Testimony of Dan Nutkis
CEO of HITRUST Alliance

Before the Oversight and Government Reform Committee,
Subcommittee on Information Technology

Hearing entitled: "Cybersecurity: The Evolving Nature of Cyber Threats Facing the Private Sector"
March 18, 2015

Prepared for Submission

Chairman Hurd, Ranking Member Kelly, and distinguished Members of the Subcommittee, I am pleased to appear today to discuss the role HITRUST plays to address persistent and emerging cyber threats to healthcare. I am Daniel Nutkis, CEO and founder of the Health Information Trust Alliance or HITRUST. I founded HITRUST in 2007, after recognizing the need to formally and collaboratively address information security for healthcare stakeholders from all segments of industry, insurers, providers, pharmacies, PBMs and manufacturers. HITRUST endeavored to elevate the level of information protection in the healthcare industry—ensuring greater collaboration between industry and government, and raising the competency level of information security professionals.

With regards to aiding industry in cyber risk management, threat preparedness and response, HITRUST has implemented numerous programs in coordination with industry stakeholders. The HITRUST CSF, is a scalable, prescriptive and certifiable risk-based framework relating to information security tailored to the healthcare industry. Over 84 percent of hospitals and health plans, as well as many other healthcare organizations and business associates, have adopted the CSF, making it the most widely adopted security framework in healthcare.

In 2008 and five years prior to the issuance of Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" issued by the President on February 12, 2013 and before the NIST published its Cyber Security Framework, HITRUST published the first volume of the CSF and had already identified information protection controls relating to cyber security and issued guidance to the healthcare industry. The CSF is continuously updated to ensure relevance, such as incorporating the NIST Cyber Security Framework and providing health industry implementation guidance as well as privacy controls.

The HITRUST CSF Assurance Program delivers simplified compliance assessment and reporting for HIPAA, HITECH, state, and business associate requirements. Leveraging the CSF, the program provides healthcare organizations and their business associates with a common approach to manage security assessments that creates efficiencies and contains costs associated with multiple and varied assurance requirements. The CSF Assurance Program includes the risk management oversight and assessment methodology governed by HITRUST and designed for the unique regulatory and business needs of the healthcare industry.

Additionally, MyCSF is a full-featured, user-friendly, fully-integrated and managed tool that streamlines the entire information compliance and risk management process, from policy creation, approval and publication to risk assessment and remediation. The optimized and powerful tool marries the content and methodologies of the CSF and CSF Assurance Program with the technology and capabilities of a governance, risk and compliance (GRC) tool.

In 2012, after identifying the need for coordination among stakeholders, particularly leveraging the expertise of more cyber-sophisticated organizations to assist less sophisticated players, HITRUST launched the Cyber Threat Intelligence and Incident Coordination Center (C^3) to provide threat intelligence, coordinated incident response and knowledge transfer specific to cyber threats pertinent to the healthcare industry. The C^3 facilitates the early identification of cyber-attacks and creation of best practices specific to the healthcare environment and maintains a conduit through the Department of Homeland Security (DHS) to the broader cyber-intelligence community for analysis support and exchange of threat intelligence. The Center was also the first to track vulnerabilities related to medical devices and electronic health record systems, which are both emerging areas of concern.

The HITRUST Cyber Threat XChange (CTX) was created to significantly accelerate the detection of and response to cyber threat indicators targeted at the healthcare industry. HITRUST CTX automates the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable formats (e.g. STIX, TAXII and proprietary SIEM formats) that organizations of almost all sizes and cyber security maturity can utilize to improve their cyber defenses. HITRUST CTX will act as an advanced early warning system as cyber threats are perpetrated on the industry. CTX is now offered free of charge to the public and has gained wide acceptance within healthcare.

Additionally, HITRUST developed CyberRX, now in its second year, which is a series of industry-wide exercises developed by HITRUST and the Department of Health and Human Services (HHS), to simulate cyber-attacks on healthcare organizations in order to evaluate the industry's response and threat preparedness against attacks and attempts to disrupt U.S. healthcare industry operations. These exercises examine both broad and segment-specific scenarios targeting information systems, medical devices, and other essential technology resources of the Health and Public Health Sector. CyberRX findings are analyzed and used to identify areas for improvement for industry, government and HITRUST C^3 and understand what improvements are needed to enhance information sharing between healthcare organizations, C^3, and government agencies.

Finally, HITRUST and HHS coordinate a monthly Health Industry Monthly Cyber Threat Briefing – which is open to the public – that provides timely insights on emerging cyber threats and countermeasures. HITRUST is also an active participant on the Health Sector Coordinating Council (SCC) and provides a monthly cyber threat briefings to the SCC.

HITRUST is also a federally recognized information sharing and analysis organization (ISAO), has strong relationships with HHS, DHS and the Federal Bureau of Investigation (FBI) and considers them integral partners to elevate the threat landscape facing healthcare today and strengthen the continuum of care.

In my testimony today, I would like to highlight how HITRUST helps elevate the cyber awareness, preparedness and response of the healthcare industry. Growing cyber threats are an increasing risk to not just all areas of critical infrastructure; but healthcare specifically. Increasingly, private sector networks are experiencing nation-state cyber activity similar to that seen on Federal networks. In addition to targeting government networks, there is a growing threat of nation-states targeting and compromising critical infrastructure networks and systems. Healthcare is no exception and is not immune from such threats.

Mitigating the risks associated with cyber threats and attacks requires a comprehensive approach including implementing strong security controls, monitoring control effectiveness, and testing preparedness and response. Commonly applied, "network hygiene" only covers the blocking and tackling. While there is not a perfect solution to information security; the best strategy is to prevent, detect and respond, before the adversary achieves his objective. Strategically, information sharing is designed to assist with this; however, information sharing is a predominantly reactive approach and also dependent on

the maturity of the industry. Since this is something we have been struggling with in healthcare, HITRUST is exploring new approachs to take information sharing to the next level by identifying the exploits that are "in the wild" and tracking how they are impact applications and implemented security products. We have named our new approach, CyberVision. While it is in the pilot stage, it is gaining increased attention and we look forward to the opportunity to continue to update the Committee on our progress.

We believe an approach like CyberVision transforms cyber risk management and is so important at this stage because we need to move all areas of critical infrastructure from a posture of being reactive to proactive. If healthcare can inform the overall proactive information sharing approach then we are eager to tackle this challenge head on. While threat intelligence can help defenders more quickly identify and respond to intrusions, this information only helps if the organization is postured to succeed. Until one invests in sound strategy, processes, people and technology, no amount of information sharing or threat intelligence will be sufficient. CyberVision is one way HITRUST is elevating the strategy, people and technology so that organizations can focus their resources where it counts.

Since 2007, HITRUST has endeavored to elevate the level of information protection by ensuring greater collaboration between industry and government, and raising the competency level of information security professionals across the healthcare industry. We have tremendous experience as a federally recognized ISAO and have many valuable lessons to share. In the past, there has been some confusion on who in the private sector companies can turn to in order to work with their government partners. HITRUST is determined to be the focal link that will continue to provide value to strengthen our government, our economy, and our nation as a whole given the growing cyber threats the nation faces.

HITRUST, as the healthcare industry's largest and leading ISAO, has taken a holistic approach to threat intelligence sharing and cybersecurity from the beginning with the HITRUST C3 program, the CTX, the Monthly Threat Briefings, and the CyberRX attack simulation exercises. HITRUST is also a leader in education and outreach. HITRUST's CSF incorporates the NIST cyber security framework to ensure the CSF is the healthcare sector's premier framework and also an example for other sectors given its rigorous privacy controls.

In the wake of the recent Anthem breach, the industry was able to experience the effectiveness of information sharing as HITRUST was able to share Indicators of Compromise (IOCs) with the healthcare industry within one hour after Anthem

posted them to the HITRUST CTX. In addition they were shared with HHS, DHS and U.S. CERT who shared the IOCs with other industry ISAOs.

In conclusion, I would like to discuss several challenges the industry faces. There is certainly a maturity problem in every industry but especially in healthcare. The industry struggles with the fact that regulators do not acknowledge companies that invest and demonstrate security maturity above the industry standard. Specifically, industry is seeking ways to demonstrate that such investments receive appropriate recognition and provide safe harbor from regulators and claims of negligence. We would like such efforts and evidence of program effectiveness to be accepted by regulators including the HHS's Office of Civil Rights and the Federal Trade Commission. The CSF is one such area of effectiveness that has wide industry support and adoption.

The industry seeks to be at the forefront of intelligence sharing and cyber collaboration with the Federal Government. Evidence gathered from the CTX and other threat streams demonstrate the growing interest in our industry by nation-state actors which introduces attack scenarios that even the best companies will have a difficult time preventing. The standard needed to resist such efforts is perfection which is very difficult to sustain. Our industry is required to maintain some of the most sensitive information available on Americans. Each dollar spent responding to an attack siphons money from the healthcare delivery system of our country. Consumer confidence is a critical component of our ability to electronically engage consumers in proactive health management and disease intervention measures. Fear of engaging with the health system can only impact the well-being of our population over time. HITRUST, through its many tools and programs seeks to ensure that the healthcare system can properly address this challenge and we stand as a leader in this endeavor.

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

Daniel Nutkis

Chief Executive Officer

Daniel Nutkis is the founder and Chief Executive Officer for HITRUST. Mr. Nutkis has more than 20 years of experience in providing strategic advisory services in areas relating to health information technology. His recent focus has been on technologies that enable information protection and strategic business objectives. Prior to founding HITRUST, he held various positions with email encryption and e-prescribing service company Zix Corporation (NASDAQ: ZIXI), including Executive Vice President, Strategy, and President, Care Delivery. He was also with Ernst & Young LLP's healthcare emerging technology groups as National Director. He has led a number of industry research activities on eHealth vulnerabilities and has been a founding member of work groups and accreditations such as WEDI, CPRI and HISPP. Dan has also been recently recognized as a top information security influencer in 2014 by SC Magazine, and in 2015 by Health Information Security Magazine.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: **Daniel Nutkis**

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

None

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

Health Information Trust Alliance (HITRUST), Chief Executive Officer

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

None

I certify that the above information is true and correct.
Signature: Date: March 2, 2015