Testimony of Daniel Nutkis
CEO of HITRUST Alliance
Before the Homeland Security Committee,
Subcommittee on Cybersecurity and Infrastructure Protection
Hearing entitled: "The Current State of DHS Private Sector Engagement for Cybersecurity"
March 9, 2017

Prepared for Submission

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the Subcommittee, I am pleased to appear today to discuss the health industry's experiences in engaging with the Department of Homeland Security relating to cyber information sharing and other cyber initiatives and the role we believe provides 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 those it collaborates with, ensuring greater collaboration between industry and government, raising the competency level of information security professionals, while maintaining trust with consumers and patients regarding their health information, and promoting cyber resilience of industry organizations.

In my testimony today, I will highlight how HITRUST helps elevate the industry's cyber awareness, improve cyber preparedness and strengthen the risk management posture of the healthcare industry. In particular, I will explain how programs like cyber information sharing, cyber threat catalogues and guidance on implementing the NIST Cybersecurity Framework[1] are integral to this process, as is the role for the Department of Homeland Security.

In 2012, HITRUST established the HITRUST Cyber Threat XChange or CTX, the health industry's Information Sharing and Analysis Organization, or ISAO. The HITRUST CTX has consistently and effectively enabled cyber information sharing across the entire industry and with government, while continuously evaluating and enhancing its services to ensure better collection, analysis and consumption of actionable cyber threat information.

At today's hearing, I would like to highlight three programs we have pioneered with industry that showcase the positive efforts underway in collaboration with DHS and then speak to our concerns over government's interference, underperformance or disregard as to the industry's cyber security efforts. Concerns, I anticipate this Committee and the new administration will share and appropriately address.

[1] https://www.us-cert.gov/ccubedvp

The first of the programs is the Enhanced Indicator of Compromise (IOC) Program; second, is Sector Guidance for Implementing the NIST Cybersecurity Framework; and third, is Automated Indicator Sharing with DHS. I will touch on each one of these briefly.

1. *Enhanced Indicator of Compromise (IOC) Program*

Since it began an IOC sharing program over six years ago, HITRUST has been a leader in information sharing and continuously evaluates the effectiveness of its cyber information sharing program against stated goals. A review in 2015 highlighted a number of gaps and deficiencies in our cyber information sharing approaches, and led to the development of an Enhanced IOC criteria to improve the collection and sharing of IOCs and maximize its benefits. These criteria defined specific requirements in terms of completeness, timeliness and accuracy of IOCs contributed. We then established a pilot to evaluate the effectiveness of this approach, which demonstrated significant improvements, highlighted in the findings below:

1. During the pilot period, over 80% of the IOCs collected were unique and not seen or known by any other open source, commercial, DHS CISCP, or user contributed feeds available to the HITRUST CTX.
2. The pilot group of eight organizations using Enhanced IOC sharing reported 45% more IOCs than a comparable group of over 800 existing CTX participants using current sharing practices.
3. 100% of organizations reported IOCs to the HITRUST CTX compared to only a small percentage of organizations – 5% – that contributed using current sharing practices during the same period.
4. IOCs were reported to the HITRUST CTX on average 13.1 days before being seen or identified by any other open source, commercial, DHS CISCP, or user contributed feeds to the HITRUST CTX. Some indicators were seen in the pilot program up to 123 days before being reported by other feeds.
5. IOCs were submitted in a matter of minutes to the HITRUST CTX compared to an average of seven weeks after detection using current sharing practices.
6. 95% of the IOCs contributed to the HITRUST CTX had metadata (e.g., malicious IPs, URLs or domains) that made them actionable for use by others, which is defined as being useful in allowing preventative or defensive action to be taken without a significant risk of a false positive. Using current sharing practices, only 50% of the IOCs contributed to the HITRUST CTX were considered actionable.

The net result is that the HITRUST CTX continues to improve on the number of unique IOCs it shares across healthcare organizations each month – going from 186 unique IOCs in September 2015 to 5,158 in September 2016.

In addition, the enhanced IOC pilot improved situational awareness and predictive threat modeling with the ability to correlate IOCs and Indicators of Attack (IOAs) between organizations, identify attack patterns, and alert participants about IOCs and IOAs. These

results are positive with regards to mitigating cyber risk, but don't speak to the investment required.

To better understand the return on investment, HITRUST is undertaking a study to quantify the value of information sharing as a tool in mitigating cyber risk, to aid organizations in prioritizing and justifying their participation. We are undertaking an ROI study to evaluate information sharing and the incremental benefits of leveraging the Enhanced IOC criteria. We look forward to updating the Committee on the results of this study in the near future.

Another important finding is that threat information sharing does not need to be limited to the largest organizations and that the scalable sharing of IOCs can be achieved throughout healthcare organizations of varying size, intelligence appetite, and the maturity of an organization's security program. This was evaluated by integrating the HITRUST CTX with the CyberAid program[2].

The results of the Enhanced IOC Collection Pilot indicate that healthcare organizations can dramatically improve the timeliness, completeness, usability and volume of IOCs contributed to the HITRUST CTX by implementing the enhanced IOC criteria. In response to these findings, HITRUST is expanding the Enhanced IOC program and announced enhancements to the CTX platform to aid organizations in reducing their cyber risk.

I reference this program to illustrate that the private sector is willing to do its part in facilitating the collection and dissemination of IOCs and other cyber threat information (CTI), and sees DHS as having a vital role in facilitating the collection and dissemination from other information sharing organizations in a streamlined and efficient manner.

2. Sector Guidance for Implementing the NIST Cybersecurity Framework

Last year, the Health and Public Health Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), along 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 "*Healthcare Sector Cybersecurity Framework Implementation Guide*".

The Sector Guide supports implementation of a sound cybersecurity program that addresses the five core function areas of the NIST 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.

[2] HITRUST CyberAid is an example of enabling information sharing with smaller organizations - https://hitrustalliance.net/documents/cyberaid/CyberAidInfographicPresentation.pdf

DHS was an integral partner and commenter during the development of the Sector Guide. The HPH SCC, which was formed under the DHS Critical Infrastructure Sector Partnership Program, is an example of industry innovation, leadership and collaboration across the entire industry on a number of topics relevant to the protection of critical infrastructure including cyber.

3. Automated Indicator Sharing (AIS)

The HITRUST CTX is fully integrated with AIS and supports bi-directional cyber threat indicator exchange to better aid organizations in reducing their cyber risk. In fact, HITRUST was the first non-government entity connected to and sharing cyber threat indicators with the DHS AIS Program.

AIS has the potential to facilitate the sharing of crucial cyber threat information from across organizations, corporations and federal agencies in real time. Given the recent rise in cyber threats targeting the healthcare industry, HITRUST believes bi-directional integration into the AIS program will ensure relevant and timely CTI from HITRUST and government is available to all industries – ultimately bolstering the overall cyber posture of the nation's critical infrastructure.

Of note, HITRUST's role as an ISAO with strong industry engagement enabled us to quickly and efficiently address any concerns regarding the liability of sharing with government. It was also our continued evaluation and enhancements to our infrastructure with our technology partners that enabled us to integrate with AIS and meet the future needs of information sharing. Both the Cybersecurity Act of 2015 (CISA) and Executive Order (EO) 13691 intended ISAOs to take up this role in an effort to help move the private sector in the right direction and enable them to robustly engage with government. AIS integration demonstrates that HITRUST, with its DHS partnership, continues to evolve, improve, and lead by innovating and ensuring cyber threat information sharing is providing the most value to the broadest group of constituents while reducing overall cyber risk.

As a non-governmental organization, sharing with AIS was not without initial challenges, we did encounter some technical and operational issues. They have since been addressed, but we would encourage greater engagement by DHS with AIS participants to ensure alignment with ongoing and future requirements.

HITRUST is of the opinion that DHS—acting as the hub for cyber information sharing—benefits the entire industry, and our engagement with the DHS AIS has been both cooperative and very productive.

However, despite all the progress the public and private sectors have made in recent years, as I referenced earlier, there are government efforts underway to undermine private-sector information sharing programs and ISAOs like that of HITRUST. Even though CISA and the EO make clear that ISAOs would be established and enable private companies to decide which ISAO to engage when sharing with DHS, there are efforts underway that will deviate from this effort by requiring healthcare organizations to only share information directly with the Department of

Health and Human Services—an agency not even identified in CISA as affording safe harbor liability protections.

This is certainly troublesome, as we can all agree that CISA placed DHS at the center of information sharing with the private and civilian sector. HITRUST supported this effort enthusiastically and continues to do so. In fact, as we have outlined in our testimony, we have invested heavily in elevating our information sharing capabilities to help industry achieve the goal of working collaboratively with the government.

Since HITRUST has led the industry in the collection of IOCs through the development of enhanced standards and collection practices, and was the first healthcare organization to begin sharing bi-directionally with DHS's AIS program, we find these efforts unnerving as they are certainly contrary to the original intent of CISA and government's commitment to partner with industry through the ISAO program.

HITRUST has always approached its role as an ISAO with the entrepreneurial spirit of innovation and leadership. While we recognize that there is a large role for government to play in supporting information sharing and ensuring liability protection, the private sector should be considered an equal partner, and our government partners should take a universal and consistent approach when engaging with industry.

We appreciate and recognize that each industry has unique dynamics and challenges with regards to CTI sharing, in healthcare they include organizational size, technical maturity, medical devices and other control systems, but that doesn't warrant interjecting another intermediary and certainly not one that regulates and has responsibility for fines and other financial penalties.

HITRUST was an early supporter of CISA and continues to support the role of government to foster transparency by establishing guidance, clarifying roles and responsibilities, and encouraging industries and segments to determine how to engage more extensively based on their value and performance. The market should drive innovation and government should promote the role of industry without changing the rules. We are seeing the opposite occur, and this was never the intent of CISA or the Executive Order. CISA established a role for the private sector around cyber information sharing, a role for ISAOs and associated liability protections offered through DHS. Unfortunately after supporting, committing and engaging along that path, we find the Department of Health and Human Services establishing guidelines and approaches that are inconsistent and without appropriate consideration and recognition of industry activities in support of CISA and the Executive Order.

HITRUST, through its many programs, remains committed to ensuring the healthcare industry can properly address these challenges. Cyber information sharing is, and will continue to be, a key component in HITRUST's approach to cybersecurity and cyber risk management, and we are excited about pioneering these approaches. Information sharing is only one tool that impacts risk management for an organization. HITRUST continues to develop innovations such as the *Healthcare Sector Cybersecurity Framework Implementation Guide*, and enhance its security and privacy framework and assurance programs. We value the partnership of DHS in these efforts and look forward to their continued support.

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