Written Testimony of

Michael H. McMillan

Chairman & CEO, CynergisTek, Inc.

Before The

Subcommittee on Health

Committee on Energy and Commerce

U.S. House of Representatives

Examining Cybersecurity Responsibilities at HHS

May 25, 2016

Chairman Pitts, Vice Chairman Guthrie, Ranking Member Green and members of the Health subcommittee, thank you for the opportunity to testify today on this important initiative. I am Mac McMillan, CEO of CynergisTek, Inc., a firm that has specialized in providing Privacy and Security services to the healthcare industry since its inception in 2004, and I am pleased to be able to offer testimony in support of HR 5068, HHS Data Protection Act. I believe my experiences as the former Head of Security for the On-Site Inspection Agency and Defense Threat Reduction Agency as well as my experiences from the past fifteen years providing security services to the healthcare industry have provided me with some unique and valuable insights on this matter. I have served in information security roles of one type or another since 1982 when I first became an Intelligence Officer in the U.S. Marine Corps and was given responsibility for managing the Battalion's classified information. In every role I have had since the protection of information systems and data has been a core component of my responsibilities. I sincerely support the elevation of the

Chief Information Security Officer (CISO) role to a position equivalent to other senior leaders within the Department of Health & Human Services (HHS) and in particular the Chief Information Officer (CIO). When these two positions have equal authority, are both focused on a common mission and working collaboratively the CIO and CISO form a complementary and effective team to ensure the protection of information assets for an organization. When there is disparity in these relationships there is opportunity for conflicts of interest to arise, stifled or abbreviated discussion of risk and an imbalance of priority. One of the most often questions I get asked by healthcare leadership and Boards is, "where should the CISO report?' I welcome the opportunity to engage the members on this matter.

Healthcare Needs Better Security

Cybersecurity is far and away one of the most critical issues for any industry today, but in particular for healthcare which has emerged as a popular target for cyber criminals, hactivists and state actors engaged in cyber theft, extortion and high stakes espionage. Since 2009 when the HITECH Act was passed and healthcare embarked on the wide scale digitization of patient information there has been an associated and steady increase in the number of cyber incidents in healthcare. The criminal community has perfected its ability to monetize stolen information and has created an elaborate darknet marketplace for buying and selling hacking services, techniques, knowledge, tools and the information itself. Healthcare is particularly lucrative to attack because unlike other industries it presents an rare opportunity to steal all forms of sensitive personal information; medical information, personal information and financial information, all in a single attack. At the same time the healthcare computing environment represents one of the most complex and difficult to secure. Multiple initiatives that seek to improve healthcare such as Health Information Exchanges, Accountable Care Organizations, Population Health, TeleHealth, networked medical devices, cloud services, big data, etc. also introduce greater challenges in securing information because it seeks to share it more broadly than ever before. Add to this the shear number of individuals accessing and handling health information and its easy to see that any CISO, let alone one in an organization as large and complex as HHS, has a full time job just attempting to stay abreast of the many cyber challenges that leadership need to be aware of. Security is best achieved as a top down priority, with strong visible leadership, disciplined practices and constant reevaluation. What most healthcare organizations suffer from most today is a lack of leadership. This resolution seeks to address that situation by creating a cyber security leadership post within HHS by elevating the CISO position.

Security As A Top Down Priority

Security programs are most successful when they are articulated from the top as an organizational or core mission priority, when there is visibility to the program, when risk is openly communicated and debated and when every member of the organization intuitively understands that security is a part of his or her role. In the Department of Defense where I had the honor to serve for more than twenty years security is second nature and understood from the most junior service member or civil servant to the Generals and Senior Executives who lead our military services and agencies. In each service and agency there is a senior security official who is a full member of the executive staff with responsibility for ensuring the protection of organizational personnel, assets, information and operations. That individual, like his or her counterparts has a responsibility to the Agency Director or Service Chief of Staff and to the broader protection of our National Security. From my earliest assignment as a Marine Battalion S-2 and Information Security Officer to my position as the Chief of Security for both the On-Site Inspection Agency and the Defense Threat Reduction Agency I understood that I had a responsibility to ensure the protection of information assets, to constantly assess the risk and to advise leadership on the right course of action to mitigate the threat. At both OSIA and DTRA we had formal accreditation standards for information systems and sensitive information. The CIO was primarily responsible for procuring, developing, implementing and managing information networks and systems in support of the Agency's mission. My responsibility was to review, test, accredit and monitor those information networks and systems to ensure they adequately protected the sensitive information they processed, stored or transmitted. Both the CIO and I were peers and were expected to work collaboratively to meet the Agency's mission as well as the mandate of National Security. The Director of the Agency communicated that information security was a priority for every member of the Agency and there were well defined policies, procedures and processes that both governed and guided our decisions and actions. When new systems or services were contemplated or introduced it was necessary for security to approve them before they could be made operational. This leveling of the playing field between the CIO and I resulted in a very collaborative environment because neither of us wanted to see something held up unnecessarily and both of us had a vested interest in deploying secure systems. So early on in projects our teams collaborated. This effectively streamlined review and testing times down the line and identified issues early so they could be resolved before they impacted accreditation. When I had a concern I could address it to the senior staff and the Director. Likewise my counterpart the CIO could also make his argument when he felt security was too restrictive or impacting productivity. Leadership then had the ability to make informed decisions based on the merits of both our arguments.

The Importance of Cyber Security Competence

The cyber security challenges that CISOs face today are more daunting than they have ever been, and by many estimates are expected to grow. In the last eighteen months in particular we have seen incredible sprints in cyber criminal activity. According to Symantec, a leading information security firm that monitors networks worldwide, in 2015 they discovered more than 430 million new unique pieces of malware, a 36% increase from the year before. Ransomware, a single variant of malware, attacks increased from roughly 3000 a month to 4000 a day from December of 2015 to March of 2016. There were 54 zero day vulnerabilities identified or roughly one a week in 2015. A zero day vulnerability being one that we have no knowledge of or defense for until after it is launched. Virtually every aspect of the health information ecosystem has been attacked from its databases, to its applications, to its use of social media, to its mobile devices to the Internet of Things and its people. What is at stake in healthcare goes far beyond protecting privacy to assuring patient care and safety. Most processes in healthcare today are automated and have been now for more than a decade, long enough that many new comers to health care do not remember a day when they did not have a device in their hand or a computer guiding what they do. Malware that disrupts access to or the use of healthcare systems and data can create real operational, safety and security concerns. The public learned this first hand when several health systems, Hollywood Presbyterian in California, Hurley Medical in Michigan, Methodist Hospital in Kentucky and Titus Regional in Texas, to name a few, had to turn away patients because they could no longer provide care due to cyber attacks. We also saw massive breaches of health information in attacks against large health care insurers and even government databases like the OPM breach. HHS as the home to Medicare and Medicaid, Healthcare.gov, and many other important programs is responsible for handling health information on millions of U.S. citizens. The Department interfaces and communicates electronically with healthcare organizations across the nation. The scope and breadth of the responsibility of the HHS CISO as a member of the larger healthcare information universe demands a highly qualified and competent individual who can advise the Secretary and other senior members of HHS on cyber security matters.

Conclusion

Members of the subcommittee, I am appreciative of the opportunity to testify on behalf of this initiative to elevate the CISO role within the structure of HHS. As an individual who has filled similar roles during my career and advised many others I understand first hand how important it is to have the authority and the visibility necessary to ensure that the voice of security is heard and considered. Healthcare has been characterized as being a soft target for cyber criminals. While the industry has made considerable strides since 2005 I agree that we are still significantly behind where we need to be. Many of the challenges we face include the lack of a credible framework for cyber security, lack of standards for medical devices and a lack of resources and investment in security technologies, to name some. HHS can provide leadership in solving some of these challenges. I believe that the right individual given appropriate authority and resources can and will improve the security posture at HHS and also serve as an industry leader at a time when it is needed most.