Testimony of Daniel Nutkis
CEO of HITRUST Alliance
Before the U.S. Senate Committee on
Homeland Security & Governmental Affairs
Hearing entitled: "Cybersecurity Regulation Harmonization"
June 21, 2017

Prepared for Submission

Chairman Johnson, Ranking Member McCaskill, and Members of the Committee, I am pleased to appear today to discuss the health industry's experiences in engaging with government agencies relating to cybersecurity regulatory harmonization and efforts we believe will provide the greatest benefit to industry. I am Daniel Nutkis, CEO and Founder of the Health Information Trust Alliance, or HITRUST. HITRUST was founded in 2007, after industry recognized the need to formally and collaboratively address information privacy and security for healthcare stakeholders representing all segments of the industry and organizational sizes. HITRUST endeavored—and continues to endeavor—to elevate the level of information protection in the healthcare industry and its collaborators, especially between industry and government. Our goal is to raise the competency level of information security professionals while maintaining trust with consumers and patients regarding their health information, and to promote cyber resilience for industry organizations.

In my testimony today, I will highlight three areas where cybersecurity regulatory harmonization should occur to reduce redundancy, unnecessary expense and delays to better support the private sector in defending against cyber threats, thereby improving cyber resilience and the management of cyber risk. First is the area of information sharing. Second is the role of government as a partner. And third is the role of government as a regulator.

1. Information Sharing

In 2010, HITRUST established a mechanism to share Indicators of Compromise (or IOCs) and other cyber threat information with organizations of varying cyber maturity. HITRUST has led the industry in the collection and distribution of cyber threat information through the development of enhanced standards and collection practices, it has published numerous reports on its progress, it continues to evaluate its effectiveness, and it continually innovates to support organizations in managing their cyber threats.

From the beginning, HITRUST participated with the Department of Homeland Security's Cyber Information Sharing and Collaboration Program (CISCP). Prior to 2015, when Executive Order 13691 was issued, HITRUST engaged with DHS to become an Information Sharing and Analysis Organization (ISAO) per the guidance provided in the Executive Order. The Order outlines the role of ISAOs in supporting information sharing to a sector or segment and how to engage with DHS to support the goals of the Order. Additionally, when DHS established a

mechanism to improve information sharing with an automated system, we were the first healthcare organization to begin sharing bi-directionally with the DHS' Automated Indicator Sharing (AIS) program.

As an ISAO, we have worked with the DHS's National Cybersecurity and Communications Integrations Center (NCCIC) as a conduit for coordination and additional information on cyber threats. HITRUST was an early supporter of the Cybersecurity Act of 2015 (CISA), allowing additional liability protections to be granted when sharing with the Departments of Homeland Security, Commerce, Defense, Energy, Justice, Treasury, and the Office of the Director of National Intelligence. We have always approached the role of an ISAO as a partner of both industry and government and believed that we were operating in a partnership towards a common goal as we understood our roles and expectations based on the Executive Order and other guidance.

We were then surprised to learn that the Department of Health and Human Services (HHS) recently established its healthcare-specific cybersecurity communication center to focus its efforts on analyzing and disseminating cyberthreats across the healthcare industry.

HHS states that the Healthcare Cybersecurity and Communications Integrations Center (HCCIC) intends to: (1) strengthen engagement across HHS Operating Divisions; (2) strengthen reporting and increase awareness of the healthcare cyber threats across the HHS enterprise; and (3) enhance public-private partnerships through regular engagement and outreach. The HCCIC intends to help organizations by sharing information and best practices around cyber threats and mitigation techniques.

While we agree these are important objectives, we believe it raises some important issues, as it appears the role of the HCCIC parallels the intended role and capabilities of ISAOs. Clear guidance and communication should be established to ensure private sector activities are supported and not duplicated by government programs.

We recognize that there is a large role for government to play in supporting information sharing and ensuring liability protection. We continue to support the role of government in fostering transparency by establishing guidance that clarifies roles and responsibilities and encourages industries and communities of interest to determine how to engage with information sharing organizations based on their applicability, level of performance and overall value.

There is a significant level of effort required for organizations like HITRUST to engage in cyber information sharing programs with the government. Though we anonymize the information shared to protect the contributing organization, the process requires soliciting buy-in, gaining approvals and amending agreements from its thousands of constituents questioning the value, liability and effort to participate in these programs. We undertake these efforts because we see the value in the program and partnership with government and believe we are all operating towards a common goal. More can and should be done to ensure the roles of industry and government are clearly defined when it comes to information sharing.

2. Government as a Partner

HITRUST values its government partners and recognizes the burden, responsibility and authority beholden on them to protect the private sector. However, we would expect in areas where the private sector has made a significant investment in establishing an effective program or approach, the government would give it due consideration before seeking a government alternative that replicates or devalues industry efforts.

Last year, the Health and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), with input from HITRUST and other sector members including the DHS Critical Infrastructure Cyber Community (C3), developed the Health Sector implementation guide for the NIST Cybersecurity Framework, specifically referred to as the "*Healthcare Sector Cybersecurity Framework Implementation Guide*".[1] This *Implementation Guide* is listed on the US-CERT website identifying multiple sector-specific guidance for NIST CSF implementation.

The Health Sector Guide supports implementation of a sound cybersecurity program that addresses the five core functions of the NIST Cybersecurity Framework to ensure alignment with national standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with other information security and privacy risk management activities in the Healthcare Sector. The Healthcare Sector leverages the HITRUST risk management framework, including the HITRUST CSF and CSF Assurance Program, to effectively provide the Sector's implementation of the NIST Cybersecurity Framework.

This guidance continues to be updated and enhanced to ensure greater applicability and ease of adoption through the efforts of the Joint (SCC/GCC) HPH Cybersecurity Working Group. Yet despite the significant public and private effort that went into its publication, HHS is working towards the development of yet another healthcare-based implementation guide of the NIST Cybersecurity Framework despite the broad adoption of the existing guidance by private sector organizations that have already made the effort to leverage existing marketplace resources.

As recent as last year, after careful deliberation, the Department of Labor's ERISA Advisory Council published "*Cybersecurity Considerations for Benefit Plans*" recommending that Retirement Plans consider following existing privacy and security frameworks available through organizations such as HITRUST.

We state these points in an effort to highlight that not only is the HITRUST CSF already the most widely accepted cyber resilience framework in healthcare with tens of thousands of organizations having adopted it, it also has support in other areas of government as well as other industries. Additionally, we have developed a CSF BASICs program, which is a streamlined version of the HITRUST CSF, designed to help small and lower-risk organizations meet otherwise difficult regulatory and risk management requirements.

[1] See https://www.us-cert.gov/ccubedvp/cybersecurity-framework, and https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

HITRUST has been collaborating with industry for over 10 years and has an advisory council to ensure we are meeting the needs of the entire industry. This council has representatives from many of the leading healthcare membership organizations representing hospitals, health plans, medical practices and physician groups.

We are perplexed as to why HHS would not partner with industry by leveraging programs already in place and offering assistance to improve them instead of replicating and dismissing the hard work of industry. We would ask that Congress require federal agencies to give due consideration to existing standards and best practices already in place before developing new ones.

3. Government as a Regulator

The Department of Health and Human Services is responsible for overseeing the implementation of the Health Insurance Portability and Accountability Act or HIPAA, and the HHS Office for Civil Rights (OCR) is responsible for assessing compliance with and enforcement of the HIPAA Privacy, Security and Breach Notification Rules, including issuance of civil and criminal penalties.

In support of their role, they conduct annual random audits that are designed to "enhance industry awareness of compliance obligations and enable OCR to better target technical assistance regarding problems identified through the audits. Through the information gleaned from the audits, OCR will develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches."[2]

There is no question that organizations, both large and small, that create, store or transmit protected health information need to comply with the HIPAA regulations, and that the HIPAA Security Rule outlines a number of actions organizations must take including implementing appropriate security controls based on their risk assessments. Further, it is clear that HHS is responsible for enforcement of the HIPAA Security Rule.

While the mission of OCR is noble, and one that we recognize as required, we have documented that these random audits are in fact causing organizations to divert their attention and resources from enhancing their information protection programs based on the potential for random audits. Said differently, organizations that have, in fact, implemented appropriate and effective information security programs are diverting resources to focus on preparing for a random OCR audit rather than investing those resources on additional cyber defense or resilience programs.

We also recognize that this is not the case across the healthcare industry. Take the recent WannaCry incident, where vulnerabilities were exploited by cyber threat actors using ransomware impacting organizations that did not appropriately implement security controls such

[2] See https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html?language=es

as patching, end point protection and the necessary network segmentation of devices and systems.

At the same time, there are many organizations that have implemented a comprehensive security framework, such as the HITRUST CSF, performed a risk assessment, engaged in cyber information sharing and are complying with the HIPAA regulations that were not impacted by WannaCry.

Yet, under the current audit model, OCR is using its limited resources to audit organizations that have already implemented appropriate privacy and security controls and conducted required risk assessments, for which OCR has no visibility. OCR resources could be better served in focusing on organizations not adequately addressing the HIPAA privacy and security requirements.

We propose that policy makers consider a system whereby organizations that can demonstrate a comprehensive information security program that complies with the privacy and security provisions of HIPAA can receive some form of safe harbor or similar relief, and focus HIPAA audits on those organizations that cannot demonstrate their compliance in meeting the criteria. As noted above, the Sector has done a tremendous amount of work, and there are a number additional industry-led initiatives that should be leveraged to incentivize industry to do the right thing, make the necessary investments and protect their environments.

We are advocating that guidelines be established to enable organizations to communicate that they have obtained a comprehensive assessment covering the HIPAA Privacy and Security Rules, such as a HITRUST CSF Assessment, and that they be excluded from random OCR HIPAA privacy and security audits.

This approach would create cost savings to industry by not having to prepare for unnecessary government audits, and save government resources by not using tax payer dollars to assess organizations that can already demonstrate compliance. The approach would likely increase compliance by providing greater incentives for organizations to comply with the privacy and security provisions of HIPAA and allowing OCR to target resources towards organizations not complying with the privacy and security provisions of HIPAA.

HITRUST is currently conducting a study that will substantiate and communicate the approach and benefits outlined above, which we hope to complete in the next 90 days. I look forward to updating the Committee on the results.

I hope my testimony illuminated a number of areas where individual activities may seem innocuous, but in totality begin to create confusion and concern. I have highlighted where additional clarity in regulation and guidance will ensure the private sector understands how to best engage with government and also the complex issues that arise when a regulator is partnering with industry.

Thank you again for the opportunity to join you today and share these insights. I look forward to your questions.