adherence with HITRUST expectations:

- **Transparency** - Are controls incorporated and the assessment approach utilized, including evaluation and scoring model, open and transparent to all stakeholders including regulators?

[91] Doubleday, J. (2022, Jul 6). Pentagon 'endorses' reciprocity for CMMC, FedRAMP requirements. Federal News Network. Available from https://federalnewsnetwork.com/defense-main/2022/07/pentagon-endorses-reciprocity-for-cmmc-fedramp-requirements/.

[92] HITRUST (2023h). HITRUST External Assessor Requirements. Available from https://hitrustalliance.net/content/uploads/HITRUST-External-Assessor-Requirements.pdf.

More specifically, will the recipient of the report 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 the third-party assessor organization professional or professional services firm engaged? More specifically, does the process ensure that individuals performing the work are evaluating and documenting their findings consistently?
- **Accuracy** – Do assessment results accurately reflect the state of controls implemented in an organization's environment? Or more specifically, what mechanisms are in place to facilitate the accurate evaluation and scoring of implemented controls?
- **Integrity** - Are assessments conducted and the results reported consistent with prescribed requirements for the assessment and reporting option? More specifically, what processes are in place to ensure the assessor conducted the assessment faithfully and reported the results truthfully?

Only reliable reports should be used for cybersecurity reliance. By leveraging the concept of assurance reliability based on the above attributes when evaluating the maturity of an entity's cybersecurity program, private sector companies and regulators can all know with confidence that the cybersecurity outcomes targeted by the organization have been consistently examined by third party assessors and that reliance on the resulting outcomes is appropriate.

i. *Appropriate circumstances*: Third-party assessments are preferred due to the availability of scale and qualified resources through a private market of multiple providers when aligned with the quality attributes identified above in Q6.l and harmonization will incent more interest and participation by potential third party assessors. However, self-attestation is also a valuable and complementary tool appropriate for (i) small businesses with quantifiable low inherent risk, (ii) any organization that presents quantifiable low inherent risk in a specific business relationship where the third-party is the relying party and providing additional oversight, and (iii) as an initial assessment in an iterative assessment process in which the final assessment is a third-party assessment. In all cases, the limitations in the use of self-assessments addressed in our response to Q2.g remain present but may be somewhat mitigated if self-attestation is based upon the same control framework and assurance scoring system. Ultimately self-assessments can serve as a valuable stepping stone to more robust forms of assurance and a powerful internal management tool where appropriate in the cases identified above.

ii. *Inappropriate circumstances*: See our response to Q6.l.i.

Q7: Cloud and Other Service Providers.

The use of cloud service providers and other service providers for cybersecurity requires consideration of both shared responsibilities and how service users and service providers together document the shared responsibilities between the service provider or providers and the subscriber or user of the cloud services. Major cloud service providers use HITRUST certifications to demonstrate the cybersecurity capabilities that they provide to their users[93] with 85% of the requirements for a HITRUST assessment available to be inherited from a certified cloud service provider.[94] This proven and scalable approach will become even more important in the growing use of generative AI and the resulting large language models provided by AI service providers with HITRUST and leading AI service providers recently announcing new collaboration focused on AI risk management and security including an AI Assurance Program.[95]

a. *Conflicting, mutually exclusive, or inconsistent requirements passed to third parties*: Three specific examples include the HIPAA Security Rule, required by HHS;[96] Centers for Internet

[93] HITRUST (2023i). HITRUST Shared Responsibility and Inheritance Program. Available from https://hitrustalliance.net/hitrust-srm-inheritance-program/.
[94] HITRUST (2023i).
[95] HITRUST (2023j). The HITRUST Strategy for Providing Reliable AI Security Assurances. Available from https://info.hitrustalliance.net/path-to-trustworthy-ai.
[96] Office of Civil Rights, OCR (2013, Mar 26).

Security Critical Security Controls (CIS CSC),[97] required by the State of California; and FedRAMP, required by Federal Agencies.[98]

b. *Direct regulation of third parties*: See our response to Q7.a above.

c. *Costs to third parties*: No comment.

d. *Inconsistent permissions*: No comment.

e. *Non-U.S. government third party models*: No comment.

f. *Comparing FedRAMP*: Consistent with our earlier responses, FedRAMP—or a similar model—would need to provide a more dynamic approach to control specification beyond the traditional low, medium, and high impact security control baselines that, while arguably appropriate for federal agencies, is much less appropriate to private sector organizations with incredibly diverse risk factors and predisposing conditions. FedRAMP would also need to expand formal reciprocity to other mechanisms for the provision of assurance such as those provided by HITRUST[99] that meet a requisite bar for reliability (as discussed earlier in our response).

g. *Inconsistent regulation of specific technologies*: No comment.

Q8: State, Local, Tribal, and Territorial Regulation.

a. *Effective regulations*: No comment.

b. *Reciprocity*: No comment.

c. *Extensibility*: No comment.

d. *Incompatibility*: No comment.

[97] PR Newswire (2016, Feb 22). California Attorney General Concludes that Failing to Implement the Center for Internet Security's (CIS) Critical Security Controls 'Constitutes a Lack of Reasonable Security.' Available from https://www.prnewswire.com/news-releases/california-attorney-general-concludes-that-failing-to-implement-the-center-for-internet-securitys-cis-critical-security-controls-constitutes-a-lack-of-reasonable-security-300223659.html.

[98] FedRAMP (2023).

[99] HITRUST (2023c).

Q9. International.

a. *International conflicts*: International regulatory frameworks often only require the implementation of 'good' security practices in support of individual privacy rather than a specific cybersecurity framework or standard.[100] We subsequently see eventual conflicts in (i) the selection of a reasonable and appropriate set of cybersecurity controls needed to adequately protect sensitive information, (ii) the level of reliability required in an acceptable approach to assurance, and (iii) subsequent issues with reciprocity between and amongst national and international regulations and the standards and frameworks allowable under those regulations.

b. *International prioritization*: Recommend consideration of the European Union (EU)[101] and Asian Pacific Economic Cooperation (APEC)[102] data protection frameworks.

c. *Most promising venues*: No comment.

d. *Ongoing initiatives*: No comment.

e. *Reciprocity*: No further comment.

Q10. Additional Matters.

We would like to reiterate 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, flexibility should not be equated with insufficient cybersecurity requirements; a low level of assurance expectations; or self-governance systems that attest against internally established, opaque, or potentially lower control expectations. Instead, we seek more robust assurances that demonstrate the outcomes required for our nation. This is possible through the use of existing and recognized cybersecurity standards and frameworks, use of proven and reliable assurances from the private and public sector, and formal

[100] For example, see European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Available from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[101] European Parliament and Council. (2016).

[102] APEC (2023, Jun). What is the Cross-Border Privacy Rules System? Available from https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

reciprocity with such reliable third-party approaches to assurance (i.e., assessment, certification, and reporting). Such an approach will both increase cybersecurity outcomes and will also improve scalability and subsequent adoption by industry. We believe the approach articulated in our responses to your questions will help ensure both; is aligned with the focus of the Office of the National Cyber Director; is efficient to implement and quicker to adoption by building on existing standards, regulations and capabilities from both the private and public sector; and will ultimately benefit the whole of government and our nation in the most effective manner possible.

Regulatory harmonization and potential expansion of the cyber regulatory framework are complex and critical topics for our nation and we thank you for the opportunity to provide input as you contemplate how best to help improve critical infrastructure cybersecurity. HITRUST looks forward to engaging in the process as you move forward and hope you will feel free to contact us with any questions or requests for additional information.

Sincerely,

Bryan S. Cline, Ph.D.
Chief Research Officer
bryan.cline@hitrustalliance.org
Phone: 469-269-1118

Robert Booker
Chief Strategy Officer
robert.booker@hitrustalliance.net