Written Testimony of

Terence M. Rice

On Behalf of

Merck & Co., Inc.

Before the

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

April 4, 2017

INTRODUCTION

Chairman Murphy, Ranking Member DeGette, and Members of the Oversight and Investigations Subcommittee, my name is Terry Rice. I have been involved in healthcare cybersecurity for more than fifteen years in a wide variety of roles including my current assignment as the Vice President and Chief Information Security Officer (CISO) at Merck & Co., Inc. I also participate in a number of public-private partnerships that are working to improve cybersecurity across the healthcare sector. These partnerships include the National Health-Information Sharing and Analysis Center (NH-ISAC), the Healthcare Sector Coordinating Council (SCC), the SAFE BioPharma Association, and the Healthcare Industry Cybsecurity Task Force, the latter of which was created by the Cybersecurity Information Sharing Act of 2015. I appreciate the opportunity to testify before you on the topic of cybersecurity in the healthcare industry and to discuss how public-private partnerships have assisted and can do even more to address the complex challenges we are facing.

THE STATE OF HEALTHCARE CYBERSECURITY

Cybersecurity has rapidly become a top concern for governments and industries around the world. In just the last four years, cybersecurity has jumped from the fifteenth greatest risk facing companies to the third highest risk in the Allianz Annual Risk Barometer, a global survey that measures the sentiments of corporate risk professionals.[i] Cybersecurity has also been listed as a top concern by many national governments and has been included as a top risk in the US Intelligence Community's annual Worldwide Threat Assessment since at least 2013.[ii] Nowhere is the situation more acute than in the healthcare industry. In just the last few years we have seen over one hundred million health records exposed in a number of well-publicized security breaches, we have observed cybersecurity researchers demonstrate how software vulnerabilities in insulin pumps and pacemakers could be exploited to cause a lethal attack, and we have witnessed entire hospitals in the United States and the United Kingdom shutting down for periods of time to combat a ransomware infection on critical systems. It is because of these events and many others that IBM named the healthcare industry as the most attacked industry in its 2016 IBM Cyber Security Intelligence Index.[iii]

Unfortunately, I believe the news stories and reports underrepresent the risk we are facing as an industry. I make this statement based on five observations:

1. The total number of cybersecurity incidents is significantly underreported. Today, organizations are only required to report cybersecurity incidents when a) personal health information is breached, b) the incident directly impacts patient safety, or c) the loss of information or disruption of service would be considered a financially material event[iv]. Organizations are unlikely to report security incidents if not required to do so given the potential reputational harm that might occur. The reports we read about are only a small fraction of the incidents that actually occur. Furthermore, the incidents that do get reported (e.g. breaches of personal health information) also create a narrow focus on privacy protections for personal health information instead of considering the full spectrum of impacts caused by healthcare cyber incidents.
2. The healthcare industry consists of many small to mid-sized businesses that lack the capital and personnel to deal effectively with all but the most basic cybersecurity issues. According to one statistic, more than 90% of firms in the healthcare services subsector employ less than 100 people and about 70% of these firms employ less than 10 employees.[v] To complicate this, the healthcare services and hospital subsectors have some of the lowest profit margins across industry.[vi] These two factors make it difficult

for these firms to acquire the advanced tools and services necessary to prevent, or at least detect, sophisticated attacks. These small to mid-sized firms often face the difficult choice of investing in the latest cybersecurity tool or purchasing a crucial medical system. More often than not the latter will win. Even if these entities are able to make the capital investments required, they are almost always unable to acquire the talent necessary to install, operate, and maintain these capabilities and develop a broader cybersecurity program.

3. The portability of healthcare information increases the risk. Unlike other industries, the healthcare industry requires information to be shared among multiple companies to provide patient care. Primary care physicians must share data with specialists, specialists must share data with labs, labs provide information to pharmacies and pharmaceutical benefits managers, and all of them share subsets of this data with insurance companies. To facilitate this information sharing, most of these entities interconnect their networks and systems. Consequently, a failure anywhere in the ecosystem may lead to impacts across the sector.
4. Proliferation of software into the healthcare ecosystem increases the attack surface. The healthcare industry was somewhat of a laggard in the adoption of software services and solutions. The Health Information Technology for Economic and Clinical Health (HITECH) provisions of the American Recovery and Reinvestment Act of 2009 provided both incentives and penalties to increase the adoption of electronic health records. This rapid adoption of electronic health record technology has spurred the development of new software solutions and services that can create, input, and analyze patient health information. While these advances offer tremendous potential healthcare benefits and

may help to reduce cost across the industry, we are rapidly increasing the cyber attack surface in the healthcare sector. The risk is exacerbated by the fact that software developers have not yet come up with a way to prevent errors and mistakes in the software they create. In fact, computer programmers continue to make many of the same mistakes in their code that were made 15-20 years ago. Today we measure software errors in the number of defects per thousand lines of code; many of medical applications being developed contain millions if not tens of millions of lines of software code. We will be dealing with these inadvertent flaws for a decade or more from now. So we must account for this with additional preventative and detective controls.

5. Anecdotal electronic evidence also suggests there are a lot more security incidents than what is currently reported. As part of normal information security monitoring, it is quite common to find information about other companies that have been attacked or even compromised. These indicators might be something as simple as malware traffic emanating from a partner's network or the observation of another company's name showing up in a data dump released by an attacker. In fact, there are web services like Shodan that specialize in identifying and cataloging vulnerable systems and devices including many from the healthcare industry in an easily searchable web interface.

When all of these observations are combined, it leads me, and many of my peers, to believe that the cybersecurity situation in the healthcare industry is far worse than what public reporting indicates. Neither private industry nor the government can solve this problem alone; we must work collaboratively and transparently to reduce this risk.

THE VALUE OF PUBLIC-PRIVATE PARTNERSHIPS IN CYBERSECURITY

The notion of public – private partnerships for cybersecurity first gained traction in 1997 following the publication of recommendations from the President's Commission on Critical Infrastructure Protection. These recommendations were codified in Presidential Decision Directive/NSC 63- Critical Infrastructure Protection which specified the industry segments that should be considered critical infrastructure, appointed a sector specific agency to coordinate the public-private partnership, and identified ten tasks that should be accomplished by each sector. A Government Coordinating Council and Sector Coordinating Council were created to represent the myriad of government departments/agencies and private sector participants respectively. The tasks included an assessment of threats and vulnerabilities that might impact the sector, the development of a sector-wide remediation/protection plan, and the sharing of intelligence information between the government and private sector. Although subsequent administrations have tweaked the industries and functions that make up the critical infrastructure and have made minor modifications to the tasks on which each sector should focus, by and large there has been support for the concept for two decades.

The healthcare and public health sector has been designated a part of the critical infrastructure since PDD-63. The Department of Health and Human Services (HHS) has been the sector specific agency since that time. However, it is only in recent years that the topic of cybersecurity has become a prominent issue. The Sector Coordinating Council now devotes a regular portion of its meetings and monthly teleconferences to discussing developments in the cybersecurity space and has established working groups to tackle items of common interest among the members. The NH-ISAC, created in 2010, has grown from about a dozen original members to more than 200 participating companies and it continues to attract more and more of the thousands of healthcare entities that exist in the United States. More importantly the quantity and quality of actionable intelligence shared by members has increased substantially in the last 12-18 months. The NH-ISAC has stood up working groups that work collaboratively to identify new sources of threat intelligence and ways to disseminate to all parties in the most effective manner, and to collaborate on ways to more effectively secure "big data" within the healthcare industry, but both organizations have the potential to do even more.

At the same time, other public-private partnerships have grown out of a desire to reduce the cost and complexity of business. The SAFE BioPharma Association was founded more than a decade ago out of a shared desire between the government and private industry to reduce the cost and complexity of submitting new drug applications to the Food and Drug Administration (FDA). In order to move away from paper-based submissions, all parties needed to agree on a mechanism that would ensure data integrity, provide for non-repudiation, and ensure trust in the identity of the signer. The members of SAFE BioPharma worked closely with the FDA, the National Institute for Standards and Technology (NIST), the General Services Administration (GSA), and regulators in the European Union and Japan to create a digital identity and digital signature standard that today is accepted by all parties. The standard creates an interoperable digital identity ecosystem in which all identities can be trusted at known risk-levels. It allows government agencies and private sector healthcare providers to have standardized trust for authentication and signing. Vendors have a tool for standardizing trust in their products and applications and the user can have a single identity for use across the ecosystem. The standard has been certified to meet US government federal identity standards[vii] and is used on electronic submissions, contracts, and other critical workflows that require integrity, identity trust, and non-repudiation around the world. More importantly, the industry has recently started adopting this digital identity standard for authentication purposes, much in the manner the US Federal Government rapidly adopted the use of Personal Identity Verification (PIV) cards for strong authentication following the Office of Personal Management (OPM) breach. According to Verizon's 2016 Healthcare Data Breach Report[viii], two out of every three healthcare data breaches have been caused by hijacked user names and passwords. SAFE BioPharma members hope to increase the use of standards-based authentication credentials across the healthcare industry. Particular emphasis is being placed on multi-factor authentication capabilities across the healthcare industry using the SAFE BioPharma standard and other recognized standards that meet the same level of security – all based on NIST and GSA standards.

As a participant and user of services provided by all three public-private partnerships, I feel each provides tremendous value and has become an essential part of my organization's cybersecurity program. We leverage the intelligence provided by the NH-ISAC to update our defenses on a continuous, 24x7 basis, we use the NH-ISAC's benchmarking service to identify areas in where we may learn from our peers, we leverage SAFE BioPharma compliant digital identities in collaborating with peer organizations, and we actively participated in the recent DHS Cyberstorm table top exercise. But there are many opportunities to further mature and develop these capabilities.

OPPORTUNITIES FOR FURTHER PARTNERSHIP AND COLLABORATION

1. **Appoint a Healthcare Sector Cybersecurity Liaison**. HHS should appoint a senior cybersecurity professional as a liaison to the private sector. Today the Assistant Secretary for Preparedness and Response (ASPR) has the responsibility for ensuring the healthcare sector is prepared to respond to a critical health emergency such as a pandemic flu outbreak or the disruption of critical health infrastructure from a natural disaster as occurred in New

Orleans during Hurricane Katrina. The Office of National Coordinator (ONC) has a Chief Privacy Officer who, along with the HHS Office of Civil Rights (OCR), works with the private sector on privacy policies and implements enforcement actions when necessary. HHS also has a Chief Information Security Officer (CISO) within the Office of the Chief Information Officer (CIO) who is primarily responsible for protection of HHS systems and services. All four of these offices interact with the private sector but none of them have cybersecurity outreach as their primary mission. A cybersecurity liaison would be the primary focal point for outreach to the private industry on topics of cybersecurity. The role would not supplant current responsibilities, but instead focus on education and awareness of cybersecurity risks within the sector, advocacy for the use of cybersecurity tools and capabilities provided by the Department of Homeland Security (DHS), and collection of key issues from the sector. The liaison would also chair a GCC working group on cybersecurity that would work closely with the Sector Coordinating Council equivalent.

2. **Develop Cybersecurity Appendix to Healthcare & Public Sector Specific Plan**. While cybersecurity concerns were captured in the latest iteration of the Healthcare and Public Health Sector Specific Plan - May 2016[ix], a more thorough and detailed appendix should be added to the existing plan to better assist public and private sector entities in developing their own cybersecurity incident response plans. This appendix should include templates and guidelines to help smaller and less mature organizations create at least a rudimentary cybersecurity response plan.
3. **Increase the Quality of Cybersecurity Intelligence and the Speed with Which It is Shared.** While there has been a significant increase in the quantity and timeliness of information shared by government agencies via DHS over the last 24 months, there is still

opportunity to improve both the quality of information and speed at which it is shared. Cybersecurity defenders need to respond to threats in minutes, if not seconds. Waiting days or even weeks for information to be shared diminishes the value of the information. For example, if an entity discovers a sophisticated phishing email that has been able to bypass an organization's email filters, it is critical that information on the subject line, sender's address, and other data about the message be sent out to others as quickly as possible so that the other security teams can search for and delete these messages before their users fall victim to an attack. Today, members of the NH-ISAC are sharing this type of information in near real-time. We still need to increase the percentage of members willing to share but we also need the government to share healthcare related cyber intelligence at similar speeds. Ultimately, we need to automate the entire process to minimize any delays in responding to rapidly changing threats.

4. **Facilitate Healthcare Cybersecurity Table Top Exercises and Simulations**. DHS conducts a nation-wide, cybersecurity exercise every two years. The latest exercise, Cyber Storm V, was conducted March 8-10, 2016. It was the first year in which the healthcare sector had dedicated participation in the exercise. The exercise included a number of healthcare specific scenarios that tested the readiness of the sector to respond to a cybersecurity emergency. The lessons learned were invaluable . As the SSA for the healthcare sector, HHS should consider conducting smaller and more frequent exercises with a broader array of healthcare firms and include scenarios that substantially test the resilience of the sector.
5. **Collaborate on the Implementation of a Digital Healthcare Identity Based on Leading Government and Private Sector Standard That Are Mature and In Place.** Passwords

are still the most frequently used authentication mechanism to gain access to healthcare data and systems and should not be. Passwords are one of the least effective mechanisms to protect sensitive data and applications. Users tend to select easy to remember passwords that can be defeated with widely available password guessing tools. If users employ complex passwords, they tend to reuse these on different systems. Consequently, if one system gets breached the attacker can use the same password to access other systems and potentially escalate the breach/attack. Most security professionals recommend utilizing multi-factor authentication solutions to protect critical systems. This technique combines a token (e.g. smartcard, smartphone, or one-time password generating device) or a biometric method (e.g. fingerprint reader) plus a password to reduce the likelihood of a breach. The problem with this approach is that without standards that allow a digital identity to be reused, users will quickly be encumbered with a wide array of smartcards, devices, and biometric readers to gain access to the many systems they need. This would be costly and extremely complex to manage and would create significant confusion for the user. The government and industry The government and industry have standards and solutions today that will work for patients and healthcare.

In some respects, the government and private sector are de facto administrators of a public-private partnership for the healthcare sector. Government agencies are responsible for public health, for regulation of therapies, medicines, and healthcare providers, and for insurance coverage of a significant portion of the US population. The private sector provides the services, products, medicines and delivery system. Government agencies and larger healthcare firms should build out the healthcare identity ecosystem by implementing existing Healthcare Digital Identity standards. Such an ecosystem would not only significantly improve cybersecurity, but also streamline business processes and rationalize the current fragmented, redundant identity trust issue in healthcare. Further, government agencies and private sector entities should facilitate the adoption of strong authentication by their small firm partners.

6. **Develop Healthcare Sector Implementation Guide to Complement the NIST Cybersecurity Framework (CSF).** Under Executive 13636 – Improving Critical Infrastructure Cybersecurity, the White House tasked NIST to develop a cybersecurity framework that "shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." NIST published the first version of the Cybersecurity Framework in February 2014. The Framework has been quickly adopted by many industry sectors as the baseline against which the members measure the maturity of their cybersecurity programs. A recent study by HIMSS[x] found that 61% of healthcare companies have already adopted the standard to some degree. However, there is a growing demand within the sector for implementation guidelines that specify how to align with the NIST controls given the unique nature of industry. NIST has already developed a draft implementation guideline for the critical manufacturing industry. HHS should consider working with NIST and the private sector to produce a set of specific guidelines for the implementation of the NIST Cybersecurity Framework within healthcare entities.

7. **Collaborate with Global Agencies and Institutions.** Although healthcare delivery and healthcare insurance are conducted by and large nationally based companies, pharmaceuticals, medical device companies, research facilities, and some public health entities operate at an international scale. It is critical that HHS and the private sector work

together with peers in other countries to ensure the adoption of common cybersecurity standards and identify ways in which threat intelligence may be shared more broadly across borders.

8. **Collaborate on Ways to Address the Small Business Challenge**. One of the growing challenges we face in sharing threat intelligence throughout the sector is that smaller, less mature entities without cybersecurity teams have a significant challenge consuming the information that is shared among NH-ISAC members. This is particularly true for the rapid dissemination of indicators of compromise that are in a machine-readable format. This information facilitates the rapid response necessary to deal with quickly evolving threats, but it hinders the ability of less mature entities to consume the information. As larger organizations move to automated sharing and response, this is likely to increase the gap between them and the small entities. HHS should work with the private sector to identify ways in which smaller entities can stay aligned with the quickly changing methods of automated sharing.

9. **Recruit Departing Service Members to Help Offset the Shortage of Cybersecurity Personnel in the Critical Infrastructure Segments**

   One of the greatest challenges we face in the healthcare sector and many other critical infrastructure segments is the shortage of adequately trained personnel to address the rapidly changing cybersecurity threat. Some studies have indicated that there as many as 200,000 open cybersecurity roles in the United States alone and that number is sure to rise as new software and devices work their way into every aspect of our lives[xi]. HHS, DHS, and other Sector Specific Agencies should work with private industry to identify critical cybersecurity roles within the private sector for departing military personnel. The departing military personnel would be required to take a basic cybersecurity curriculum at Cyber Command before leaving active duty. In return for this valuable training, the service member would be required to serve an additional period of time in the National Guard or Reserves during which time the service member would be subject to recall in a national or state-level cyber emergency within any critical infrastructure segment. The private sector would assist the service member in the completion of any degree required for the private sector role. This would provide an immediate pipeline of cybersecurity talent to the private sector. It would also provide states and the federal government with a cadre of trained cyber professionals upon which they could draw. Finally, and perhaps most importantly, it would create opportunities for departing service members to enter a lucrative and growing field.

I believe that if these recommendations were implemented, we would significantly improve the state of cybersecurity in the healthcare industry. We would be able to respond to emerging threats in a more rapid and effective manner while we made it harder for those threat actors to gain a foothold in any healthcare entity. More importantly, these recommendations would help create a greater level of trust among public and private members of the sector which would ensure better collaboration in a time of crisis.

I will conclude my testimony on one final note. If we are unsuccessful in these endeavors and we are unable to significantly reduce the cybersecurity risk that we face, we may delay or even lose the opportunity to utilize promising new health information technology that has the potential to save and improve lives around the world. We may also hinder the ability to take cost out of the healthcare system through more aggressive automation. We cannot let that happen. Thank you again for the opportunity to present and I look forward to your questions.

[i] http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2017/

[ii] https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

[iii] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEJ03320USEN

[iv] The reporting of material events is only required at publicly traded companies. Many, if not most, of the healthcare delivery entities are privately-held or operate as non-profit associations and this requirement would not apply.

[v] https://www.aei.org/wp-content/uploads/2014/06/-american-health-economy-illustrated_145021349951.pdf

[vi] http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/margin.html

[vii] The SAFE BioPharma standard meets both the US Federal Public Key Infrastructure (PKI) and Federal Identity, Credential, & Access Management (FICAM) standards. The SAFE BioPharma PKI Certificate Authority is cross-certified with the US Federal PKI Bridge.

[viii] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[ix] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf

[x] The second annual HIMSS Analytics HIT Security and Risk Management Study

[xi] http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/