NEAL R. GROSS & CO., INC.

RPTS MORRISON

HIF146140

EXAMINING CYBERSECURITY RESPONSIBILITIES AT HHS

WEDNESDAY, MAY 25, 2016

House of Representatives,

Subcommittee on Health,

Committee on Energy and Commerce

Washington, D.C.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2123 Rayburn House Office Building, Hon. Joe Pitts [chairman of the subcommittee] presiding.

Members present: Representatives Pitts, Guthrie, Shimkus, Burgess, Blackburn, McMorris Rodgers, Lance, Griffith, Bilirakis, Long, Ellmers, Bucshon, Brooks, Collins, Green, Engel, Schakowsky, Castor, Matsui, Schrader, Kennedy, and Pallone (ex officio).

Staff present: Rebecca Card, Assistant Press Secretary; Paul Edattel, Chief Counsel, Health; Charles Ingebretson, Chief

Counsel, Oversight and Investigations; JP Paluskiewicz, Professional Staff Member, Health; Graham Pittman, Legislative Clerk, Health; Jennifer Sherman, Press Secretary; Alan Slobodin, Chief Investigative Counsel, Oversight and Investigations; Heidi Stirrup, Policy Coordinator, Health; Sophie Trainor, Policy Coordinator, Health; Josh Trent, Deputy Chief Health Counsel; Jessica Wilkerson, Professional Staff Member, Oversight and Investigations; Kyle Fischer, Minority Health Fellow; Tim Robinson, Minority Chief Counsel; Samantha Satchell, Minority Policy Analyst; Andrew Souvall, Minority Director of Communications, Outreach and Member Services; and Arielle Woronoff, Minority Health Counsel.

Mr. Pitts. The subcommittee will come to order.

The Chair recognizes himself for an opening statement.

In today's digital connected world cybersecurity is one of the most important, most urgent problems that we as a society face. Indeed, a great deal of sensitive information has been entrusted to the federal government. And as the recent breach at the Office of Personnel Management showed, we are not always the most sophisticated at protecting that information. We, therefore, must always be on the lookout for opportunities to improve and adapt to changing cybersecurity threats and realities.

As a result of an investigation conducted by the Energy and Commerce Subcommittee on Oversight and Investigations to examine information security at the U.S. Food and Drug Administration, it was determined that serious weaknesses existed in the overall information security programs at the U.S. Department of Health and Human Services, HHS. It seems a major part of the problem is the organizational structure in place at HHS that puts information security second to information operations. This stems from the fact that right now at the top official responsible for information operations at HHS is the Chief Information Officer, or CIO, and the official responsible for information security, the Chief Information Security Officer, or CISO, reports to him. In other words, the official in charge of building complex information technology systems is also the

official in charge of ultimately declaring those systems secure. This is an obvious conflict of interest.

Today's hearing will take a closer look at bipartisan legislation designed to address these organizational issues. H.R. 5068, recently introduced by our Energy and Commerce Committee colleagues, Representatives Long and Matsui, is known as the HHS Data Protection Act. This bipartisan bill elevates and empowers the current HHS CISO with the creation of the Office of the Chief Information Security Officer within the Department of Health and Human Services, which will be an organizational peer to the current Office of the Chief Information Officer.

This type of structure is not novel or untested. A branch of the Department of Defense has already implemented a similar structure. Many industry experts such as PricewaterhouseCoopers now recommend that CIOs and CISOs be separated, quote, "to better allow for internal checks and balances," end quote.

We are very lucky today to have expert witnesses who can talk to us about not only the bill itself, but help us understand more about the CIO/CISO relationship and why the structure currently in place at HHS could benefit from an update. In particular, I would like to highlight that one of our witnesses, Mr. Mac McMillan, experienced the very structure that H.R. 5068 seeks to create at HHS during his time working for the Department of Defense, and we will be able to provide valuable perspective on

how HHS might implement this reform.

Today's hearing provides members an important opportunity to examine cybersecurity responsibilities at HHS and discuss a bill that will help raise the visibility and priority of information security across the Department.

I now yield the remainder of my time to Mr. Long from Missouri.

Mr. Long. Thank you, Mr. Chairman, for holding this hearing, and thank you to my colleague, Ms. Matsui, for her fine work and cooperation in working with me on this important issue.

Today we live in an age of the internet. While that has spurred faster and more efficient communication between the American people and their federal government, it has also meant having to confront the threat of cyber criminals. Last year this committee released a study with alarming results which included proof that five HHS operating divisions had been breached using very unsophisticated means, and a non-public HHS Office of the Inspector General report detailing seven years of deficiency across HHS's information security programs.

It is impossible to completely eradicate the threat of cyber-attacks, but the American people deserve to know that their sensitive information is being safeguarded with the utmost security.

Mr. Chairman, ensuring the safety of Americans' data is a

vital necessity for the government agencies to operate efficiently. The legislation we are examining today, which I introduced along with Ms. Matsui, would restructure HHS's positions so that prioritization will be given to meeting the critical data security needs expressed by their Chief Information Security Officer.

With that in mind, I look forward to the testimony of our witnesses today.

Mr. Chairman, I yield back.

Mr. Pitts. The Chair thanks the gentleman.

Now I recognize the ranking member, Mr. Green, five minutes for an opening statement.

Mr. Green. Thank you, Mr. Chairman, and welcome to our panel to our subcommittee today.

Cybersecurity represents a current and growing threat to our economy as everyday lives become more digitized. From the 2014 breach at the Office of Personnel Management and the high-profile private sector breaches of companies like Target, JPMorgan Chase, Anthem, we are too frequently reminded of how vulnerable we are to security incidents involving personally-identifiable information.

An unauthorized breach of personal information is particularly concerning when it is sensitive information about our health. As with the private sector, information and

technology security management remains a challenge for all federal agencies.

The principal law concerning the federal government's information security program is the Federal Information Security Management Act, FISMA. The 2002 law requires agencies to provide information security protections for IT systems and information collected or maintained by agencies, quote, "commensurate with the risk and magnitude of harm that could result from unauthorized access or disruption".

Recognizing the importance of cybersecurity and vulnerabilities of HHS, Congress enacted the Cybersecurity Information Sharing Act as part of the Consolidated Appropriations Act in December 2015. CISA requires the Secretary of Health and Human Services to review and report a plan for addressing cyber threats and designate a clear official who is responsible for leading and coordinating efforts within HHS and the healthcare industry.

That law has established the Health Care Industry Cybersecurity Task Force. Members were recently appointed to the task force and will deliver the final report by March of 2017. We should let HHS carry out the provisions outlined in CISA, and I am a bit surprised by my colleague's decision to have a hearing today on H.R. 5068, the HHS Data Protection Act, the legislation that was recently introduced by Representatives Billy Long and

Doris Matsui. And I thank them for their leadership on this issue.

Unfortunately, with the last-minute timing of the hearing, it is impossible for the Administration to testify. Having HHS's perspective would have greatly enhanced our evaluation of the current cybersecurity improvements efforts and this legislation, since HHS will be carrying out the organizational reform proposed in H.R. 5068.

Again, cybersecurity remains an issue, and today is an opportunity to further the conversation. I look forward to hearing from our witnesses about what the private sector and enhanced cybersecurity, including both defensive and offensive capabilities.

I would like to thank you, and I yield the remaining of my time to my colleague from California, Congresswoman Doris Matsui.

Ms. Matsui. Thank you, Mr. Green, for your opening and, Mr. Chairman, for holding this important hearing.

The intersection between technology and our health is impacting nearly every aspect of our daily lives. As we move toward a more connected system of care, we need to make sure our security practices are nimble and forward-thinking to meet this new, exciting health IT landscape.

Making technological investments in our cyber defense systems is absolutely critical, but it is also just as important

that our organizational structures are set up for success. The HHS Data Protection Act that I introduced with my good friend Billy Long would elevate the Office of Chief Information Security Officer within HHS.

The privacy of our health data is of critical importance, and this legislation would establish HHS as a model and leader across the federal government. It builds on the Obama Administration's Cybersecurity National Action Plan, which created the first ever Federal Chief Information Security Officer, a dedicated senior official in the administration focused exclusively on coordinating cybersecurity operations across the entire federal domain.

We are already seeing the shift happen in the private sector, and I look forward to hearing more about this from the witnesses today.

We must also include the important perspective of HHS as the committee continues our consideration of this legislation. A security, connected healthcare ecosystem is better for everyone. This health IT transformation requires a solid regulatory and legislative foundation to work from.

I will continue to work with my colleagues in Congress on forward-thinking solutions to combat cyber threats across both the public and the private sector, and I do appreciate the witnesses being here today. I look forward to your testimonies.

Thank you, Mr. Chairman. I yield back.

Mr. Pitts. The Chair thanks the gentlelady, and now recognizes the gentleman, Dr. Burgess, five minutes for an opening statement.

Mr. Burgess. Thank you, Chairman Pitts, and thank you for holding this hearing.

There are certainly more and more reasons every day to be concerned about our health data security. Digitization of health information has accelerated in all sectors of medicine, and electronic data is taking the place of paper files everywhere from research labs to hospitals, to public health departments.

I am fully committed to advancing progress towards an interoperable universe of health information because I am confident it will offer benefits for medical information and for healthcare delivery.

However, this progress has brought with it threats to patient privacy, threats to patient security, and even threats to safety, unlike anything we have ever faced before. We have seen hospitals that rely on electronic health records be held ransom by hackers, demanding a fee payable in bitcoins, before they can regain access to patient records.

This is no small victimless crime. This could be a matter of life and death, particularly when you consider the care of a critical-needs patient or a critical-care patient in an intensive care setting. This is something that is being perpetrated by sophisticated criminals who I don't think understand the seriousness of the illness of the patients that they are dealing with.

We have learned that there are fundamental weaknesses in the foundation of data security at every major division of HHS, and that hardly inspires confidence. Although the breaches and vulnerabilities at HHS have not been as serious in nature as ransomware attacks in the private sector, there is no reason in the world to just sit back and wait for that disaster to happen and, then, be tasked with examining the smoking ruins.

Data held by the divisions at Health and Human Services seriously affect every single American. Just a few "what ifs":

What if our enemies could hack into the CDC's systems? What is to stop them from using our own biodefense plans against us?

If the FDA's data on clinical trials is vulnerable to hackers, how can companies be confident that their proprietary trade secrets and intellectual property will not be stolen?

There is no limit to the cavalcade of harsh headlines if we don't get serious about data security at the Department of Health and Human Services before it is too late. Mr. Long and Ms. Matsui have taken an important first step in making data security a priority, and I am certainly grateful that we have our witnesses here today. I look forward to hearing from them.

And I will yield to the Vice Chair of the full committee, Ms. Blackburn.

Mrs. Blackburn. Thank you, Mr. Chairman.

And we appreciate our witnesses being here.

This is something that I think many of us recognize is truly a problem. In 2003, when we did the Medicare Modernization Act, I recommended that we put in process an orderly process and incentives for the healthcare provider system to move to electronic records. Well, the hospitals did not want that. So now, what you have is kind of a mixed bag of different systems and people that are in different places along this transition to electronic records. What you also see -- and Politico has a great article in today.

Mr. Chairman, we should put this article in the record because it points out why we need this legislation.

Mr. Pitts. Without objection, so ordered.

Mrs. Blackburn. Thank you.

[The information follows:]

**********COMMITTEE INSERT 1**********

Mrs. Blackburn. As Chairman Burgess said, interoperability it an issue, data security protections. We still have not passed data security or privacy legislation, breach notification, things of that nature, out of this committee, and we should do so.

And also, going back and revisiting HIPAA, which would help us to put in place some protections. We have seen, the hospital industry that is in my district, they have seen some hacks, millions of records, patient records, that have been taken and have been exposed. This is the type of crime that happens to you. You do not know that it is coming. You are not aware many times until months after it has occurred. And that entire time, you have patients that are vulnerable.

So, we thank you for helping turn the attention to cybersecurity, and I yield back the balance of my time.

Mr. Pitts. The Chair thanks the gentlelady.

I now recognize the ranking member of the full committee, Mr. Pallone, five minutes for questions.

Mr. Pallone. Thank you, Mr. Chairman.

I appreciate today's hearing topic on cybersecurity and examining the cybersecurity responsibilities within HHS. I think we would all agree that cybersecurity is a critical issue facing us in our ever-evolving 21st century world. Everything we do on a daily basis is more and more connected through the internet. And when it comes to our health information, just like

our personal information, we must find ways to improve our systems, so that they are secure and protected.

I have said before that this committee has a long history on cybersecurity issues. We also recently held a hearing in the Oversight and Investigations Subcommittee in which we heard firsthand how difficult and complicated this problem is.

Unfortunately, our ability to protect against cyber-attacks while improving still appears to lack what is needed to prevent these intrusions. And what we have discovered is that, while the federal government has had their share of breaches, the private sector is also battling these attacks.

Today we are going to examine one solution to this problem, how an agency should be organized to encourage efficiencies and best practices within the federal government. This legislation, introduced by Representatives Matsui and Long, would move the Chief Information Security Officer, CISO, to the same level as the Chief Information Officer, CIO. Currently, the CISO is located within the same office as the CIO and reports to the CIO.

I look forward to hearing about what this can accomplish, but, also, if there are any shortfalls to such reorganization. For example, would moving the system out of the Office of the CIO create silos? Should information security considerations be integrated into the information technology planning process instead of in parallel, as this bill would suggest? Would this

bill create inefficiencies by removing responsibility for the CIO to take into account cybersecurity? Are there major differences between HHS and the private sector that should be taken into account?

So, let me just say that I am disappointed we couldn't ensure that HHS had an opportunity to be here today to express their own views. HHS should be able to testify to whether this organizational change makes sense from their perspective and whether it could potentially exacerbate the problem it is trying to solve. And this is why I wish the majority had not rushed this hearing.

While this bill may, in fact, be a good approach and I appreciate the efforts of our committee colleagues, the timing of this hearing means that the committee, stakeholders, and HHS itself have not had a chance to fully vet the bill.

Finally, Congress passed a bill at the end of last year that requires HHS to do a thorough cybersecurity report and plan, and I am concerned that we would move forward on these changes before we are able to hear the outcome of this report.

We may never be able to completely eradicate the threat of cybersecurity, but we have to take comprehensive action, and I am glad to see this committee is exploring ways to do that.

I yield back, Mr. Chairman.

Mr. Pitts. The Chair thanks the gentleman.

Although both sides tried to get a witness from HHS, they were unable to produce a witness today. But we will get their consultation, work with them, before moving on this issue.

That completes the opening statements. As usual, the written opening statements of members will be included in the record. We will now go to our panel. Thank you for your attendance today, and I will introduce you in the order of your presentation. You written testimony will be made part of the record. You will each have five minutes to summarize your testimony.

And in the order of your presentation, Mr. Joshua Corman, Director of Cyber Statecraft Initiative, Atlantic Council; Ms. Samantha Burch, Senior Director, Congressional Affairs, Healthcare Information and Management Systems Society North America; Mr. Marc Probst, Vice President and Chief Information Officer, Intermountain Healthcare, on behalf of the College of Healthcare Information Management Executives, and, finally, Mac McMillan, Chief Executive Officer, CynergisTek, Inc.

Again, thank you for coming.

Mr. Corman, you are recognized for five minutes for your summary.

STATEMENTS OF JOSHUA CORMAN, DIRECTOR, CYBER STATECRAFT INITIATIVE, ATLANTIC COUNCIL; SAMANTHA BURCH, SENIOR DIRECTOR, CONGRESSIONAL AFFAIRS, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY NORTH AMERICA; MARC PROBST, VICE PRESIDENT AND CHIEF INFORMATION OFFICER, INTERMOUNTAIN HEALTHCARE, ON BEHALF OF THE COLLEGE OF HEALTHCARE INFORMATION MANAGEMENT EXECUTIVES, AND, MAC McMILLAN, CHIEF EXECUTIVE OFFICER, CYNERGISTEK, INC.

STATEMENT OF JOSHUA CORMAN

Mr. Corman. Chairman Pitts, Ranking Member Green, and distinguished members of the Subcommittee on Health, thank you for the opportunity to testify today.

My name is Joshua Corman. I am the Director of the Cyber Statecraft Initiative at the Brent Scowcroft Center for International Security at the Atlantic Council, a nonpartisan international policy think tank.

I am also a founder of a grassroots volunteer organization focused on cyber safety in the internet of things called I Am The Calvary, and an adjunct faculty for the CISO Certificate Program at Carnegie Mellon University's Heinz College. And lastly of note is I am one of the delegates serving on the HHS Cybersecurity Task Force that came out of the Cybersecurity Act of 2015.

Over the past 15 years, I have been a stanch advocate of the CISO and the emerging challenges that confront that role, and

tried to focus on the vanguard of emerging issues, whether it be the rise of hacktivism, the rise of nation-state espionage, or the increase to cybersafety and cyber physical systems threats that face medical devices, automobiles, and the like. It is an increasingly challenging role, and I work deeply with the Fortune 50 and the Fortune 100.

I say all of this because I have had a front-row seat at the turbulent evolutions that confront this role of the Chief Information Security Officer and have seen the healthy and unhealthy adaptations that the profession has taken in the private sector and the public sector, often through business relationships or my students at Carnegie Mellon University.

What I hope to do here is frame a few of the factors that contribute to a successful CISO and a CISO cybersecurity program; also, speak to some of the costs and benefits and tradeoffs of alternative reporting structures that have been tried in the private sector and elsewhere; also, to answer any questions as you consider your choices.

A brief comment on the current state of cybersecurity which I think is becoming clearer and clearer to this body. Our dependence on connected technology is growing much faster than our ability to secure it, and now it is affecting public safety and human life. The breaches are getting bigger, as we have seen with Target and Ashley Madison. The breaches are affecting

federal agencies, as we have seen with OPM, the Pentagon, and now HHS. And the breaches are getting more dangerous, as we are seeing with power outages in the Ukraine or denial of patient care at Hollywood Presbyterian Hospital due to an accidental impact of ransomware.

I am more deeply concerned, less about the ransomware itself with a financial-motivated adversary, but more concerned at what this has revealed to ideological adversaries who may wish to cause physical harm and a sustained denial of service to patient delivery. And for these reasons, it is important that we avail ourselves of the best practices that are emerging at the vanguard of how we organize cybersecurity programs.

Some factors which I have noticed contribute to the success of a CISO, a CSO, or a cybersecurity program:

No. 1, the individual qualifications of the CISO in question.

No. 2, at topic today, the reporting structure to the CIO, CFO, general counsel, CEO, board of directors, or alternatives.

No. 3, the relationship the CISO maintains, regardless of reporting structure, to key stakeholders throughout the organization.

No. 4, CEO and board-level visibility and prioritization to be supported in the execution of the mission.

No. 5 is the application of risk management principles versus minimum compliance standards, which you often hear a quote of,

"We can spend only on compliance mandatory spending and not one penny more," often truncating true risk management or defensive countermeasures that are required to fend off these modern adversaries.

And lastly, ability for the CISO to both influence IT and business choices, not simply IT or CIO choices. So, the scope is expanding as well.

In general, as an observation, there is a migration away from reporting to the CIO as an inherent conflict of interest for a bevy of reasons which I can get into during your Q&A. And with each of the alternative structures, you see better aspects of the program manifest. For example, a CIO is typically concerned about availability and uptime of IT as opposed to privacy or sensitive information or trade secrets.

Moving simply to a general counsel, for example, typically expresses greater focus on risk management principles on harder-to-replace information like trade secrets, sensitive organizational data, intellectual property, and the like. Reporting to the CIO allows true tensions and natural conflicts which emerge to get top full visibility on how to resolve those differences. And reporting to the CFO often brings to bear very rigorous accounting and audit principles, as have been introduced by the rigor of things like Sarbanes-Oxley on the financial services sector.

Lastly, for 10 seconds here, essentially, there is a tremendous value in experimentation, and I really applaud the spirit of this bill to try an alternative reporting structure in one agency and, if successful, it could be replicated across other agencies to rise to these growing challenges.

I thank you for your time.

[The prepared statement of Joshua Corman follows:]

**********INSERT 2**********

Mr. Pitts. The Chair thanks the gentleman.

I now recognize Ms. Burch, five minutes for your summary.

STATEMENT OF SAMANTHA BURCH

Ms. Burch. Chairman Pitts, Ranking Member Green, members of the subcommittee, thank you for the opportunity to testify today on behalf of the Healthcare Information and Management Systems Society in support of H.R. 5068, the HHS Data Protection Act.

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology. HIMSS North American encompasses more than 64,000 individuals plus hundreds of corporations and not-for-profit partner organizations that share this cause. Our organization has spent more than a decade working to support the healthcare sector in improving its cybersecurity posture through thought leadership, proactive policy development, surveys, toolkits, and other resources.

Today's hearing begins a critical conversation that mirrors conversations occurring in healthcare organizations across the country regarding the most appropriate approach to governance to ensure effective data protection and incident response.

Cybersecurity has been a growing area of focus for healthcare organizations in recent years. Highly-publicized, large-scale breaches of patient and consumer information and other high-profile security incidents have resulted in the increased

hiring of Chief Information Security Officers to serve as the lead executive responsible for safeguarding an organization's data and IT assets. Further, the trend towards elevating the CISO to be a peer of the CIO reflects the recognition that information security has evolved into risk management activity historically within the purview of other executives.

This recognition requires a reporting structure that creates a direct channel to the CEO, CFO, general counsel, and board of directors to facilitate management of security risk in the context of business risk, operational, legal, financial, reputational.

For healthcare providers, a significant security incident or breach may lead to a disruption in patient care, the primary business mission of the organization. As such, it is clear that healthcare organizations need a cybersecurity leader to manage as well as mitigate security risk.

However, it is important to note that it is not simply the organizational change of the CISO which will dramatically improve the security posture of an organization. The right people, processes, and technology must also be in place.

The August 2015 Report on Information Security at HHS raised several important points related to the impact of the current HHS CISO reporting structure and detailed the resulting internal security challenges faced by the Department. This report reflects the criticality of the discussion we are having today.

Like the private sector, HHS needs programs in place that support the specific business missions of its various operating divisions such as CMS is the largest healthcare payer or NIH as the government health research agency. Breaking down silos will better position the Department to move from an audit-driven approach to a proactive, ongoing business risk management approach to cybersecurity that encourages information-sharing within the Department.

Additionally, we believe that external threat information-sharing is essential for HHS with other federal agencies such as DHS and FBI and, also, with private sector healthcare organizations. We see an important external-facing role for the Office of the CISO as well. I direct the subcommittee to my written statement for additional details on that point.

Healthcare organizations have come a long way in building the IT capabilities to make the goals of 21st century cures a reality. Over the past five years, rates of adoption of advanced EHR capabilities have increased significantly. The health information now contained in these systems hold great lifesaving potential.

These goals are particularly meaningful to me, as a five-year survivor of a rare brain tumor, and to the Heinz organization after our colleague tragically lost her 22-year-old son to cancer and other complications last week.

We see clearly that it is trust that will enable these efforts to succeed, trust in the system that will house and control access to the patient's data and trust in the public/private collaborative effort. The HHS CISO, appropriately positioned within the Department, will be uniquely qualified to lead this important mission.

In closing, I would like to thank Congressman Long and Congresswoman Matsui for their leadership on this legislation and the subcommittee for prioritizing this issue. I look forward to your questions.

[The prepared statement of Samantha Burch follows:]

**********INSERT 3**********

Mr. Pitts. The Chair thanks the gentlelady.

Now I recognize Mr. Probst, five minutes for your summary.

STATEMENT OF MARC PROBST

Mr. Probst. Thank you, Chairman Pitts, Ranking Member Green, and members of the subcommittee. It is an honor to be here today to testify on behalf of the College of Healthcare Information Management Executives, or CHIME, concerning the relationship of Chief Information Officer and Chief Information Security Officer at the Department of Health and Human Services.

CHIME is an executive organization serving nearly 1900 CIOs and other health information technology leaders at hospitals, health systems, and clinics across the nation. In addition to serving as chairman of the CHIME board of trustees, I am the CIO and President of Information Systems at Intermountain Healthcare in Salt Lake City, Utah. Intermountain is a nonprofit, integrated health system that operates 22 hospitals in Utah and Idaho and approximately 200 clinics as well as an insurance plan. Intermountain also has over 36,000 employees.

Nationally, Intermountain is known for providing high-quality care at sustainable costs. Essential to our ability to deliver high-value, coordinated patient care is the proper and effective use of health information technology. CHIME members take very seriously their responsibility to protect the security of patient data and devices networked to the systems they manage.

We appreciate the committee's interest in health

cybersecurity and the role that the Department of Health and Human Services plays in helping to combat cyber criminals. We completely agree that cybersecurity must be a priority for HHS, just as it is for the nation's healthcare CIOs.

While this hearing is largely focused on organizational and reporting structures for the CIO and CIOS at HHS, CHIME believes that the subcommittee must also look closely at how the Department coordinates cybersecurity across its divisions. In the private sector, reporting structures vary based on how organizations define the role of CISO. At Intermountain Healthcare, where the CISO reports to me, the CIO, we have made cybersecurity and privacy a major priority and focus.

As an example, I have instructed my team, as they prioritize their efforts each day, I would rather have our data center go completely dark, meaning a complete loss of all of our information systems, than to have a major breach of our data and systems. Losing our information systems would be horrible and highly disruptive, but our patients, members, employees, clinicians, and others have entrusted us with their most personal data, and we need to do all we can to protect it.

Security is not an afterthought. Everyone across the organization needs to make it a priority. Even then, no system is perfectly secure.

As I mentioned, at Intermountain the CISO reports directly

to me, as CIO. In our organization, the CISO is focused on developing and overseeing the implementation of the technical strategy to achieve our security posture as well as managing our security team. Working across information systems/operations ensures that the technical components and processes required for cybersecurity are in place and are managed. The interpretation of regulations, rules, corporate policy, procedure, and development of our strategy to achieve our security posture, what we need to secure and how to set priorities is the role of our Compliance and Privacy Office, which reports to the board of directors.

While these responsibilities are organizationally separate, our management structure helps us achieve a high level of cooperation. My peer in Compliance and Privacy is aligned with me; the Chief Privacy Officer is aligned with the CISO. Together, we develop the plans and manage execution.

We have architected a cooperative model for cybersecurity that ensures appropriate checks and balances, that facilitates high levels of cooperation in achieving a more secure environment. This works at Intermountain. The focus isn't on the CIO's reporting structure. Rather, what is important is that there is an appropriate focus and appropriate checks and balances on both security plan development and execution.

A similar structure is employed at Penn State Hershey Medical

Center, where the CISO reports to the CIO. According to the CIO, this partnership ensures tight integration and solid support for the cybersecurity program across the entire team.

Where the CISO should report is highly dependent on how the various roles accountability for cybersecurity are defined by the organization. Consider some other examples from CHIME members.

At a large children's hospital, the CISO reports to the Data Security Officer. They want to look at analytics. The CIO for a multi-state provider reports to the Chief Technology Officer, who, then, reports to the enterprise CIO. CHIME members at several smaller organizations across the nation report that they have the dual role of CISO and CIO.

There is no question that the committee's interest in this topic is timely and efforts in the healthcare sector to improve the industry's cyber hygiene must be met with similar efforts within HHS.

On behalf of CHIME and my colleague healthcare CIOs, I sincerely thank the committee for allowing me to speak to the evolving role of the healthcare CIO, particularly as it relates to IT security. Thank you.

[The prepared statement of Marc Probst follows:]

**********INSERT 4**********

Mr. Pitts. The Chair thanks the gentleman and now recognizes Mr. McMillan, five minutes for your summary.

STATEMENT OF MAC McMILLAN

Mr. McMillan. Thank you, sir. Chairman Pitts, Vice Chairman Guthrie, Ranking Member Green, and members of the Health Subcommittee, thank you for this opportunity to testify today on this important initiative.

I am Mac McMillan, CEO of CynergisTek, a firm that specializes in providing privacy and security services to the healthcare industry since its inception in 2004. I am pleased to be able to offer testimony in support of H.R. 5068, the HHS Data Protection Act. I believe my experiences as former head of security for the OnSite Inspection Agency and the Defense Threat Reduction Agency, as well as my experiences from the past 15 years providing security services to the healthcare industry after leaving government, 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 United States 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 role to a position equivalent to other senior

leaders within the Department of Health and Human Services and, in particular, the Chief Information Officer. When these two positions have equal authority, are both focused on a common mission, and work collaboratively, the CIO and the 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 priorities.

One of the most often questions I get asked by healthcare leaders today and boards is, where should the CISO report? Cybersecurity is far and away one of the most critical issues for our industry today, but, in particular, for healthcare, which has emerged as a popular target for cyber criminals, hacktivists and state actors engaged in cyber theft, extortion, and high-stakes espionage.

Since 2009 when the HITECH Act was passed and healthcare embarked on a 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 dark-net 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 represents a rare opportunity to steal all forms of personal information, medical, personal information, 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 today. Multiple initiatives that seek to improve healthcare, such as Health Information Exchanges, Accountable Care Organizations, population health, telehealth, network medical devices, cloud services, big data, et cetera, also introduce greater challenges in securing information because it seeks to share it more broadly than ever before.

Add to this the sheer number of individuals accessing and handling health information, and it is easy to see that a CISO, let alone one in an organization as complex as HHS, has a full-time job attempting to stay abreast of the many cyber challenges that leadership needs 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 today in this area is lack of leadership. This resolution seeks to address the situation by creating a cybersecurity leadership post within HHS by elevating the CISO.

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 20 years, security is second nature and understood from one of 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 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 OSIA and DTRA, I understood and had responsibility to ensure the protection of information assets, to constantly assess the risk and 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 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 we worked collaboratively to meet the agency's mission as well as the mandates from national security. The Director communicated that information security was a priority, and every member of the agency, we had well-defined policies, procedures, and processes that both governed and guided our decisions and actions. When new systems and services were contemplated or introduced, it was necessary for security to accredit those before they could be made operational.

This leveling of the playing field between the CIO and myself resulted in a very collaborative environment, because neither one 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 that they could be resolved before they impacted accreditation.

When I had a concern, I could address it to 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 of our arguments.

Mr. Pitts. Could you wrap it up?

Mr. McMillan. In conclusion, sir, I believe that this is a very necessary act for HHS to take.

[The prepared statement of Mac McMillan follows:]

**********INSERT 5**********

Mr. Pitts. The Chair thanks the gentleman, and thanks to each of the witnesses for your testimony.

I will begin the questioning and recognize myself for five minutes for that purpose.

We will start with you, Mr. McMillan. One of the concerns we have heard with this proposal is that, because the roles of CIOs and CISOs are well-established throughout the federal government and many federal government mechanisms rely on those roles being the same across departments, that any change at HHS will disrupt HHS's ability to coordinate cybersecurity activities with the rest of the government.

How did you coordinate with other federal departments and agencies when you were Director of Security with the Defense Threat Reduction Agency?

Mr. McMillan. Thank you, sir.

We actually had a very formal process for doing that. The accreditation process for all of our systems within the Department of Defense depended on everybody in the Department following that accreditation process. So, all of the Directors of Security across the defense agencies and across the military services were essentially all marching to the same drum, if you will, in terms of how we managed our environments and how we accredited our systems.

We did that so that we could create a trusted environment

between all of us to facilitate the sharing of information. We did that, also, with other departments and other agencies throughout the government in order to share information there, because, as you know, the military services and DoD share information with the intelligence community, with Justice, and many other departments, as we work in interagency operations. So, we had to have a structure. So, that structure actually facilitated the ability for that communication to happen in a very effective way, in a very smooth way.

Mr. Pitts. Did the fact that you were ultimately responsible for cybersecurity and not your CIO counterpart impact the ability for you or the CIO to participate in intergovernmental forums and working groups focused on cybersecurity?

Mr. McMillan. Not at all. In fact, if I may, I would say that we actually shared that responsibility. I had responsibility for implementing the information security program or the computer security programs, but the CIO and I together shared responsibility for implementing the cybersecurity program or secure systems. And he had his committees and working groups, and whatnot, that he worked in; I had ones that I worked in. But, ultimately, we worked together very collaboratively up and down the line.

Mr. Pitts. Do you have any suggestions for how HHS might harmonize this reorganization with their participation

responsibilities in federal initiatives, in forums, or programs focused on cybersecurity, where the CIO is usually the agency's representative?

Mr. McMillan. Unfortunately, I am not completely familiar with how they are organized today within the federal government in terms of how that all occurs. But I would say that the CISO in this arena should interact with their counterparts across the government.

We had interagency committees on information security, on computer security that all of the Directors of Security participated in. And even for those agencies where there wasn't a Senior Director of Security who had responsibility like some of us did, those individuals still participated in those forums at that time. I am assuming they still do. I would just suggest that in this arena that what we are really talking about is leveling the playing field within HHS itself in terms of how it makes decisions.

Mr. Pitts. Mr. Corman, do you have any thoughts or suggestions in this regard?

Mr. Corman. Their relationship has to be incredibly strong between the CISO and the CIO. It is just one of many stakeholders that has to have a strong relationship. So, the communication cannot be replaced. It is more a matter of when a conflict arises -- and I have outlined several in my written testimony -- they

can now have an equal footing to resolve those. So, it is not about eliminating communication or siloing information. A CISO cannot succeed without successfully working with its executive stakeholders, and the CIO being a key one. So, I don't think this should be looked at as a siloing effort; more of a balancing of raising visibility and tension decision to a higher level.

Mr. Pitts. Ms. Burch, do you have any thoughts or suggestions?

Ms. Burch. I would agree with what has been said by the other panelists. I think this move of elevating the CISO, what it really does is it allows two complementary skill sets to come together. I think, as Mr. Probst mentioned, there is no necessarily one right way to do this, but ensuring that those direct channels to the executive leadership exist, to ensure that that risk management approach is there, and is factored into the decisions being made. I think we see them really as collaborative and the need for collaboration.

Mr. Pitts. My time has expired. The Chair recognizes the ranking member, Mr. Green, five minutes for questions.

Mr. Green. Thank you, Mr. Chairman.

From what I understand, the bill before us today relates to another piece of legislation passed late last year, the Cybersecurity Information Sharing Act of 2015. Since it required the Secretary of the Department of Health and Human Services to

take certain steps to address cybersecurity, Mr. Probst, can you describe for the committee some of the steps that the Department is currently taking as a result of this?

Mr. Probst. Well, the fact that an individual is to be put in charge to look at the issue of cybersecurity, that it can be focused on someone to actually come up with a plan, CISA does a pretty good job of facilitating that effort, as well as the Task Force that supports some of the decisionmaking. So, I think it is incredibly important, CISA, that it is getting a good focus within Health and Human Services, as well as looking across the various areas of HHS and making sure there is strong coordination.

And let me just emphasize that, as we have been talking about the role of the CISO and the CIO. You know, I think, well, coordination is the key and cooperation. And architecting how you are going to do security is probably the most important aspect, I think, of cybersecurity, not necessarily where an individual reports.

I think if the strategy is, by raising a particular position, and that somehow is going to raise cybersecurity, I don't think that is the case. I think the case is, if it doesn't permeate the organization in all aspects -- I mean, a CISO, it really depends on the role. Like I said, at Intermountain that is a technical role to work and implement a plan. Most of that plan gets developed by compliance people, by legal people, by internal

audits, and it requires the cooperation of all these pieces.

So, I am less about where that role resides, and I think there are good arguments for the CISO to report other than the CIO. But the fact that what the CISO does, it impacts everything within our environment. It impacts our networks, our servers, our physical security, everything within the purview of the CIO. I think it is very difficult to make those too much at a peer level because there is a lot of coordination that has to happen at the technical level.

Mr. Green. How do you see the provisions in CISA working with the legislation we are considering in today's hearing?

Mr. Probst. Well, again, it goes back down to the coordination. Now it is not due until the end of the year. So, HHS has a lot of time still to focus on it, and we will see what comes out of that, the efforts of CISA.

But I would, again, go back to it is coordination and cooperation across the areas and really getting a focused plan for how cybersecurity is going to happen within HHS. Then, I think I would make the decisions where the specific roles report.

Mr. Green. Okay. Ms. Burch, in your testimony you note that "it is not simply the organizational change of the CISO which would dramatically improve the security posture of the organization. The right people, process, and technology must be in place." Can you elaborate on what you meant by that point?

Ms. Burch. Sure. I think that point was meant to underscore the need for collaboration. So, it is not simply, again, changing the reporting structure and you automatically have a culture that elevates cybersecurity. It is about whether all the pieces are in place and whether decisions are being made across the organization to support security as a priority.

Mr. Green. In the short time that we have had the current law in effect, do you see that happening at HHS? And this is for our other witnesses, too. The coordination, the right people, process, and technology in place?

Ms. Burch. We believe that there is certainly room for improvement.

Mr. Green. Okay. Mr. Corman?

Mr. Corman. At our public meeting last month for the HHS Task Force we had NIST come in and give a readout on the voluntary surveys they are doing. Again, it is adoption of the voluntary cybersecurity framework. And they did point out that, while the adoption is comparable in certain aspects of the cybersecurity framework, some of things like asset and inventory management were deficient, which is essentially a linchpin. If you don't know what you have and you don't know when it changes, it is difficult to do successful vulnerability management and good hygiene to avoid some of these attacks.

And if you look at the broad swath of attacks, one of the

most common elements is they are attacking known vulnerabilities that were avoidable and patchable with good hygiene. So, across the government and the private sector there is certainly room for improvement. A hundred of the Fortune 100 have had a breach of intellectual property/trade secrets. No one can be heralded as doing an excellent job, but I believe giving increased focus and priority to this may encourage them to meet and exceed best practices.

Mr. Green. Okay. Mr. Probst or Mr. McMillan, do you all have a comment on it, in my last second?

Mr. McMillan. I do not, sir.

Mr. Green. No? Okay.

Thank you, Mr. Chairman.

Mr. Pitts. The Chair now recognizes the Vice Chairman of the subcommittee, Mr. Guthrie, five minutes for questions.

Mr. Guthrie. Thank you, Mr. Chairman.

And thanks to the panel for being here.

My first question, actually, I would like all of you to address a little bit, but start with Ms. Burch. In your testimony you cited two statistics, and I think it is the heart of why we are here today. It is from the PricewaterhouseCoopers' study.

One, you said that organizations that have the same reporting structure with the CIOs/CISO reporting structure as HHS has have 14 percent more downtime due to cybersecurity incidents and, also,

46 percent higher financial losses in organizations with the same reporting structure. Would you elaborate or tell us why you think that is?

And, Mr. Corman, I think you cited the same statistics. So, I will let Ms. Burch and, then, Mr. Corman go second.

Ms. Burch. Mr. Corman may be able to better answer that question.

Mr. Guthrie. Okay.

Mr. Corman. This is one study; it is a popular study. There is a lot of anecdotal evidence of things like this. One of the reasons, for example, just to give you a concrete, is a CIO is often responsible for and measured by uptime and availability of services. And oftentimes, it is required and necessary for security teams to interrupt uptime to do security assessments or to do healthy security patching to maintain hygiene and reduce risks and exposure. So, that natural tension usually leads to the CIO winning. And if you put off the hygiene and the remediation to enclose exposures for a long enough time period, it can exacerbate the magnitude and the duration of a breach or an outage.

Mr. Guthrie. Okay. So, Mr. Probst and Mr. McMillan, would you like to address that? Why do you think this structure leads to higher downtime and higher financial losses?

Mr. Probst. Again, I think it really comes down to how you

define the roles of the CIO and the CISO and what their priorities are. As I mentioned in my testimony -- and this is serious -- when I talk to my team, I would rather lose all of our systems than have a serious breach. Now I don't know if that is common across every CIO in the industry and it may be unique to just Intermountain Healthcare and the focus our board and our leadership has put on it. But, because of that, I wouldn't have the tension that Mr. Corman mentioned about. We would do the things we need to do to do the best job we can to secure our systems.

Again, the role of CIO in healthcare varies dramatically. If you are a small, 20-bed hospital in the middle of Indiana, you are the CIO, you are the CISO, and you are the guy that changes the ink in the printers because that is what you have to do because of the nature of our business.

So, I think because the roles are so different based on the organizations, and even the emphasize they have placed on security, it is going to be different. I think it goes back to what Ms. Burch said. She talked about how you have to architect this, how it is a holistic approach, and if you have a plan, then you can put the pieces in place to make that plan work.

So, thank you.

Mr. Guthrie. Mr. McMillan?

Mr. McMillan. I would like to answer that question with three things. One, some anecdotal information and, the second

one, some of my own personal experience and, then, why I think it is important.

The first one on the anecdotal side is my company works for hundreds of hospitals across the nation. And I can tell you that not every hospital shares Mr. Probst's philosophy on how to manage security. Marc has been one of the most outspoken proponents of security that I have worked with over the last 15 years in the healthcare industry, and his organization is probably one of the best out there, bar none.

But, unfortunately, that is not the norm. If you look at the breaches that we have had in recent time and you look at my testimony, I think I put one telling tale in there that goes to what was commented on earlier. That is, over 90 percent of the breaches that occurred last year occurred with a vulnerability that was more than a year old, and more than 50 percent of those occurred with a vulnerability that was five or six years old, meaning there was a fix; there was a patch that somebody could have applied. There was a configuration that somebody could have made. There was a port that somebody could have closed. There was a policy that somebody could have pushed out. And those things weren't done. Unfortunately, that gave the bad guys an opportunity to get a foothold and, then, do harm in our environments.

So, I have seen organizations where they have put off what

I call the blocking and tackling or the housecleaning, the hygiene, because they are too operationally-focused on the number of projects they have. Some of our hospitals have literally hundreds of projects on their project board that their IT teams are trying to get done. And then, somebody says, "Oh, by the way, you also have to do this patching and fixing and hardening," and all these other things that take care of systems day-in and day-out.

Unfortunately, what happens is the pressure is on them so intensely to roll systems out, to roll services out, to roll productivity out, that, unfortunately, it does create conflicts and they do make choices. Sometimes those choices are not the best ones from a security perspective.

Mr. Guthrie. Thank you. I am about out of time. Actually, I have run out of time. So, I yield back.

Thank you for the answer. I appreciate it.

Mr. Pitts. The Chair thanks the gentleman.

I now recognize the gentlelady from California, Ms. Matsui, five minutes for questions.

Ms. Matsui. Thank you, Mr. Chairman.

Mr. Corman, I understand you are serving on the HHS Cybersecurity Task Force which was created by Congress in the Cybersecurity Information Sharing Act at the end of last year. Can you elaborate on the work that the Task Force is doing and

what types of industry best practices you are reviewing?

Mr. Corman. So, we are very early in the stages. We have had three meetings to date of the 12 that were prescribed. What we have been doing is inviting exemplars from adjacent agencies which may have instructive lessons for us. For example, we brought in the financial services ISAC and the Financial Services Sector Coordinating Council to explain, as they are the tip of the spear for innovating new ideas and more effective ideas that threaten information-sharing, risk reduction.

One thing the FS-ISAC introduced that is very attractive, for example, is the idea of requiring a software bill of materials from their third-party IT providers through their contract language. What this allows them to do is understand the known vulnerabilities they are inheriting at procurement time to make more informed free market choices. And No. 2, it allows them to do an impact analysis of am I affected and where am I affected when there is a new attack like this ransomware with JBoss, for example.

So, we are trying to bring them in. We have brought in the energy sector as well. While they are not as mature as the financial services sector, they do share similar consequences of failure to the medical field, where it could be measured in life and limb, where bits and bytes meet flesh and blood.

And on the docket, we have more testimonies coming in from

adjacent sectors. So, we are trying to grab the best from each, recognizing fully that medical and healthcare do have some unique challenges that won't be represented by others.

Ms. Matsui. Okay. Now you also in your testimony outlined six factors that contribute to the success of a cybersecurity program, including the reporting structure, which our bill would address. You also cite several metrics that demonstrate the improvements that organizations see when CISA does not report to the CIO. Would you expect those factors and improvements to hold true across both the public and the private sector?

Mr. Corman. Many of them do. This is a nascent field, and I encourage the parallel experimentation. So, for example, none of us expected it was a good idea for a CISO to report to a general counsel. It didn't make sense. It turns out it is one of the best reporting structures for protecting intellectual property and trade secrets and anything material to the business.

So, it is through that experimentation and comparatives that people make these decisions. I have seen excellent relationships where the CISO does report to a CIO, much like Mr. Probst has indicated. It is just not universally the case. In general, depending on the most acute needs of the organization, you may orient differently.

Ms. Matsui. Right. Okay.

Ms. Burch, in your testimony you quoted a study that found

that reporting to the CEO or the board of directors rather than the CIO significantly reduces downtime and financial losses resulting from cybersecurity incidents. Can you talk a little bit about how that idea of reworking organizational structure would translate to an agency like HHS?

Ms. Burch. Absolutely. I think, again, it gets to the prioritization of security concerns. Where does security exist in the culture of the organization? Is it a top-down or is it sort of bottom-up with a lot of roadblocks in between?

So, I think it is very likely, and I think the hope would be, that that would translate. But, again, I think we need to see how a different reporting structure would play out. Obviously, Mr. McMillan has some experience with that to be able to say, you know, were there equal experiences and can they translate? We think that they can, and we think that, whether the reporting structure is to the general counsel or to, in this bill, the Assistant Secretary for Administration, that an alternate reporting structure that elevates security in the case of HHS would be positive.

Ms. Matsui. Right, and I know that we are focusing on HHS here, trying to develop a model here, and knowing that each of the departments/agencies are not similar. However, having said that, I think that there is a lot of focus on this because I think we all believe, based on what has been happening, that health data

is especially sensitive or vulnerable to attack.

And if you think about HHS today, how would you suggest HHS build on the current efforts to take the lead on protecting our health data?

Ms. Burch. From the HIMSS perspective, we think that the Cybersecurity Act of 2015 started us down that path. I think it forced HHS to elevate its role in working with the private sector. I think more and more it is not just internal to HHS, but it is how the information is flowing through the Department. It is coming in many forms. It is coming from many different places. As it comes and goes, there needs to be strong collaboration with the private sector as well. So, I think it is not possible to talk about this issue just in a silo.

Ms. Matsui. Right.

Yes? Quickly.

Mr. Corman. I think that what is often lost is that it is not simply patient information. There are billions of dollars of intellectual property from the private sector contained within the remit of this agency. That is a very attractive target to nation-states or adversaries.

Ms. Matsui. Right, and I see the small discussion we are having here is a very complicated thing moving forward. So, this is really the first step. So, thank you.

And I yield back.

Mr. Pitts. The Chair thanks the gentlelady, and now recognizes the gentleman from Illinois, Mr. Shimkus, five minutes for questions.

Mr. Shimkus. Thank you, Mr. Chairman.

My colleague Jan Schakowsky is over there. Tomorrow is her birthday. And even though she did not vote for my bill, I want to wish her a happy birthday.

[Laughter.]

One of the few in the whole country, but I didn't want to call you out.

[Laughter.]

Mr. Green. Mr. Chairman, you only had 12 votes against you, is that correct?

Mr. Shimkus. I wasn't really counting.

[Laughter.]

So, welcome.

And, Mr. McMillan, Brett Guthrie is also an Army guy; I am an Army guy. So, Marine intelligence is kind of an oxymoron, isn't it?

[Laughter.]

So, we are going to take your testimony with a grain of salt here.

[Laughter.]

No, it is great. This is great because this is really about

organizational structure. As a military guy, someone has to be in charge. I mean, that is really the basic debate.

And you can have good people come in, in Mr. Probst's testimony, but when I was watching you all in the testimony shaking your head or nodding yes, it is my view, watching the body language, that Mr. Probst's story is more unique than the norm. Is that true to the rest of the table?

Mr. Corman, go ahead.

Mr. Corman. As I said earlier, I have seen excellent relationships when the CISO does report to the CIO. It is the historical orientation. And when you have two excellent individuals who have excellent collaboration and they unify their goals and measurements, you can have success, but that is often in spite of the reporting structure, not because of it. And that is why I can acknowledge the truth of his experience and know that it may not be as universally repeatable.

Mr. Shimkus. Okay. In common language, you are saying that is unique, not the norm, from your observation? Go ahead, you can say it. It is all right.

Mr. Corman. Yes. Yes, it can succeed; it can often fail --

Mr. Shimkus. Okay.

Mr. Corman. -- more often fail.

Mr. Shimkus. Ms. Burch?

Ms. Burch. I would agree. I think in what we have seen across the sector, it can certainly work, but, again, it is about the culture of the organization.

Mr. Shimkus. Right, right.

And, Mr. McMillan, obviously.

Mr. McMillan. So, first of all, I would like to say that there are some excellent CIOs out there who do care very much about security and they do an excellent job in supporting their CISO and supporting the program and their organizations.

The problem I have with leaving it up to personalities is that I don't trust personalities. I want structure, so that there are reporting responsibilities, so that there is, as you say, a responsible individual, regardless of what the personalities are involved, that says in the morning, "It is my responsibility to secure this organization and this organization's assets, and it is my responsibility to raise the alarm when I see something that is risky," regardless of whether it is popular, regardless of whether it is going to get in the way of progress at the moment, regardless of what the issues are.

Any good CISO, any good Director of Security understands that they don't drive the train; they are there to support. And they understand that they have a responsibility to raise the alarm with respect to risk and to identify what those risks are and to understand what they are in a balanced way with respect to what

the organization is trying to accomplish. But you don't shy away from doing it. My concern is that, when you leave it to personalities, that may not happen.

Mr. Shimkus. And that is your experience, I mean when you did the DoD stuff?

Mr. McMillan. It has been my experience working with organizations in healthcare. It has been my experience in the government as a Director of Security.

Mr. Shimkus. And I think we are talking on the same issue, and I am going to stop real quick. But just my point of contention will be the same. You have to have someone in charge, and people are going to be moving in and out, especially at the federal agency in this line of work. And one good working relationship, one movement could just change that.

Anybody else want to add anything? Go ahead, Mr. Probst. We were picking on you.

Mr. Probst. Well, yes, thanks for picking on me. It is good to be unique, I think.

I would say, on a bed basis across the country, if you talked to the CIOs that manage the largest numbers of beds across the country, you are going to see their structure very similar to the structure that Intermountain Healthcare has, where the CISO is reporting up to the CIO. Now that can be changing, and I am sure of that, but, again, you are talking about more sophisticated

organizations. And it has worked incredibly well.

And I go back to what you said, sir, which is, who is accountable? And we make really important decisions. I have told you what I feel about the security of the data and the systems, but our systems also save lives on a daily basis. We have to make decisions that are critical. We may have someone sitting on a table where now the technology is providing --

Mr. Shimkus. Yes, my time is almost done, and I appreciate that. The hostage-taking that has occurred on major hospital systems and when people have to go to paperwork transactions, it just really risks people's lives, and we have got to get on top of this. I think that is the same thing with federal agencies.

I thank you for your testimony.

I yield back, Chairman.

Mr. Pitts. And the gentleman yields back.

At this time, we will go to the president of the John Shimkus fan club and the birthday girl, Ms. Schakowsky.

[Laughter.]

Ms. Schakowsky. I thank you for pointing out my aging.

[Laughter.]

No, thank you very much.

I wanted to ask Marc Probst a question, but I wanted to start first by just thanking all of you for joining us today on this very, very important issue.

I mean, how common data breaches are is just incredible. There have been more than 112 million healthcare records that were breached last year. It sounds like just about everyone. I understand that these records are rich with personal information, which usually includes a patient's Social Security number, which is used as an identifier with a bevy of other personal information, as the patient moves through the treatment continuum. Access to such information, then, enables all those bad actors out there to execute identity theft and fraud, which we have had hearings on that, too, as a growing problem.

So, Mr. Probst, I know you talked about it, but if you could just summarize, what can we do to make electronic healthcare records less of a target for hackers?

Mr. Probst. Well, I don't know about making them less of a target. I mean, one thing we could do is look at how the data is being used within those records and try to stop any abuse that might be coming.

Now, if they are going out and getting a new credit card, that is going to be hard because we are going to have that kind of information. There is just no way we are not going to have it.

But I think one thing we could do and should do, and I think we are beginning to focus on, is getting to a better identification system, so that we can have a national patient ID that actually

is consistent across the industry. That really helps us to not have to carry a lot of data that we otherwise have to have to identify a patient in any kind of situation, whether it is in a hospital or a clinic or elsewhere. So, I do think there are things we can do like those types of standards that will help us to protect the data.

Ms. Schakowsky. Would this be instead of -- give us an opportunity to remove, for example, Social Security numbers and substitute something else? Is that what you are saying?

Mr. Probst. I am saying that, yes, if we didn't want to have the Social Security number out there -- we use that as an identification tool, as we use address, as we use age, as we use all these different data items. If we could come with a very unique way of identifying the patient, there are certain pieces of data that we wouldn't need that, clearly, the bad guys are looking for.

Ms. Schakowsky. And what do you think that Congress can do to aid healthcare organizations, especially small and rural providers, for them to be able to better protect their patient data?

Mr. Probst. Well, again, going back to some standards on how we are going to -- even things like HIE, and Mac brought that up earlier, Health Information Exchange, we don't have good standards right now to do that. And so, you have all different

kinds of technology out there trying to do things within healthcare to make it better.

If we could get better standards on how we interchange data, on how we store data, what the data looks like, like I said, identifiers, that is going to help everyone because, if we can figure it out in a large organization, we can, then, share those capabilities with smaller organizations. But, right now, they are kind of on their own.

Ms. Schakowsky. Let me just ask everyone, is there any hope that we could establish a zero-tolerance standard, given it seems like we make a change and, then, the hackers improve on it?

Yes, Mr. McMillan?

Mr. McMillan. Yes, ma'am. That would be, in my opinion, a very unwise thing for anybody to try to do in the security realm. Security is such a dynamic phenomena in that everything about security as it relates to systems is changing as we sit, as we sit here talking. I mean, the environment changes; the threat changes; the systems change; operations change; the network changes. The number of changes that an organization has to manage that can affect the security or the risk of a system is incredible, and it is constantly changing. There are things that we don't know yet.

For instance, right now, this whole focus on ransomware, in my opinion, is focused on the wrong thing. Ransomware is not what

we should be focusing on. That is just one form of malware that is affecting systems. There are hundreds of forms of malware that affect systems.

What we ought to be focusing on is the impact of that particular malware or malware in general, which means we should be focusing on things that take systems down and make them unavailable to health systems to serve patients. If we want to make a change, increase the penalties that people stand to face if you do something that interferes or disrupts a hospital's ability to deliver care, regardless of the way you do it, whether you drive a truck through the door into the data center or whether you send some sophisticated ransomware in there. At the end of the day what is important is that the data is not available to take care of the patient, not how it happened.

Ms. Schakowsky. Thank you. Thank you very much. I yield back.

Mr. Pitts. The gentlelady yields back.

At this time, we recognize the gentleman from New Jersey for five minutes, Mr. Lance.

Mr. Lance. Thank you, Mr. Chairman.

Good morning to the panel.

Mr. Corman, in your testimony you spoke briefly about some of the reasons that the current CIO/CISO reporting structure at HHS might create conflicts of interest. Could you provide us with

some examples from your professional experience in this regard?

Mr. Corman. I did put a few in the written testimony. But, verbally, often there is a project to roll out a new service, and the time to do so involves software development, procurement, a number of things. In that long relay race, one of the stages needs to be security. That is usually the one cut to make sure that you deliver on time and on budget. So, you can often have a CIO deploy the service before it is seaworthy, before it has been properly assessed, before the vulnerabilities have been enumerated. So, that is one of the areas where it is a conflict of interest to try to tack it onto the end and usually run out of time and budget.

Another one is a zero-sum budget where you can either buy a new server or a new security appliance. If the CIO is more measured on supporting business intent as opposed to being compliant or reducing risk, they tend to buy the things that are more familiar to their schooling, their experience, et cetera. And these don't always have to occur, but there will be natural tensions like that.

Mr. Lance. And how do you think we should address this issue, working with experts like yourself?

Mr. Corman. Well, it is a tough problem. That is why we have the Task Force. And we are quite overwhelmed by it, especially because they environments are target-rich but

resource-poor.

Mr. Lance. That is an interesting way to sum it up, target-rich but resource-poor. I think that is critical to an understanding of this.

Mr. Corman. Yes. I think one of the things that we did not say yet, but is worth noting, is when a security person is inheriting IT choices made without them, there is only so much they can do to secure them. If you flip the relationship and they are more peers, a security person can help make the more defensible and securable IT choices. So, there are certain things you could buy in your life that are harder to maintain, for example. One of the benefits of having these relationships be peers is they both have criteria for which cloud service to choose, which servers, which laptops. And if it has more informed criteria out front, the total cost of ownership later from a security perspective goes way down.

Mr. Lance. Is there anyone else on the panel who would like to comment? Perhaps Mr. McMillan?

Mr. McMillan. Yes, sir, and I think I alluded to this in my testimony. When there is a balance between those two roles and the security person owns the process for evaluating the technology before it is deployed or as it is being deployed or as it is being developed, what you end up with is the shortcuts that were just alluded to don't happen because, when I see that

shortcut not happening, I say, wait a minute, we have to do the testing; it is time for testing, or it is time for doing whatever.

When the IT organization owns the process from soup to nuts and security only comes in at the end, there is opportunity for things to get missed as it relates to staying on track or on schedule. Now, again, that doesn't mean that everybody is skipping steps or everybody is not doing things, but there have been instances where we have deployed systems or organizations have deployed systems, clearly, that everything wasn't taken into consideration that should have been. And primarily, it was because security wasn't addressed at the beginning of the project; it wasn't until the end.

As the gentleman on the end said, once you select a product and you implement that product and deploy it, if things have been missed that are critical, it is very difficult to bring that back in.

Mr. Lance. Ms. Burch or Mr. Probst?

Mr. Probst. Well, I hate to keep coming back to roles. But, listen, if the CIO is cutting corners around security in healthcare, you have the wrong CIO. And I believe that is starting to be seen more and more within organizations in healthcare. It is relatively new. Six years ago, information security in Intermountain Healthcare was two people, and they mostly worried about passwords. It is now 50. So, it is

different.

Mr. Lance. And this, of course, is the wave of the future, and we all have to be concerned, so that security is protected.

Mr. Chairman, I yield back half-a-minute. Thank you.

Mr. Long. [presiding] The gentleman yields back.

At this time, we will recognize the gentleman from New York, Mr. Engel, for five minutes.

Mr. Engel. Thank you, Mr. Chairman. Thank you for convening today's hearing.

Mr. McMillan, you mentioned in your testimony that healthcare has been characterized as being a soft target for cyber criminals, an idea that I think we can all agree is quite unsettling. Has healthcare always fallen into this category and, if not, how did it come to be a soft target?

Mr. McMillan. So, I think, sir, that healthcare has always been in this category, and I think it is just of late, as the threat has focused more and more on healthcare, that it has become so apparent. I mean, if you look at the evolution of the incidents that we have had in healthcare, they closely track the evolution of how we have evolved in healthcare as well with respect to our systems and our data.

I mean, you can actually go back to before 2009, before meaningful use and before electronic health records and before we started digitizing most of our patient information, and you

can see a marked difference between the kinds of issues that we had or incidents that we had back then and the types of incidents that we have had from 2009 on. Those incidents have done nothing but increase as time has gone by and as cyber criminals have figured out that, one, they can monetize this information and they can make a business out of it. That is really what it is.

I mean, I saw a study just this past week that said we are looking at $6 billion in revenue in cyber crime this year. That is not crime anymore; that is an industry. And that is the way we need to look at it.

You can go out there today and it is very simple for just about anybody to get involved in this industry. You go out there to the dark-net and buy services, buy techniques, buy tools, buy exploits, buy information, and it is all readily available. And that is why it is growing so exponentially.

And healthcare, up until just recently, had not really been focused on security. As Marc said, a few years ago he had two folks in that department; today he has 50. An organization his size, I would never have imagined that they only had two people.

But I can tell you, when I left the government in 2000 and came out into the private sector and started working with healthcare, I was absolutely appalled at the state of security at most of the hospitals that I went into at that time.

Mr. Engel. Yes, Mr. Corman, you wanted to comment on it?

Mr. Corman. Yes. I sometimes think it is in terms of just normal police work. It is motive, means, and opportunity. And I think it is undeniable that, as we connect more medical technology and meaningful use -- I posed a question to the Task Force. I said, "Is meaningful use our original sin? Did we basically throw gasoline on the fire by essentially encouraging that we connect everything to everything else before we had done proper design and threat modeling, and whatnot?"

Of course, there are benefits to that and, of course, we are about to do the same thing again with precision medicine and machine learning and big data. We have to understand the tradeoffs between those.

So, I would say I just saw a chart yesterday from IBM, Pete Aller, showing that the top five data records stolen in the prior year didn't have healthcare on them, and last year, the most recent data had it No. 1.

So, I think one of the reasons you have seen more records isn't that they weren't vulnerable before. It is that, as we have more opportunity and more connectivity and we now have the motive to go with it, this is going to accelerate, I believe.

Mr. Engel. Thank you.

Mr. Probst?

Mr. Probst. Yes, I think one other issue to think about is in healthcare our systems weren't built to be protected. We

weren't the NSA figuring out how are we going to build a system that no one else can externally get into. We built systems so that people could have immediate access across lots of different platforms and places, so they could save someone's life in the time that it was needed. And that is how our systems were built. And now, we are going back and saying we have to architect these a little bit different; we have to change them because we have a lot of important data to protect. I think we are soft for a number of reasons, but that would be one of them.

Mr. Engel. Thank you.

Ms. Burch, let me ask you a question. You noted that a significant security incident might not only endanger patient privacy, but could also disrupt patient care. Can you provide any examples in which a disruption like this took place? And I ask this because I would like to understand how severe this kind of disruption might be. Have treatment plans, for instance, been interrupted? What kinds of effects have these disruptions had on patient outcomes?

Ms. Burch. In our experience in talking to our members, certainly, when you don't have access to information and you have a patient you need to treat, more and more as we are automated and that information is included in the electronic health record, you can't just pull a paper chart and, all of a sudden, you have got all the information there. So, I think the concern is whether

it is an attack that prevents access to information, or whatever it might be, that there are real potential negative patient outcomes here.

And that goes with the privacy side, that you have both internal and external risks that you are facing. Certainly, many privacy issues stem from security issues. So, was there an inappropriate disclosure by a staff member because access was granted when it shouldn't be, or something like that?

So, I think it is possible that Mr. Probst might be able to provide experience that he has had personally. But I think, generally, that is what we have heard from our members in terms of, yes, I mean, they think about this in terms of potentially lives lost. It is that serious.

Mr. Engel. Well, thank you. Thank you all very much. I very much appreciate your testimony.

Thank you, Mr. Chairman.

Mr. Long. The gentleman yields back.

And at this time, I will recognize the gentleman from Virginia, Mr. Griffith, for five minutes.

Mr. Griffith. Thank you very much. I want to make a couple of comments before I ask a couple of questions.

First, this is one of those hearings that we won't see extensive coverage on CNN or the nightly news, but we appreciate your being here. One of the reasons that you won't see it is that

it is a bipartisan bill trying to solve problems for Americans where nobody is shouting at anybody or making any accusations against the folks who are here, and both sides of the aisle are generally in agreement.

Mr. Long, you and Ms. Matsui have come up with a good idea, and I commend you for that.

Mr. Probst, I like the way you look at this. This bill, of course, deals with HHS that we are talking about today, but there has been a lot of discussion about hospitals should be doing. One of my early concerns before you made your comments was, okay, wait a minute, one-size-fits-all from Washington doesn't usually work. You made that point very well in a larger system like your own, talking about separating the CIO and the CISO. You all have made a great case for that today. But, in the 20-bed hospital where the CIO is also changing, I think you said the photocopier toner or something along those lines, it doesn't necessarily make sense, although we have to be vigilant.

Also, in your testimony, Mr. Probst, I notices that you touched on device manufacturers related to HIPAA. Because there will be some folks, probably insomniacs, who will watch this, could you explain that dilemma? I am very concerned about HIPAA issues, and I thought it was a very salient point that you made.

Mr. Probst. Well, HIPAA gives us good guidelines on the privacy and security that we should apply to all of our

information. Specific issues around medical devices, they don't have the same level of sophistication around cybersecurity, at least historically they haven't. And we have a lot of old medical devices. I think they are getting much more aware of it today.

But today we have thousands of medical devices. They are all connected to our networks. They are essentially computers. They have personal health information on them, most of them, and they become a pretty interesting entry point for the bad actors to get into our networks. It doesn't take much of a crack in the hull for the water to start pouring in. So, that would be my major concern with medical devices, is just how we have been able to treat them.

Because they are regulated by the FDA, most of them, I assume all of them -- I don't know -- but because they are regulated, many of their operating systems are decades old. So, we don't have all the patches that Mr. McMillan talked about that we can apply to it to get the security at a level that we want. So, medical devices I think are something we are paying attention to as an industry, but we are going to have to pay a lot more attention to.

Mr. Griffith. And when you talk about they are regulated by the FDA and, therefore, some of them have operating systems that are decades old, that is because if there is any change, it has to go back through the process --

Mr. Probst. Exactly right.

Mr. Griffith. -- to be reapproved by the FDA? So, what you are suggesting is that, maybe in the same bipartisan spirit that this bill was put together, some of us might want to be looking at a way that we could change at least for the security side, say that if you do a patch on security issues, it does not have to go through that FDA process? I know you haven't had time to think about it, and maybe you want to answer that question later.

Mr. Probst. Yes, maybe --

Mr. Griffith. That is a reasonable conclusion, is it not? Maybe put it that way. Would that be a reasonable conclusion for someone like myself to make?

Mr. Probst. I think that is a reasonable conclusion, that it should be looked at. I don't know the exact answer --

Mr. Griffith. Sure.

Mr. Probst. -- for the FDA, but it definitely needs to be looked at.

Mr. Griffith. And I appreciate that, and that is why I love coming to these hearings and listening, because there are often things that you learn that you never thought you would. And that sounds like a good suggestion.

I do appreciate it very much, all of you being here. You have really opened a lot of our eyes and convinced me this is (a) a good bill and that, in fairness, every healthcare provider in

the nation ought to be reexamining what they are doing and see what fits for them to try to give us some more security in these areas.

With that, Mr. Chairman, I yield back.

Mr. Long. The gentleman yields back.

And I believe Mr. Corman wanted to add something.

Mr. Corman. On that point, the I Am The Cavalry group, founded by volunteers, we are specifically focused on cyber safety for connected medical devices. And many of them are very hackable. There was a recent DHS ICS-CERT announcement on a single device that had over 1400 known vulnerabilities in it.

But, to clarify, we have been working with the FDA, the Food and Drug Administration, on their guidance for connected cyber safety in medical devices. Their pre-market guidance has clarified that you can, in fact, patch without going through recertification. There has been poor education awareness that that has been clarified, and some vendors claim that it can't patch, even though it has been clarified repeatedly that they can.

And, No. 2, this January the post-market guidance for ongoing care, feeding, and hygiene for those devices has also been published, and the 90-day comment period is closed.

So, the FDA is taking actions to modernize the very things you are concerned about. I think there is a long way to go, but they are on the right journey.

Mr. Griffith. Thank you.

I yield back again.

Mr. Long. Thank you.

And at this time, I will recognize myself for five minutes.

Ms. Burch, in your testimony you talked about the evolving role of the Chief Information Security Officer and how information security has evolved into a risk management activity. I think most of us hear this job title and think about firewalls, antivirus, not risk management. Can you elaborate a little bit on what you mean by that?

Ms. Burch. Sure. So, we think it is important in this rule to be looking at the business risk that is faced by the organization. So, we don't like to think of healthcare as businesses, hospitals as businesses, but, you know, in functioning in that way, they have to keep their doors open and they have to treat patients, and they have certain business missions that they are trying to work through.

So, for us, we think that it is really important to look at the range of risk and the way that the CISO looks at the range of risk in terms of working with the various other executives, whether it be the general counsel on legal and compliance risks, or whatever it happens to be. So, it is looking sort of across the entire organization at why are we securing our information and assets. What are we trying to prevent from happening? First

of all, being harm to patients, but there are certainly other risk involved.

Mr. Long. Okay. Thank you.

And you go on to state that, because the Chief Information Security Officer is now a risk management position, that it should be moved out of its traditional subordination to IT. Can you connect the dots for us? Does the fact information security is currently subordinated to IT mean that the risks aren't always appropriately communicated to officials higher in the organization?

Ms. Burch. That is what we have heard from our members in certain situations. Again, every situation is unique and, as we said from the beginning, it gets back to the organizational culture. But we have certainly heard of instances where operations has been prioritized over security.

One example that we have heard is you have a device, let's say a bedside monitor that works really well in its base function. You know, the medical staff is happy with it. However, said device happens, also, to be operating on Windows XP, which is obviously no longer supported. Therefore, it is very vulnerable to attack that could result in substantial harm to a patient.

So, I think that is sort of an example why we need to level the playing field at least in terms of elevating security within organizations.

Mr. Long. Mr. Corman, you had something?

Mr. Corman. Yes. One change in IT in business models, even in the federal government, is the increased use of third parties and supply chain partners and third-party services. And the CIOs, traditionally, while they can inform and create criteria for the selection of those third-party services, they have less operational visibility and control over them. So, it has been increasingly important for the CISO to provide upfront guidance and ongoing audit against those third-party risks as we become more dependent on third-party technology.

Mr. Long. I have a sign in my office that says, "Bring back common sense." And it is the most commented sign or anything in my office. People always say, "That is exactly what we need to do."

And I know that Mr. Probst, as the CIO of his organization, is very much in tune with the CISO and gives that person everything they need. But, for any of the panel, in my last minute here does anyone care to comment? Doesn't it make common sense that, if someone is charged with being a Chief Information Security Officer and they want to implement new systems, and then, the person above them has bigger fish to fry and doesn't care about that right now, doesn't that lead to the types of things we saw at HHS, Mr. McMillan?

Mr. McMillan. Yes, sir, it certainly can. But I will have

to go back to something that Marc said because I do absolutely agree with him that it is not just about the position; it is also about the processes and the structure within the organization as a whole, and how the leadership of the organization views security as well.

The reason Marc is able to do a lot of the things he does and the support that he gives his CISO is because he also has the support of the rest of the executive team for his model. There are situations where that isn't necessarily the case.

Again, it gets back to what I said earlier, and this gets back to your comment about common sense. Anytime we leave it up to people, people will disappoint us, and that is one thing that we have learned in security. They will make bad decisions. They will make good decisions for the wrong reasons. I mean, there are all kinds of things that can happen.

What I have come to understand over the years in doing this is that, when there is a separation of duties and there is a clear delineation of responsibilities, and both parties are doing what they are supposed to be doing and communicating openly, and the leadership has the ability to hear both those arguments, they make much better decisions.

Mr. Long. Mr. Probst?

Mr. Probst. Yes, I mean, if the CIO's at HHS job is to be the tech guy, to go install systems and monitor networks, and those

types of things, and it isn't around highest security, then, by all means, the CISO should report somewhere else. If the CIO's job is to protect the data and to do all those other things that I mentioned, then, potentially, maybe the CISO should report to the CIO. But it goes to what Mac just said: what are the accountabilities? What are the responsibilities you are putting on those roles? And then, see that they do it. But this is a major issue, you know, security.

Mr. Long. But the person charged within it should be able to make the final decision, should they not if --

Mr. Probst. They should.

Mr. Long. -- they implement a security system?

Mr. Probst. They should.

Mr. Long. Okay. Thank you all for your time.

And at this time, I am going to yield to the gentleman from New York, Mr. Collins, for five minutes.

Mr. Collins. Thank you, Mr. Long.

I want to follow on that with Mr. Probst and Mr. McMillan because I absolutely agree with the comments you just made. I spent my life as a CEO in the private sector; in fact, was CEO of the largest upstate county in New York.

And at some point, a person has to call the shot because you are always going to have the potential -- you are not going to have perfection. We are saying there will always be some

differences between operational efficiencies and security, always. I can make it 100 percent secure and we do nothing or I can open it wide up and be as efficient as you could imagine and have a lot of backdoors.

So, a person, an individual, a human being has to make a judgment call, correct?

Mr. Probst. Yes.

Mr. Collins. All right. So, what you have to have in an organization is a good, smart person with common sense to make that judgment call, understanding the potential consequences, which may be different with a medical health record than something else. I mean, they have got to make a judgment call. In hindsight, if something goes wrong, they are always going to be attacked on that judgment call.

So, I guess I am somewhat ambivalent on this, only in thinking, when there is a disagreement on security and operations, it goes to someone else. Now, if it goes to the CEO in a small company, the third time those two people walk in his office will be the last time they walk in his office because he has got too much going on, and he is going to say, "You know what, Joe? You are now in charge of both. Sam, you report to Joe. You have security and other operations. You figure it out. Your head is on the line. Get out of my office." That is how a small company would work.

Now HHS is different. It is a huge organization. But, at some point, these two concerns come together and somebody has got to make the call.

I think, Mr. Probst, as you pointed out, the right individual, given guidance by the person in charge and the board of directors, or whatever, could be the CIO, and everything would be fine. On the other hand, if the organization is inept, then it would never be fine.

So, I am just sitting here -- at some point, Congress has a role to play. At some point, you have got to hope the President appointed the right person to be the Secretary of HHS, who, in turn, appointed the right person here and here. And I just have to wonder sometimes, is it Congress' role to get into the operational structure of an administrative department or do we need to just trust that smart people are government? I mean, what would you say to that, Mr. Probst? Should Congress be micromanaging at a CIO/CISO level and writing job descriptions?

Mr. Probst. Well, I don't believe they should personally, but that kind of just puts aside everything that we talked about today. I mean, the things have to happen, right? You have to have an architecture. You have to have an approach, and you have policies.

Mr. Collins. Correct.

Mr. Probst. If you do, you can have smart people.

The one thing we didn't talk about while you were speaking, sir, was the presidential appointment of the CISO. That concerns me a little bit as well because now you are going to politicize a really important role. If you have smart people as the Secretary of HHS -- by the way, I think we do, and there is some very good leadership there -- they ought to be able to find the right person to do it.

Mr. Collins. Oh, no question. No question.

Mr. Probst. But that is part of this role.

Mr. Collins. Yes, Mr. McMillan, do you have a comment, having come out of DoD?

Mr. McMillan. I agree with that as well. I think, again, it gets back to having all the different components. And you are right, if you have the right structure, if you have the right expectations in terms of how we do things, then you are right, smart people can make good decisions and they will do responsible things.

I think it is a combination of all those things. But, even so, my experience has been that there does need to be that open communication with respect to managing risk. And there have been countless situations where the IT organization, which ultimately at the end of the day is responsible for delivering services, has numerous pressures put on them to meet deadlines, et cetera, things like developing software where we have to hit a deadline

to meet software. So, we get rid of the regression testing or we get rid of the security testing. The next thing you know, we have a piece of software out there that has got bloated code in it or it has got insecure code. But we hit our deadline, right? So, we didn't have any penalties.

We can't let those things happen when we are talking about something as serious as this. When you are talking about things, to get back to medical devices, what we haven't talked about yet is why don't we have a solid standard for how a medical device has to be engineered and architected from the beginning. The FDA guidance is just that, guidance. The manufacturers don't have to listen to it.

Mr. Collins. I think my time has expired. You know, I appreciate that, and I just would conclude by saying we all, I think, know a person is ultimately going to have to make the call on the balance. It is a human being. Sometimes they make a mistake. In hindsight, people would always say they made a mistake. And we just need to recognize, whatever we do here, we are not going to end up with perfection and it is going to be a human being making that call between efficiency and security.

Thank you all very much. It has been very interesting.

Mr. Long. Thank you, Chairman.

Mr. Pitts. [presiding] The Chair thanks the gentleman, and now recognizes the gentleman from Indiana, Dr. Bucshon, five

minutes for questions.

Mr. Bucshon. Thank you, Mr. Chairman.

I was a healthcare provider before I came to Congress. So, this is a pretty interesting issue. And I will probably diverge, go away from the pathway we have been on just a little bit to talk more about why are people going after healthcare information.

To start, what data is the most important that people can get from an electronic medical record?

Mr. Corman. Well, some of this is just the natural expansion of the dark markets and the criminal organizations. The street price of a credit card has plummeted due to a surplus from our rampant failures. It used to be over $100; now it is under $1 in certain circles. So, they have migrated to other forms of assets they can turn into currency.

A difference between a credit card and some of the healthcare records is that I can get a new credit card; I can't get a new body.

Mr. Bucshon. Right.

Mr. Corman. So, it is the durability of the information.

Mr. Bucshon. Say, for example, though, that you are a patient.

Mr. Corman. Yes.

Mr. Bucshon. Okay? And you have a specific disease. Why is that marketable?

Mr. Corman. It is not as much the disease. A lot of the information there can be used to perpetrate bank fraud, check fraud, account takeover.

Mr. Bucshon. Okay. So, it is not necessarily the health information. Like say you have heart disease, or whatever. It is everything that is in your record at the hospital, which includes your Social Security number or your other financial information, things like that?

Mr. Corman. Yes. If it is someone famous or if it is someone important, that could be a high-value target.

Mr. Bucshon. Right, right. I understand. Then, you could leverage --

Mr. Corman. Yes.

Mr. Bucshon. Say someone has a particular disease and they don't want the public to know, for example.

Mr. Corman. Even employer discrimination. There is a bunch of markets for that.

I just want to remind, part of the testimony is, you know, we have a joke that we say we love our privacy; we want to be alive to enjoy it. So, as we do tackle these, we want to make sure we are looking at the privacy and the safety of this.

Mr. Bucshon. Anybody else have any brief comments on that one?

Mr. McMillan. I agree with all of it. I would say the one

exception to that that I worry about is, when you start looking at things like the OPM breach and the Anthem Blue Cross breaches, et cetera, where enormous amounts of medical information and background information on government workers was exposed, there are national or state actors out there who absolutely would like to know if we have medical conditions that are sensitive to certain individuals in our government and certain positions in our military, et cetera.

So, there is time where medical information is valuable to certain other individuals, and it is not necessarily the cyber criminal who is looking to commit fraud or commit identity theft or those types of things. I don't think we can discount those things. They didn't steal 80 million records from Anthem Blue Cross for nothing. They didn't steal 23 million records from OPM for nothing. There was a purpose behind that. We probably don't know what the purpose is yet.

Mr. Bucshon. Yes, I just wonder whether like, you know, I mean, people can find out that I have high blood pressure, which I do. Why do they care? Why would they care? Do you know what I am saying?

So, that is the thing I was trying to get at. Is it the other information? In certain circumstances I understand that could be valuable information to people, right?

It seems to me that the reason -- and I think, Mr. McMillan,

you pointed this out -- that the focus is on now criminals going after health information, it is not the health information per se; it is the fact that now everything is being connected, and it is a portal through which they can get other information that in many other areas of our society, banking and other areas, those portals have been closed, effectively closed. They are never closed.

And we haven't gotten ahead of it on the health IT side, Mr. Probst, as you pointed out. I mean, exactly, as a physician, you know, it always drove me crazy if it took me very much time to get into the health record or not. So, it is going to be a real easy -- you know, I put in my password, and there it is, right? I can get into the entire system because that was the focus, right?

So, I am just trying to get at, it is not necessarily that this is healthcare IT; it is a portal into people's financial lives and everything else. Is that true or not true?

Mr. Probst. I think that is part of it. I mean, we are talking about people stealing data and using that data for inappropriate things. But the whole concept of cyberterrorism is very real. I mean, if you think about healthcare as an infrastructure piece of our country, I mean very key component of the infrastructure, cyberterrorism is very real and it probably scares me more than even some of the data that is being taken.

Mr. Bucshon. Okay. I have got one more question. So,

briefly?

Mr. Corman. Yes, real fast, on that point, none of us in the room are really that concerned about the ransom aspect of Hollywood Presbyterian. We were concerned of someone like Trick, a former Anonymous hacker who radicalized into an ISIS. Someone like that could do a sustained denial-of-service attack --

Mr. Bucshon. Okay.

Mr. Corman. -- in any crisis. It is not even the deaths per se; it is the crisis of confidence in the public to trust these --

Mr. Bucshon. So, I guess the last question I have is, briefly, creating a separate healthcare ID for all of us based on either biometrics or based on a number or something versus our Social Security number, for example, would that improve the ability to protect non-medical information that is in our health records from cyber-attack? Mr. McMillan?

Mr. McMillan. No, sir. If that information is still in that record and I can misappropriate those records, then I can still use that information.

I think what Marc was referring to -- and I will let him answer that -- but I think what he was referring to is that, if we have that unique identifier, then we could remove a lot of that personal information that today is in there just for the purpose of identifying the patient. So, think of it as --

Mr. Bucshon. But that could be important.

Mr. McMillan. Think of it as the ID cards that veterans now have, I, as a veteran, and other veterans have or as Medicare/Medicaid now have. They have taken the Social Security number off of those cards.

Mr. Bucshon. Okay.

Mr. McMillan. Right? Why have they done that? Because it put that number at risk.

Mr. Bucshon. Okay.

Mr. McMillan. Why do we have it in the health record?

Mr. Bucshon. I am over time. So, I will yield back, Mr. Chairman.

Mr. Pitts. The Chair thanks the gentleman.

I now recognize the gentlelady from Indiana, Ms. Brooks, five minutes for questions.

Mrs. Brooks. Thank you, Mr. Chairman.

I would like to build on my colleague from Indiana's questions and allow each of you to answer and give your opinion with respect to his proposal or idea that, Mr. Probst, you talked about earlier, having a specific identifier for healthcare records. Specifically, if you could each comment on what your views are of the pros and cons of that?

Mr. Probst. Well, I actually completely agree with what Mr. McMillan said. I mean, it is our opportunity to reduce the amount

of data that we have that, then, could be used for nefarious purposes. So, by having that national patient ID, that is going to help there.

From a clinical perspective, it is going to help massively because we want to be able to align our clinical data with the patients. And so, the national patient ID has huge benefit from a clinical perspective. But, from a security, I think Mac hit it perfectly.

Mr. McMillan. So, the other benefit that a unique identifier for patients would provide is in the form of access control. As we expand our sharing of information into things like population health, where we are going to have disparate physicians and other individuals touching a record for different reasons at different times, the old role-based access control rules that we have followed in the past are not going to be adequate anymore. We are going to have to go to more attribute-based access-control-type principles.

When we have everybody or everything uniquely identified in the system, whether it is an individual, whether it is the patient, whether it is the physician, whether it is environmental factors, et cetera, I can now create rules that actually facilitate access quicker for that gentleman to get into the record that he needs to get into and assure the patient that he is the right physician that is looking at that information.

Mrs. Brooks. Thank you.

Mr. McMillan. So, unique identifiers are beneficial.

Mrs. Brooks. Thank you.

Any further comments, Ms. Burch or Mr. Corman?

Ms. Burch. Absolutely. The issue of patient matching and patient identification is something that HIMSS has been working on for a long time. We currently fund an innovator-in-residence at HHS in the Chief Technology Officer's Office to look at perfecting algorithms and other ways that you can identify patients and match patient information.

From the HIMSS perspective, we absolutely think there needs to be a national strategy for patient data matching. We don't believe that a unique patient identifier is the panacea solution for that problem.

Given the short amount of time, we can certainly share the research that we have done and the arguments that we have that may not support a unique patient identifier, but we do believe that there needs to be a serious look taken at what are new and emerging technologies around digital identity. What is right for healthcare?

So, we have for a long time been a proponent of GAO or some other group really looking at this issue from the standpoint of what is the right solution of healthcare, and it may be multi-solutions.

Mrs. Brooks. Thank you. We would be interested in receiving that research and seeing what some of those ideas are.

[The information follows:]

**********COMMITTEE INSERT 6**********

Mrs. Brooks. Mr. Corman, anything you would like to add?

Mr. Corman. Yes. I would concur that it is not a panacea. As someone representing the security research community, often we place too many hopes in the efficacy of these things. I will say it is important as a principle to reduce your attack surface and reduce how many copies of these things you have and how they are come as you are, do as you please. You know, the less data you have, the less exposed you are. So, that is a good principle.

But, typically, when you do something like this, you are just simply moving the focal point of the adversary. So, you would have to take a more strategic and holistic approach.

I also know there are some privacy concerns around the downside or unintended consequences of such things.

Mrs. Brooks. Thank you. I would be interested in knowing whether or not having what is proposed under this bill, 5068, would that help the federal government become more innovative with respect to security if we adopted this proposal for HHS to create this new office specifically? Do you think that would improve the innovation? I am all about innovation in government, and I am curious whether or not this could actually help promote some more innovation in our systems.

Mr. Corman. My immediate instinct is no. I think it is a very different role. It is going to be a more operational role for the agency as opposed to the genesis of new and holistic ideas

for the industry.

Mrs. Brooks. But, with respect to security -- and maybe I should go to you, Ms. Burch. You were talking about innovation research and work that is being done with respect to security. Is that correct?

Ms. Burch. Yes, I was speaking to the importance of the security aspect and being foundational to the innovation work that is happening. So, if you don't have a strong security architecture, patients won't trust sharing their information. You don't have the information to feed the research pipeline, and then, you ultimately don't get to cures.

So, we think a CISO position within HHS that is empowered to work both internally and externally is critically important.

Mrs. Brooks. Thank you, and I am sorry my time -- I yield back my time. Thank you.

Mr. Pitts. The Chair thanks the gentlelady.

That concludes the questions of the members present. We will have further questions, follow-up, and other members will submit them to you in writing. We ask that you please respond promptly. And that means members have 10 business days to submit questions for the record. So, they should submit their questions by the close of business on Thursday, June the 9th.

[The information follows:]

**********COMMITTEE INSERT 7**********

Mr. Pitts. We will also be consulting with HHS and work collaboratively and bipartisanly.

And we thank you very much. This has been a very important and complex really issue that we must deal with. Thank you very much for your testimony.

Without objection, this hearing is adjourned.

[Whereupon, at 11:55 a.m., the subcommittee was adjourned.]