AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

EXAMINING CYBERSECURITY RESPONSIBILITIES AT HHS

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MAY 25, 2016

Serial No. 114–150

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
21–352 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
Vice Chairman
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
CHRIS COLLINS, New York
KEVIN CRAMER, North Dakota

FRANK PALLONE, Jr., New Jersey
Ranking Member
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY McNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJÁN, New Mexico
PAUL TONKO, New York
JOHN A. YARMUTH, Kentucky
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California7

SUBCOMMITTEE ON HEALTH

JOSEPH R. PITTS, Pennsylvania
Chairman

BRETT GUTHRIE, Kentucky
Vice Chairman
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
CATHY McMORRIS RODGERS, Washington
LEONARD LANCE, New Jersey
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILLY LONG, Missouri
RENEE L. ELLMERS, North Carolina
LARRY BUCSHON, Indiana
SUSAN W. BROOKS, Indiana
CHRIS COLLINS, New York
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

GENE GREEN, Texas
Ranking Member
ELIOT L. ENGEL, New York
LOIS CAPPS, California
JANICE D. SCHAKOWSKY, Illinois
G.K. BUTTERFIELD, North Carolina
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
DORIS O. MATSUI, California
BEN RAY LUJÁN, New Mexico
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY, III, Massachusetts
TONY CÁRDENAS, California
FRANK PALLONE, Jr., New Jersey *(ex officio)*

CONTENTS

WITNESSES

SUBMITTED MATERIAL

EXAMINING CYBERSECURITY RESPONSIBILITIES AT HHS

WEDNESDAY, MAY 25, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON HEALTH,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2123, Rayburn House Office Building, Hon. Joseph R. 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; James 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 Advisor, Health; Josh Trent, Deputy Chief Health Counsel; Jessica Wilkerson, Professional Staff Member, Oversight and Investigations; Kyle Fischer, Democratic Health Fellow; Timothy Robinson, Democratic Chief Counsel; Samantha Satchell, Democratic Policy Analyst; Andrew Souvall, Democratic Director of Communications, Outreach, and Member Services; and Arielle Woronoff, Democratic Health Counsel.

Mr. PITTS. The subcommittee will come to order.

The Chair recognizes himself for an opening statement.

OPENING STATEMENT OF HON. JOSEPH R. PITTS, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

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 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 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.

[The prepared statement of Mr. Pitts follows:]

PREPARED STATEMENT OF HON. JOSEPH R. PITTS

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 lookogut 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, 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 sySSstems 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, Reps. 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, and many industry experts such as PricewaterhouseCoopers now recommend that CIOs and CISOs be separated "to better allow for internal checks and balances."

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'd 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 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 to discuss a bill that will help raise the visibility and priority of information security across the Department.

[H.R. 5068 appears at the conclusion of the hearing.]

Mr. PITTS. 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 cybercriminals. 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 nonpublic HHS Office of the Inspector General reports detailing 7 years of deficiency across HHS' information security programs.

It is impossible to completely eradicate the threat of cyberattacks, 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 Government agencies to operate efficiently. The legislation we are examining today, which I introduced along with Ms. Matsui, would restructure HHS' 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, 5 minutes for an opening statement.

OPENING STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

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 our 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' perspective would have greatly enhanced our evaluation of the current cybersecurity improvement 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 is doing to enhance cybersecurity, including both defensive and offensive capabilities.

[The prepared statement of Mr. Green follows:]

PREPARED STATEMENT OF HON. GENE GREEN

Cybersecurity represents a current and growing threat as our economy and everyday lives become more digitized.

From the 2014 breach of the Office of Personnel Management and high-profile private sector breaches of companies like Target, JP Morgan Chase, and 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 technology security management remains a challenge for all Federal agencies.

The principle 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 "consummate 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 (CISA) as part of the Consolidated Appropriations Act in December 2015.

CISA required the Secretary of HHS to review and report a plan for addressing cybersecurity threats and designate a clear official who is responsible for leading and coordinating efforts within HHS and the health care industry.

The law also established the Health Care Industry Cybersecurity Task Force.

Members were recently appointed to the task force and will deliver the finalized report by March of 2017.

We should let HHS carry out the provisions outlined in CISA.

I am a bit surprised by my colleagues' decision to have a hearing today on H.R. 5068, the HHS Data Protection Act.

This legislation was recently introduced by Representatives Billy Long and Doris Matsui, and I thank them for their leadership on this issue.

Unfortunately, the last-minute timing of this hearing made it impossible for the administration to testify.

Having HHS' perspective would have greatly enhanced our evaluation of current cybersecurity improvement efforts and of the legislation, since HHS would be the 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 is doing to enhance

Thank you, and I yield 2 minutes to my colleague from California, Congresswoman Doris Matsui.

Mr. GREEN. 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 cyberdefense 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 securely 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, 5 minutes for an opening statement.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

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 appears at the conclusion of the hearing.]

Mrs. BLACKBURN. As Chairman Burgess said, interoperability is 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, 5 minutes for an opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

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 cyberattacks 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. Your written testimony will be made part of the record. You will each have 5 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, Mr. Mac McMillan, Chief Executive Officer, CynergisTek, Inc.

Again, thank you for coming.

Mr. Corman, you are recognized for 5 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; MARC PROBST, VICE PRESIDENT AND CHIEF INFORMATION OFFICER, INTERMOUNTAIN HEALTHCARE, ON BEHALF OF THE COLLEGE OF HEALTHCARE INFORMATION MANAGEMENT EXECUTIVES; AND MICHAEL H. (MAC) McMILLAN, CHAIRMAN AND 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 cybersafety in the Internet of Things called I Am The Cavalry, 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 cyberphysical 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 Mr. Corman follows:]

Statement of Joshua Corman

For the House Energy and Commerce Committee's Subcommittee on Health
"Examining Cybersecurity Responsibilities at HHS"

May 25, 2016

Opening:
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 for the Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security at the Atlantic Council – a non-partisan, international policy think tank. I am also a Founder of I am The Cavalry (dot org) – a grass roots, cyber safety volunteer focused on public safety and human life in the internet of things. Additionally, I am an adjunct faculty for CISO Certificate Program at Carnegie Mellon University's Heinz College where I've worked with dozens of CISOs at a time. Lastly, I am currently serving on the HHS Cybersecurity Task Force – initiated by Congress in the Cybersecurity Act of 2015.

Over the past 15 years, I've been a staunch advocate for the role of CISO (Chief Information Security Officer) – an increasingly difficult role. A significant portion of my research and career has been focused on the vanguard of emerging threats, and challenges affecting cybersecurity as well as identifying, advancing, and originating new and more effective responses to these growing challenges. As such, I've worked deeply with many of the Fortune 50, 100, and 1000 – on emerging issues such as the rise of cybercrime, the rise of nation state espionage, the rise of Anonymous & hacktivism, and the growing exposures to cyber safety and national security as we become increasingly dependent on the Internet of Things.

I say all of this, because I've had a front row seat to the evolution of the role of a CISO (and related titles and duties: ISO, CSO, CRO, Risk Management, Director, etc.). While there is no "one true path" to success, there are a number of factors which contribute to the overall success of a Cyber Security program. What I hope to do here today is to frame a few of those factors for the Subcommittee, to explore some of the costs/benefits of alternative reporting structures to the CIO, to speak to the value of experimentation in this evolving space, and then to answer any questions that you may have as you consider your choices.

Cybersecurity context in 2016:
It is worth noting that Cybersecurity is a relatively nascent field – and is having a very difficult time rising to meet the challenges. High profile failures in the private

sector and in governments are becoming quite clear. About 100 of the Fortune 100 have lost intellectual or trade secrets to foreign industrial and nation state adversaries. Most Merchants have had a breach of credit cards – despite being compliant with "best practices" and industry compliance regulations like PCI DSS (Payment Card Industry Data Security Standard). Breaches are getting bigger like Target and Ashely Madison. Breaches are hitting Federal Agencies like the Pentagon and OPM. Breaches are getting dangerous as we connect everything in the Internet of Things – such as the denial of patient care at Hollywood Presbyterian Hospital in California due to Ransomware. The Internet of Things is where bits & bytes now meet flesh & blood. In fact, the problem statement which caused me to form "I am The Cavalry" was:

"Our dependence on connected technology is growing faster than our ability to secure it – in areas affecting public safety and human life."

As society (and the government) increasingly depends upon IT, the importance of effective cybersecurity must also rise in kind. In the case of HHS, the consequences of failure may bleed into public safety and human life. We must be at our best.

It is hard to argue that we're (collectively) doing a very good job. A situation like this merits experimentation, innovation, and even a grand challenge – to ensure we can enjoy the promise of connected technologies (versus the perils of getting them wrong). It seems prudent to look at what the best are doing and to do controlled experimentation.

Factors which enable an effective CISO and Cybersecurity program:
Some of the factors contributing to the success of a cyber security program include:

1) The individual CISO's qualifications and experience
2) The reporting structure (e.g. to the CIO or others) <- *in focus today*
3) The relationships the CISO maintains across key executive stakeholders
4) CEO and Board level visibility and prioritization
5) The application of Risk Management principle versus blind, minimum compliance to standards and "best practices".

6) The ability of the CISO to both influence IT and business choices in advance – versus react to/inherit the downstream consequences of indefensible choices

Migration away from reporting to the CIO:
Regarding the #2 "Reporting structure", it is important to note there is not "one path to success". While CISOs can be successful reporting to various different executives, there has been a migration *away* from the more historical relationship under the CIO and *toward* other formats such as to the General Counsel, CFO, CEO, and the Board of Directors, etc. - including dotted lines and the like. In general, the belief is that a CISO reporting to a CIO is a structural conflict of interest – as there can be tensions between their missions, their performance objectives, and their budgets.

Availability and Uptime: The CIO is (in part) measured on the availability of IT services. In contrast, the CISO may need to temporarily interrupt said service in order to test for exploitable weaknesses – or to patch and update vulnerable systems to avoid successful exploitation.

Deployment of Services: The CIO may be held to deploy new services within an acceptable, projected time frame. A lack of acceptable security and/or compliance readiness may merit delays to the launch of said services. Worse, even the assessment of security and/or compliance can be skipped or compressed – affecting the overall outcome.

Cost Reductions: The CIO may wish to use lower cost alternatives for IT (Information Technology), and if they fail to properly factor the ability to meet security and/or compliance requirements, they may see the CISO as an obstructionist and/or a budget risk.

Zero Sum Budgets: The CIO has a dedicated budget, and they tend to prioritize more IT staff and more IT purchases than over more security staff or security reduction. It is not uncommon for a CIO to state: "We will only approve compliance mandatory security spending and not one penny more." First, compliance is no proxy for security or resilience against attackers. Second, compliance regimes can't possibly inform the agency specific or business specific risks and objectives – which require broader Risk Management practices. More importantly, this approach has the mistake of focusing only on regulated data – and often misses less replaceable asset types such as intellectual property, trade secrets, sensitive organizational data, and even cyber physical systems damage and safety implications (depending upon the industry/use case).

NOTE: This should not suggest that Cybersecurity should be expense. On the contrary, intelligent selection of more defensible IT , smarter security by design architectural choices, complexity reduction, operational excellence, and situational awareness can both improve cybersecurity and reduce costs and wastes in the agency or business.

IT tunnel vision: While historically, CISO mostly focused on IT risk, the modern CISO must factor for other types of risks, mission/business objectives, and the like. An effective and comprehensive Risk program must span multiple disciplines

Alternative Reporting Structures for the CISO:
Each reporting structure comes with trade-offs and advantages/disadvantages. I've often joked that after 2 years under each – in rotation – you just might achieve a full security program.

There have been dozens of articles and studies recently showing evidence of the gains organizations get from reporting structures (other than CIO). This article highlights "Seven reasons the CISO should report to the CEO and not the CIO" http://www.cio.co.uk/it-security/seven-reasons-ciso-should-report-ceo-not-cio-3634350/

It highlights two oft quoted metrics from a PWC Study, namely:

- Organizations where the CISOs report to CIOs have 14% more downtime due to security incidents, according to a study by PwC.
- Organizations where the CISO reports to the CIO have financial losses that are 46% higher, according to the same PwC research.

For these or others, I can provide anecdotes and examples – as merited. Here are a few simple examples:

General Counsel: CISOs who previously could not find support for anything but regulated data and/or compliance minimums, find that reporting to the General Counsel affords them more attention to trade secrets, intellectual property, sensitive organizational data, and anything deemed "material". This also elevates risks closer to board level attention.

CEO: With a direct line to the CEO, it is often easier to truly align the program to business priorities and objectives. Also the CEO is better poised to explicitly resolve tensions between competing priorities or trade-offs. It doesn't hurt to drive a culture of security when the top executive is making it a priority – all the way at the top. The odds of informing lower risk business and IT moves before they are made go up (versus reacting to less tenable or defensible choices after they are too late to materially improve).

CFO: Given the scrutiny and legal consequences introduced upon CFOs of publically traded firms via, for example, Sarbanes-Oxley, working for a CFO often affords you the permission and rigor of using audit functions and the internal gravitas they convey. This is useful for streamlining the more established aspects of a cybersecurity. In theory, this will liberate the CISO to do better on emerging and less established parts of their programs. However, I have seen a CFO reporting structure create a tunnel vision on the easy-to-audit-only bits.

The value of experimentation:
IT is in a constant state of flux and improvement. It is one of the fastest moving parts of the global economy. At the vanguard of this innovation is a movement called DevOps - short for the union and aligned incentives of software Development (Dev) and IT Operations (Ops). In fact, DevOps is being further extended by some (including me) into Rugged DevOps - a further Union with the Rugged Software Manifesto and adopters.

Core to their philosophy and success is a spirit of continuous experimentation and improvement. Fail Fast, Iterate. An advantage of controlled experimentation is one can "fail small" with little downside risk, and uncover very large upsides which can be later replicated and scaled. An HHS reporting structure change, if successful, could reveal a pattern worth repeating in other agencies. Einstein is quoted saying that insanity is doing the same thing over and over but expecting different results. The modern Lean and DevOps cultures have fully integrated this mindset and continue to shatter expectations of what was previously thought possible. Combined with the private sector trends toward more effective CISO reporting structure models, a controlled experiment in HHS may carry little downside - especially if objectives/measurements are established early and tracked.

Members may have heard about experiments within the federal government like the GSA program known as 18F – which is bringing modern DevOps principles into Federal IT. One of their early projects with DHS USCIS (US Citizenship and Immigration Services). The USCIS CIO Mark Schwartz is enjoying tremendous results at a more nimble, responsive, and less wasteful approach to IT. Part of the hope of such experiments is to fail small – and also to find new and more effective patterns which can later be applied to more parts of government.

Lastly, in the context of a DevOps culture, there is an increased "flattening" of organizational relationships which may diminish the importance of exactly where the CISO reports, but in a more hierarchical and traditional context, the negative effects of being underneath a CIO may be more pronounced.

Mr. PITTS. The Chair thanks the gentleman.

I now recognize Ms. Burch, 5 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 America 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 as 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 5 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 5-year survivor of a rare brain tumor, and to the HIMSS 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 Ms. Burch follows:]

HIMSS®

Testimony before the United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Health

Hearing on "Examining Cybersecurity Responsibilities at HHS"

May 25, 2016

Statement of Samantha Burch

Senior Director of Congressional Affairs

Healthcare Information and Management Systems Society

Chairman Pitts, Ranking Member Green and Members of the Subcommittee - Thank you for the opportunity to testify today on behalf of the Healthcare Information & Management Systems Society (HIMSS) regarding our support for 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 (IT). In North America, HIMSS focuses on health IT thought leadership, education, market research, and media services. Founded in 1961, HIMSS North America encompasses more than 64,000 individuals, of which more than two-thirds work in healthcare provider, governmental, and not-for-profit organizations, plus over 640 corporations and 450 not-for-profit partner organizations, that share this cause.

From our perspective, the organizational change included in this legislation would mark an important step in elevating the critical importance of information and cybersecurity within the Department of Health and Human Services (HHS).

Today's hearing on the HHS Data Protection Act begins a critical conversation that mirrors conversations occurring in healthcare organizations regarding the most effective approach to organizational governance to ensure optimal data flows, processes, and reporting for effective data protection and incident response. Many healthcare organizations now have a Chief Information Security Officer (CISO) and others are in the process of hiring a CISO as the healthcare organization's lead executive responsible for safeguarding data and IT assets.

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 impacted both the private and public sectors. Such incidents have included massive amounts of medical information being stolen and sold on the black market at a premium price, hacktivists defacing websites and launching cyber attacks for a political or a socially motivated purpose, hackers leveraging cyber extortion techniques to threaten the release of data in exchange for the fulfillment of a demand, and ransomware attacks holding medical information and data hostage in exchange for ransom.

Hacking the healthcare sector is now easier and more profitable than ever before. Organized cybercriminals are launching campaigns (such as targeted ransomware campaigns) targeting the healthcare sector. These cybercriminals are more sophisticated and agile than ever before, nearly equaling the sophistication and ability of the highly trained, nation state actor. Non-state actors are also gaining skill and launching effective cyber attacks. Additionally, even those individuals with a relatively low level of skill can successfully conduct cyber attacks (including those types mentioned previously), especially if healthcare organizations have unpatched systems and applications and have vendor default or null passwords—thus, leaving the door wide open to hackers. With so many threats and threat actors—as well as weak cybersecurity—healthcare organizations need a planned, coordinated approach to their cybersecurity programs and initiatives with a CISO at the helm.

HIMSS has spent nearly a decade working to support the healthcare sector's efforts to combat cyber threats. As part of this work, HIMSS released its inaugural 2015 HIMSS Cybersecurity Survey.[1] The concerns of healthcare provider cybersecurity personnel included phishing attacks (69% of respondents), negligent insiders (65%), advanced persistent threat (APT) attacks (63%), cyber-attacks (other than by nation state actors or hacktivists) (59%), and exploitation of known software vulnerabilities (53%). The key takeaways from these findings are that healthcare organizations must focus not only on protecting and defending against external cyber attacks, but also mitigating insider threat such as negligent insider threats (e.g., lost, unencrypted laptops and thumb drives) and malicious insider threats (e.g., breached data due to the actions of a rogue employee or contractor).

[1] http://www.himss.org/2015-cybersecurity-survey

The Evolving Role of the CISO

Elevating the Chief Information Security Officer (CISO) to be a peer of the Chief Information Officer (CIO) reflects the recognition that information security has evolved into a risk-management activity, historically the purview of other executives. In the private sector context, this recognition requires not just a revised job description, but a removal of the traditional subordination of the information security program to the information technology program to create a direct channel to the Chief Executive Officer (CEO), Chief Financial Officer (CFO), General Counsel and other senior executives. Such recognition requires:

- Independence from IT and removal of the inherent subordination of the information security program to the IT program under the current organizational structure,
- A direct channel to CEO, CFO, CCO, GC, etc., and,
- Direct reporting to the Board of Directors (BOD).

Direct reporting to an organization's CEO or other executive management facilitates management of security risk in the context of business risk, which can be operational, legal, and/or reputational. A significant security incident or breach may lead to a disruption in patient care or coordination of patient care. As such, it is clear that healthcare organizations need a cybersecurity leader to manage, as well as mitigate, security risk. Recent surveys find CISOs prefer to report to the CEO, and see the trend moving in that direction.[2,3]

Further, recent studies indicate there are real, positive impacts when the CISO has this reporting structure. "Reporting to the CEO or the Board of Directors, instead of the CIO, *significantly reduces downtime and financial losses resulting from cyber security incidents."*[4]

As far as operational impact, one study[5] found that "organizations in which the CISO reported to the CIO experienced 14% more downtime due to cyber security incidents than those

[2] http://www.darkreading.com/operations/top-infosec-execs-will-eventually-report-to-ceos-cisos-say/a/d-id/1321980

[3] http://www.klogixsecurity.com/ciso-trends/

[4] http://www.csoonline.com/article/2365827/security-leadership/maybe-it-really-does-matter-who-the-ciso-reports-to.html

[5] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html

organizations in which the CISO reported to the CEO." And, when the CISO reported to the CIO, financial losses were 46% higher than when the CISO reported to the CEO. In fact, having the CISO report to almost any position in senior management *other* than the CIO (Board of Directors, CFO, etc.) reduced financial losses from cyber incidents.

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. Additionally, information sharing must be encouraged and fostered within the organization. If the CISO does not know about a security incident or other issue, he or she cannot take action to address it.

Positioning HHS to Lead on Security

The August 2015 report[6] on Information Security at HHS prepared by the Committee's Majority Staff raised a number of important points related to the impact of the current HHS CISO reporting structure including lack of prioritization of security concerns and resulting constraints on operating division audits. The report also details the resulting internal security challenges and recent breaches incurred by the Department. This report reflects the seriousness and criticality of the discussion we are having today.

HHS needs security programs in place that support the specific business missions of its various agencies and operating divisions, including: the largest healthcare payer (CMS); the enforcer of HIPAA and holder of associated data on breaches and sensitive private sector company data (OCR); the agency responsible for protecting the public health by assuring the safety, efficacy and security of drugs, biologics, medical devices, products that emit radiation, etc. (FDA); and, the government health research agency (NIH). These agencies represent only a handful of the HHS operating divisions that have experienced data breaches.

[6] https://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Analysis/20150806HHSinformationsecurityreport.pdf

This move would break down silos and put the structure in place to allow the Department to move from an audit-driven approach to security to a proactive and ongoing enterprise business risk management approach to cybersecurity. We also believe that this organizational change would encourage information sharing, but again we emphasize that the organizational culture must also support information sharing about incidents and other potential security issues. Additionally, we believe that external information sharing is essential for HHS with other Federal agencies (such as DHS, FBI, and others) and also with private sector healthcare organizations about the threats which they are facing. Only with a community-based, holistic approach to healthcare cybersecurity can we, as the healthcare sector, collectively improve our security posture and, ultimately, successfully prevent and thwart breaches and other security incidents which may occur.

We see an *important external facing* role for the Office as well. These functions should include:

- Working with the healthcare sector and National Institute for Standards and Technology (NIST) on security best practices and minimum standards for the healthcare industry, consistent with Section 405 of the Cybersecurity Act of 2015, codified at 6 U.S.C. §1533.
- In collaboration with the Office of the Assistant Secretary for Preparedness and Response at HHS, facilitation of cyber threat data sharing between the government and the private sector, and among private sector healthcare entities.
- Development of the security architecture for national initiatives such as the Precision Medicine Initiative and 21st Century Cures.

Advancing Innovation through Trust

Healthcare organizations have come a long way in building the information technology capabilities to make the goals of 21st Century Cures a reality. The HIMSS Analytics Electronic Medical Record Adoption Model (EMRAM) is an 8-step process for tracking progress in building

EMR capabilities.[7] Since the implementation of the HITECH Act, rates of adoption of advanced EMR capabilities have increased significantly. Between Q2 2011 and Q4 2015, hospitals at EMRAM Stage 6 (defined as having structured physician documentation, full clinical decision support and full picture archiving and communications systems) increased from 4.0 percent to 27.1 percent.

The health information contained in these systems holds life-saving potential. These goals are particularly meaningful to me as a five-year survivor of a rare brain tumor and to the HIMSS organization after our colleague and dear friend lost her young adult 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 national program, trust in the system that will house and control access to the patient's data and trust in the public-private collaborative effort. Without this trust that the system will protect data and defend against threats, these efforts simply cannot succeed. Therefore, in order to effectively harness that potential, these ecosystems need a strong security architecture, designed and built-in *from the beginning* of development. The HHS CISO, appropriately positioned within the Department, and empowered with a mandate to focus both internally and externally, will be uniquely qualified to fulfill 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 the issue of cybersecurity at HHS. HIMSS believes the HHS Data Security Act marks a great opportunity to better position HHS to meet the growing challenges of securing health information, information critical to moving the nation's innovation and health agenda forward.

[7] http://www.himssanalytics.org/provider-solutions

Mr. PITTS. The Chair thanks the gentlelady.

Now I recognize Mr. Probst, 5 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 cybercriminals. 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 CISO 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 accountable 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 cyberhygiene 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 Mr. Probst follows:]

Testimony before the United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Health

Hearing on "Examining Cybersecurity Responsibilities at HHS"

2123 Rayburn Office Building

May 25, 2016

Statement of Marc Probst

Vice President and Chief Information Officer, Intermountain Healthcare

Board of Trustees Chairman, College of Healthcare Information Management Executives

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 the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) at the Department of Health and Human Services.

CHIME is an executive organization serving nearly 1,900 CIOs and other senior health information technology leaders at hospitals, health systems and clinics across the nation. CHIME members are responsible for the selection and implementation of the clinical and business technology systems that are facilitating healthcare transformation.

In addition to serving as chairman of the CHIME board of trustees, I am the CIO and vice president for 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; more than 200 clinics; and an insurance plan, SelectHealth, which covers approximately 900,000 lives in Utah and Idaho. Additionally, Intermountain Medical Group employs approximately 1,600 physicians, and about 4,000 other physicians are affiliated with Intermountain. Intermountain has over 36,000 employees.

Nationally, Intermountain is known for providing high quality care at sustainable costs. One way we achieve this is by identifying best clinical practices and applying them consistently. Research reviewed by John Wennberg, M.D., director emeritus of the Dartmouth Institute and founder of the Dartmouth Atlas of Health Care, showed that "Intermountain is the best model in the country of how you can actually change health care for the better." Dartmouth estimated that if healthcare were delivered nationally in the way it is provided at Intermountain, "the nation could reduce health care spending for acute and chronic illnesses by more than 40 percent." Essential to Intermountain's ability to deliver high-value coordinated patient care is the effective use of health information technology.

CHIME members take very seriously their responsibility to protect the privacy and security of patient data and devices networked to their systems. We appreciate the committee's interest in healthcare cybersecurity and the role that the Department of Health and Human Services plays in overseeing our rapidly progressing and innately innovative industry. We completely agree that cybersecurity must be a priority for HHS, just as it is for the nation's healthcare CIOs.

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 that, as they prioritize their efforts each day, I would rather have our data centers go completely dark — meaning a complete loss of all of our information systems — than to have a major breach of our data. 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 after-thought. Everyone across the organization needs to make it a priority. Even then, no system is perfectly secure.

To meet market pressures and regulatory requirements, including the Meaningful Use program and the shift to alternative payment models, CIOs have transformed their healthcare systems to become digital enterprises. This includes balancing the need to give clinicians immediate access to electronic protected health information while maintaining strict cybersecurity protocols. Some industries developed their information systems with a focus on security and restricted access (financial, government, security, etc.), however, in healthcare our systems were developed in a manner to facilitate rapid access to life saving data. This fundamental difference at the basic architecture and planned use of healthcare systems increases our challenge.

Further, there are several unique distinctions of the healthcare sector's data security environment that warrant consideration, including:

- Healthcare's highly-regulated environment
- The various settings where healthcare is delivered and data is required
- The range of resources available to devote to information technology and security
- Healthcare's unique financial models
- The frequency and volume of data exchange within healthcare delivery
- The increasingly mobile nature of healthcare technology and healthcare delivery
- Dependency on integration of systems and data (medical devices, niche applications, governmental requirements, business partners, etc.)

Cybersecurity in the Healthcare Industry

The Department of Homeland Security (DHS) deems healthcare one of the nation's 16 critical infrastructure sectors. The digitization of personal health information (PHI), the sharing of data encouraged and, in certain instances, required by the Meaningful Use program, and an increase in the "Internet of Things," has led to an increase in the number and types of cyber threats facing healthcare providers. For the second year in a row, criminal attacks were cited as the top cause of data breaches in the healthcare industry, with 50 percent of the breaches resulting from a criminal attack and 13 percent due to a malicious insider.[1] CIOs and CISOs face countless other malicious malware attacks on a daily basis, including Trojans, viruses, worms, and more. New threats will continue to arise, some can be anticipated while others will not, thus the notion of zero-day threats.

Meanwhile, providers with very limited resources, struggle to balance the huge demands for cybersecurity technology and information risk management programs. Threats to healthcare organizations are growing more sophisticated every day and too many health systems are not properly equipped to combat the myriad of attacks that could penetrate their networks. Even large healthcare delivery organizations that have made significant investments in security programs may fall victim to bad actors. We have seen this with some of the largest retail organizations, financial institutions and even the federal government suffering large-scale breaches.

No industry can enable perfect security; rather organizations must enumerate and manage their risks. The healthcare organization and its IT security team are challenged with understanding every possible avenue of attack by which a hacker might gain access to the healthcare network,

[1] *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (Rep. No. 6). (2016, May 12). Retrieved May 12, 2016, from Ponemon Institute LLC website: http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1

whereas the hacker only needs to find and exploit one weakness. In many cases, that one weakness is preying upon the behaviors of individuals through social engineering. As many studies have shown, and as many organizations that conduct penetration tests and other social engineering assessments will attest, it is impossible to prevent every human being in an organization from falling prey to such an attack.

Internal Coordination to Combat Cyber Threats

Given the breadth and depth of cyber threats, it's paramount that all facets of a healthcare organization, from the information technology department to clinicians to the board of trustees and many in between coordinate efforts to improve the cyber hygiene of their organizations. While organizational and reporting structures vary by healthcare institution, coordination is imperative. The role of the healthcare CIO has evolved from being an IT director to an executive who is tightly engaged in nearly every facet of the enterprise. As such, CIOs have a holistic view of how various pieces of the health system are connected. That perspective is critical to providing a safe and secure environment, whether it is finances or clinical care.

As I mentioned earlier, at Intermountain, the CISO reports directly to me, the 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 (Security Operations Center, Perimeter Services, etc.). Working across information systems (I.S.) operations ensures that the technical components required for cybersecurity are in place and managed. The interpretation of regulations, rules, corporate policy, procedure and *development of 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 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 developed a cooperative model for cybersecurity that insures appropriate checks and balances, but facilitates high levels of cooperation in achieving a more secure environment. This works at Intermountain. The focus isn't on the CISO's reporting structure. Rather, what's 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, Penn State Health System and Penn State College of Medicine, where the CISO reports to the CIO. The chosen structure was selected to build a strong cybersecurity program and transition to an IT shared services organization with tighter discipline, structure and process focus. This partnership ensures tight integration and solid support for the cybersecurity program across the entire IT team. Notably, the CISO established a "Cyber Security Advisory Council" that includes a number of key leaders from the organization. This group serves as the CISO's operational leadership link, offering input and direction independent of the CIO even with a formal CIO reporting relationship.

To exemplify the variation across healthcare delivery organizations, consider the following examples:

- At a large children's hospital, the CISO reports to the data security officer in order to combine expertise in data analysis and to take a more proactive approach to security. The CISO has dotted-line reporting to the chief compliance and privacy officer.
- The CISO at a large health system operating in two states reports directly to the CIO. The CISO is not only responsible for cybersecurity, but also account administration and disaster recovery.
- The CISO for a multi-state provider reports to the chief technology officer, who then reports to an enterprise-wide CIO.
- CHIME members at several smaller organizations report that they have the dual role of CIO and CISO.

Where the CISO should report is highly dependent on how the role is defined by the organization. As I stated, at Intermountain, the CISO is responsible for developing and overseeing the implementation of the *technical strategy to achieve our security posture,* managing our security team and working with I.S. peers to assure that the technical components required for cybersecurity are in place and managed. A different department acting as a check and balance is responsible for regulatory interpretation and development of the requirements for cybersecurity. This is not unlike other technology solutions where end users who own operational controls define requirements and I.S. handles implementation. Other organizations may choose to combine these roles. In such situations, different reporting relationships may make sense. I feel strongly, however, that there must be a continuous check and balance.

According to a March 2015 survey, 63 percent of AEHIS members indicated that they report to the CIO. Meanwhile, 16 percent report to the CEO and 11 percent report to the chief financial officer (CFO). According to a 2015 ThreatTrack study of 200 C-suite executives, the CISO reports to either the CIO or the CEO. The survey shows the prevailing trend is to put the CISO under the CIO, with 55.5 percent of respondents saying their CISO reports to the CIO, an increase of 10 percentage points from 2014. That compares with 40.5 percent who report to the CEO, a drop from 47 percent in 2014[2].

Further, CIOs may manage various pieces of the organization's IT infrastructure; some may manage biomedical devices, while others may not. Given the variability in reporting structures across the industry, federal policies must enable organizations to employ protocols that best match their IT security needs and the organization's internal IT workflow. Thus, it is important to emphasize it's not enough to rely on reporting structure changes to initiate meaningful change, instead security must be an organizational priority for true change to be enacted.

Cyber Readiness at HHS

In many ways, healthcare information technology is a maturing industry and HHS faces similar organizational challenges as today's healthcare CIOs. CHIME is pleased with the important advances set forth in the Cybersecurity Act of 2015[3] that was signed into law with the

[2] *CISO Role Still in Flux: Despite Small Gains, CISOs Face an Uphill Battle in the C*-Suite (Rep.). (2015). Retrieved May 23, 2016, from ThreatTrack website: https://www.threattrack.com/getmedia/5d310c4c-aed6-4633-929f-0b5903d2bc79/ciso-role-still-in-flux.aspx

[3] Consolidated Appropriations Act, 2016, 113 741 § Improving Cybersecurity in the Health Care Industry - 405 (2015).

government funding package on December 28, 2015. Notably, HHS, by December 28, 2016, must present Congress with a report that identifies the individual who will be responsible for coordinating and leading efforts to combat cybersecurity threats. HHS must also present a plan from each relevant operating division with respect to how each division will address cybersecurity threats in the healthcare industry, and a delineation of how personnel within each division will communicate with each other regarding efforts to address such threats.

Just as healthcare institutions must coordinate efforts to thwart cyber threats, it is vital that HHS have a coordinated plan to address threats to the data and systems used and housed by the department. Further, the industry welcomes the direction Congress issued as it will mitigate some of the continued concern about contradictory or unclear guidance from different subdivisions of the department. Concerning the HHS Data Protection Act, CHIME suggests that such legislation account for the ongoing efforts within the agency to evaluate how best to coordinate efforts on cybersecurity.

Illustrating the need for improved coordination, CHIME members point to inconsistencies in the enforcement of the rules around the Health Insurance Portability and Accountability Act (HIPAA), the law governing privacy and security requirements providers must meet, as a major impediment to being able to implement sound risk mitigation strategies. The existing enforcement paradigm is heavily focused on compliance activities which in some cases actually make it harder for providers to commit resources to areas they deem to be worthy and critical. This can be a distraction or drain on already limited resources necessary to actually secure the numerous points of entry — medical devices, networks, EHRs. Variability around who is required to comply with HIPAA contributes to the difficultly providers face in securing each and every potential vulnerability.

HIPAA requires only three covered entities comply with the law: providers, payers, and healthcare clearinghouses. Business associates of these three entities must also commit to protecting PHI as part of their contractual relationships with covered entities. However, device manufacturers are not HIPAA covered entities. Our members often describe scenarios in which medical devices are deployed with default passwords, some of which are unable to be changed by the providers. This creates a situation where once the device is connected to a provider's network it can be easily penetrated by bad actors, potentially threatening the functionality and safety of the device and introducing risk to the overall system. Worse than that, it creates a clear and present danger to the health and safety of the patients who have entrusted us with their care.

In other instances, today's current rules are insufficient to ensure interconnected devices adequately protect patients from harm and fend off privacy, cyber and other security threats. Additionally, some medical devices operate on private networks, not controlled by providers, creating large holes in perimeters and firewalls. CHIME recommended in recent comments to the Food and Drug Administration (FDA) that enhanced collaboration between device manufacturers and healthcare delivery organizations is necessary, and that the FDA approval of high-risk devices should include an assurance that the data collected and shared by the device is secure and that the device is not an easy entry point to a health system's network, as has been proven to be the case today.[4]

HHS Data Protection Act

CHIME encourages the committee to fully evaluate the potential negative consequences that could result from making the HHS CISO a presidential appointment. We've seen other instances where politicizing a role can hamper an agency's ability to affect change. For instance, Marilyn Tavenner in 2013 became the first Centers for Medicare and Medicaid Services administrator to win congressional approval since Mark McClellan, M.D., in 2004. That lack of official leadership creates uncertainty in the industry. Additionally, as a former member of the Health IT Policy Committee, a federal advisory committee created under Health Information Technology for Economic and Clinical Health Act (HITECH), I witnessed firsthand how important initiatives for improving care delivery can get bogged down in politics and bureaucracy.

As a healthcare CIO, I again echo the importance of coordination. What's central to this conversation is meaningful coordination, avoiding any unintended consequences of complex reporting that instead may impede the coordination and flow of information necessary to thwart cyber threats.

I would also ask the committee to consider these additional and essential actions to help the nation's healthcare providers improve their cyber readiness:

1. **Provide Ample Time to Ensure Cyber Readiness.** We are rapidly increasing the interconnectedness of the nation's healthcare system, and the Meaningful Use program, particularly what is proposed in Stage 3, will only accelerate information sharing with new sources using untested standards. Meaningful Use requires providers under Stage 3 to facilitate patient access to their records through application programming interfaces (APIs). As such, providers will be required to provide this access to applications chosen by patients. The rapid proliferation of new applications connecting to the system will create a host of new entrance points into providers' systems and cybersecurity vulnerabilities.

   Rushing implementation of health IT raises patient safety and cybersecurity concerns. We believe it is premature to include such mandates in the Meaningful Use program given the lack of mature standards, especially relating to security. Therefore, CHIME suggests that Stage 3 start no sooner than 2019 to allow for additional time to ensure proper security protocols are in place before the widespread use of APIs is mandated.

2. **Incentivize security.** Budgetary constraints can severely hamper a hospital's ability to pursue sophisticated cybersecurity measures. As noted above, at some smaller organizations, the CIO also serves as the CISO and has few human and capital resources to allocate to security. In many cases, a hospitals total spend on health IT – everything from clinical IT systems to revenue cycle to data warehousing – only accounts for 3 to 5 percent of the total operating budget. Given the low degree of spending/resources for IT

[4] *Postmarket Management of Cybersecurity in Medical Device* [Letter sent April 21, 2016 to R. Califf, Commissioner, Food and Drug Administration]. Retrieved from https://chimecentral.org/wp-content/uploads/2014/11/CHIME-AEHIS-Letter-to-FDA-on-Device-Cyber.pdf

spending, policymakers should look for ways to encourage investment through positive incentives for those who demonstrate a minimum level of cyberattack readiness and mature information risk management programs. The federal government and the nation's largest retailers have found themselves victims of large-scale breaches, there's no question that healthcare providers are at a disadvantage especially as they transform to meet the demands of new payment models, many of which will lower hospital reimbursements. Can reimbursement schemes include cyber preparedness? Should MACRAs Clinical Practice Improvement activity list include security improvements? We believe so.

3. **Enabling the Use of a Healthcare-Specific Identification Solution.** Reducing the reliance on Social Security Numbers (SSNs) and other identifiable information that help bad actors execute fraud will immediately devalue health records on the black market. We need a healthcare identification solution that, if stolen, does not have the same potential for fraud and abuse. It is essential that Congress remove the language in the Labor-HHS Appropriations bill prohibiting HHS (in Sec. 510) from using any federal funds to "promulgate or adopt any final standard .... providing for the assignment of a unique health identifier for an individual." Technology has provided for alternatives to a numeric or alphanumeric identifier as a solution, and the government does not need to be the arbiter of the identification solution, but HHS must be able to provide technical assistance to private sector initiatives. Unfortunately, HHS has interpreted the annual funding ban to prohibit them from collaborating or assisting with private sector efforts to improve patient identification on a national level.

   As health information increasingly flows across unaffiliated providers in order to coordinate care and as patients increasingly access and share their own data, it becomes even more important to ensure that patients are accurately identified and matched to their data. Ensuring correct patient matched is the first step toward effectively protecting and securing identities and mitigating fraud. CHIME encourages subcommittee members to work with the relevant appropriations committees to loosen the annual funding ban and allow HHS to work with the private sector to improve patient safety by enhancing the ability of the health sector to accurately match patients to their data.

   Recognizing that the industry can no longer wait, CHIME, through its Healthcare Innovation Trust, has launched a $1 million crowd-sourcing challenge to find a safe, private and secure approach to ensure accurate patient identification. The first phase of the competition saw 113 innovators from around the world submit ideas; more than 340 individuals and teams from 39 countries have registered for the National Patient ID Challenge. We expect to announce a final solution in February 2017.

4. **Reduce Regulatory Complexity**. Congress should pursue legislation that harmonizes other privacy, security and information risk management requirements to eliminate the complex patchwork of regulations across industries and state lines. Currently, healthcare organizations dedicate highly valuable resources to navigating these complexities to demonstrate compliance with its regulators; if a streamlined regulatory framework were

in place these resources could focus more time on actively monitoring and protecting against the daily variable threats.

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 ever evolving role of the healthcare CIO particularly as it relates to IT security. I look forward to answering your questions.

Mr. PITTS. The Chair thanks the gentleman and now recognizes Mr. McMillan, 5 minutes for your summary.

STATEMENT OF MICHAEL H. (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 On-Site 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 cybercriminals, hacktivists, and state actors engaged in cybertheft, 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 for 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 Mr. McMillan follows:]

Written Testimony of

Michael H. McMillan

Chairman & CEO, CynergisTek, Inc.

Before The

Subcommittee on Health

Committee on Energy and Commerce

U.S. House of Representatives

Examining Cybersecurity Responsibilities at HHS

May 25, 2016

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

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

Healthcare Needs Better Security

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

Security As A Top Down Priority

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

The Importance of Cyber Security Competence

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

Conclusion

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

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 5 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' 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. The 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, 5 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. OK. 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. OK. 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. OK. 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? OK.

Thank you, Mr. Chairman.

Mr. PITTS. The Chair now recognizes the Vice Chairman of the subcommittee, Mr. Guthrie, 5 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 that they have 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. OK.

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. OK. 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 emphasis 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 5 or 6 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, 5 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. OK. 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 the CISO 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. OK.

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, 5 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. OK. 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. OK.

Mr. CORMAN [continuing]. 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 5 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 5 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 cybercriminals, 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 cybercriminals 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 cybercrime 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 5 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 what hospitals should be doing. One of my early concerns before you made your comments was, OK, 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 [continuing]. 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 [continuing]. 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 cybersafety 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 cybersafety 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 5 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 role 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. OK. 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 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 [continuing]. They implement a security system?

Mr. PROBST. They should.

Mr. LONG. OK. Thank you all for your time.

And at this time, I am going to yield to the gentleman from New York, Mr. Collins, for 5 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 in 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, 5 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. OK? 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. OK. 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 cybercriminal 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. OK. 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. OK.

Mr. CORMAN [continuing]. 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 cyberattack? 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. OK.

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

Mr. BUCSHON. OK.

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, 5 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.

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.

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.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. FRED UPTON

The House Energy and Commerce Committee knows, better than I think just about any committee on the Hill, how important cybersecurity is. We've examined issues surrounding encryption, considered how best to address data breaches, and evendug deep into the protocols that run our cell phones, studying the vulnerabilities. We understand that our digital infrastructure is under attack—every second of every day—from actors of all motivations and levels of sophistication.

And that is why we are here today. Just like every other Federal department and private organization, HHS' networks and the information contained within them are under constant threat. At first glance, some may assume that we're holding today's hearing to chastise HHS for cybersecurity incidents that have happened in the past. We are not.

We are holding this hearing because we are looking to the future. We are holding this hearing to examine whether or not HHS has the opportunity, by embracing the reforms suggested in Mr. Long's and Ms. Matsui's bipartisan bill, not only to improve its own internal cybersecurity, but to become a leader in cybersecurity within the Federal Government and in the health care industry.

Consider this: the current structure for cybersecurity officials in place at HHS was originally mandated in 2003. The Internet looked radically different 13 years ago; smartphones were rare, cloud computing had yet to really take off, and the biggest threats to our digital infrastructure were viruses and worms, both of which could be stopped using standard firewalls and anti-virus software.

But the cyberworld is constantly changing, and the threats that we faced 10 years ago are not the threats that we face today. Instead, we face a daunting array of cybersecurity threats, from sophisticated thefts of personal information held by health care providers, to the hostage-taking of hospital networks and equipment by ransomware.

So I hope Members will take this opportunity to examine closely the issue before us, and give careful consideration as to whether or not an organizational structure established a decade ago is as agile, versatile, and powerful as we need it to be in order to combat the growing threats that we face.

Our oversight identified a problem. And we have a thoughtful solution in the HHS SData Protection Act to address it.

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

114TH CONGRESS
2D SESSION

H. R. 5068

To amend the Public Health Service Act to establish the Office of the Chief Information Security Officer within the Department of Health and Human Services.

IN THE HOUSE OF REPRESENTATIVES

APRIL 26, 2016

Mr. LONG (for himself and Ms. MATSUI) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To amend the Public Health Service Act to establish the Office of the Chief Information Security Officer within the Department of Health and Human Services.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "HHS Data Protection Act".

SEC. 2. CHIEF INFORMATION SECURITY OFFICER.

(a) IN GENERAL.—Title II of the Public Health Service Act is amended by inserting after section 229 of such Act (42 U.S.C. 237a) the following:

"SEC. 229A. CHIEF INFORMATION SECURITY OFFICER.

"(a) IN GENERAL.—Effective on October 1, 2016, there shall be a Chief Information Security Officer of the Department of Health and Human Services. The Office of the Chief Information Security Officer shall be within the Office of the Assistant Secretary for Administration of the Department of Health and Human Services. The Chief Information Security Officer shall be appointed by the President.

"(b) PRIMARY RESPONSIBILITY.—The Chief Information Security Officer, in consultation with the Chief Information Officer and the General Counsel of the Department of Health and Human Services, shall have primary responsibility for the information security (including cybersecurity) programs of the Department.

"(c) FUNCTIONS TRANSFERRED.—The Secretary shall transfer the functions, personnel, assets, and liabilities of the Chief Information Security Officer in the Office of the Chief Information Officer of the Department of Health and Human Services, as such position exists on September 30, 2016, to the Chief Information Security Officer.".

(b) EXECUTIVE SCHEDULE.—Section 5316 of title 5, United States Code, is amended by inserting after "Director, United States Fish and Wildlife Service, Department of the Interior." the following: "Chief Information Security Officer, Department of Health and Human Services.".

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary of Health and Human Services shall submit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Health, Education, Labor and Pensions of the Senate that details—

(1) the plan of the Chief Information Security Officer of the Department of Health and Human Services to oversee and coordinate the information security programs of the Department; and

(2) the steps being taken within each operating division of the Department, including the steps being taken by the chief information security officer of each such division—

(A) to implement such plan; and

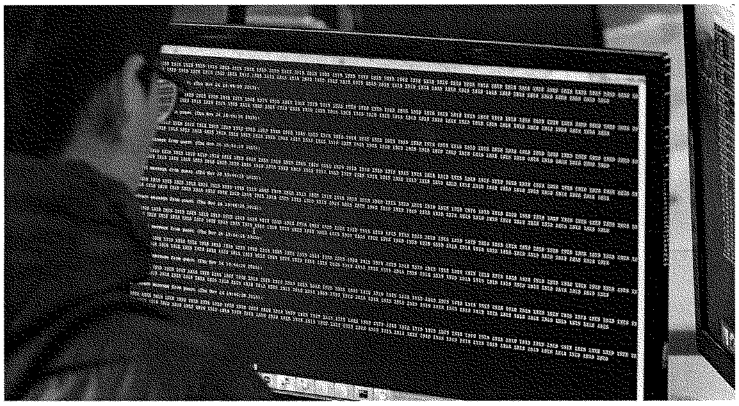
(B) to report to the Chief Information Security Officer on the status of such implementation.

(d) NO ADDITIONAL APPROPRIATIONS AUTHORIZED.—No additional funds are authorized to be appropriated to carry out this Act, or the amendments made by this Act. This Act, and the amendments made by this

Act, shall be carried out using amounts otherwise authorized or appropriated.

○

POLITICO



One of the main purposes of electronic health records is to encourage information sharing among doctors, so that patients can be looked after in a more holistic way. | Getty

Cyber ransom attacks panic hospitals, alarm Congress

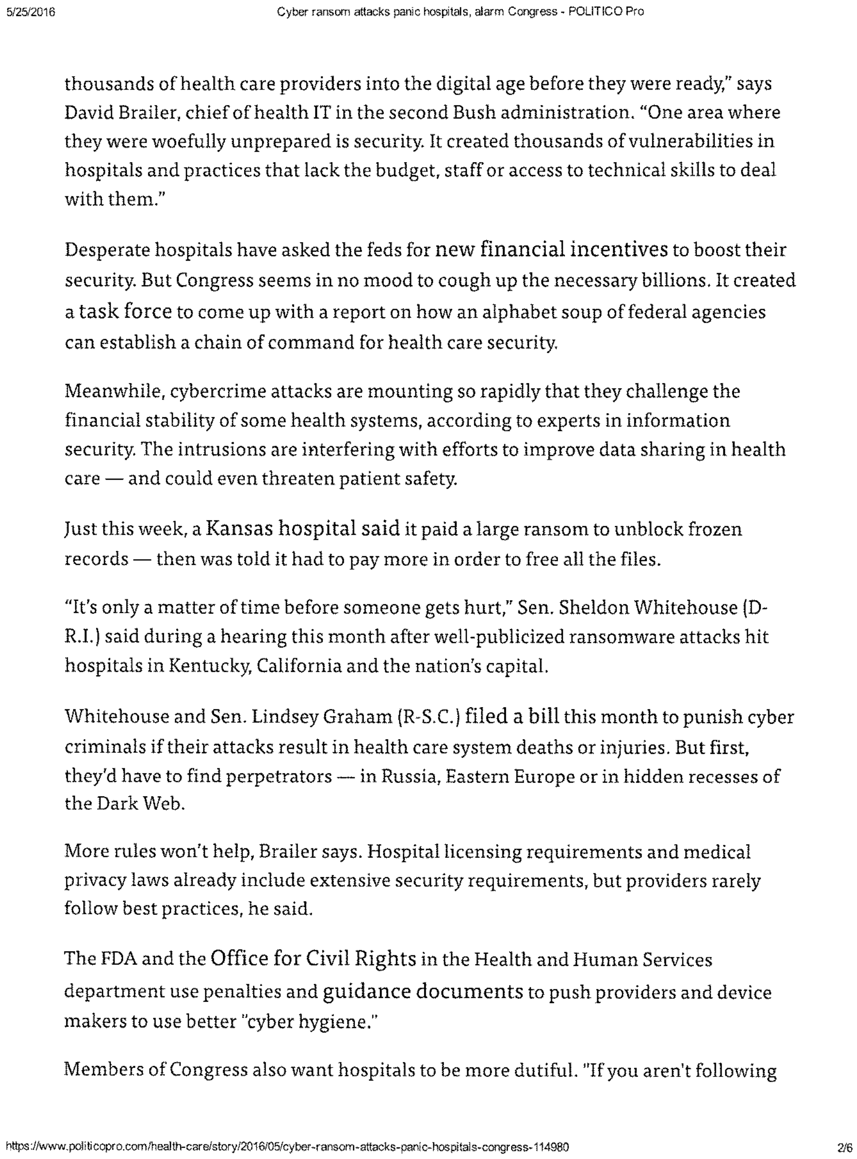
By **ARTHUR ALLEN** | 05/25/16 05:00 AM EDT

When the Obama administration pushed out a $35 billion incentive program to pay doctors and hospitals to convert to electronic records, the idea was to modernize the health care industry, not serve it up on a platter to cyber criminals.

But now, American hospitals face weekly ransom threats. If they don't pay up, files get frozen, surgeries delayed and patients sent across town. One of these days, someone could die as a result. And no one in government has a clear plan to handle it.

Such are the unintended consequences of shovel-ready projects.

The incentive program, which started paying out cash in 2011, "thrust tens of



thousands of health care providers into the digital age before they were ready," says David Brailer, chief of health IT in the second Bush administration. "One area where they were woefully unprepared is security. It created thousands of vulnerabilities in hospitals and practices that lack the budget, staff or access to technical skills to deal with them."

Desperate hospitals have asked the feds for new financial incentives to boost their security. But Congress seems in no mood to cough up the necessary billions. It created a task force to come up with a report on how an alphabet soup of federal agencies can establish a chain of command for health care security.

Meanwhile, cybercrime attacks are mounting so rapidly that they challenge the financial stability of some health systems, according to experts in information security. The intrusions are interfering with efforts to improve data sharing in health care — and could even threaten patient safety.

Just this week, a Kansas hospital said it paid a large ransom to unblock frozen records — then was told it had to pay more in order to free all the files.

"It's only a matter of time before someone gets hurt," Sen. Sheldon Whitehouse (D-R.I.) said during a hearing this month after well-publicized ransomware attacks hit hospitals in Kentucky, California and the nation's capital.

Whitehouse and Sen. Lindsey Graham (R-S.C.) filed a bill this month to punish cyber criminals if their attacks result in health care system deaths or injuries. But first, they'd have to find perpetrators — in Russia, Eastern Europe or in hidden recesses of the Dark Web.

More rules won't help, Brailer says. Hospital licensing requirements and medical privacy laws already include extensive security requirements, but providers rarely follow best practices, he said.

The FDA and the Office for Civil Rights in the Health and Human Services department use penalties and guidance documents to push providers and device makers to use better "cyber hygiene."

Members of Congress also want hospitals to be more dutiful. "If you aren't following good practices, the regulatory environment isn't going to save you," says Rep. Will Hurd (R-Texas), leader of the House Oversight cybersecurity subcommittee. While FBI and other agencies can do better at sharing threat intelligence, "health care has to help itself."

More federal inspections might increase readiness, but none of these measures attack the underlying problem — the massive gap between the industry's needs and its resources, Brailer said.

Meanwhile, hackers are launching billions of health care-focused attacks. One major health system was bombarded with a million emails in March alone seeking to implant ransomware in its computers. A small Kentucky hospital had 3,500 attacks on Mother's Day, according to Leslie Krigstein, vice president of the CHIME.

Last year there were 54 "zero-day," or brand new attacks; approximately once a week, in other words, hackers sent out an electronic bug so novel that no computer could recognize it.

Ransomware is of particular concern. In these attacks, hackers send out code that freeze computer files until the owner pays ransom in untraceable Bitcoins in exchange for a numeric decryption to unfreeze them. The attacks allow hackers to cash in quickly, whereas stolen medical records may be more difficult to monetize. (More than 100 million records were stolen in 2015 — some for sale on the black market or use in Medicare fraud, some by state actors, apparently for intelligence purposes).

Freakout in the C-Suite

For the first time, the threat of cyberattacks is grabbing the attention of senior health care executives, said Russell Branzell, CHIME's CEO, who says the executives are "freaking out" as we "enter into a security war for health care."

Cybersecurity legislation signed into law last year allows health care companies to share information about threats they've encountered without risk of being sued for any data breaches they reveal. Other privately run organizations also serve this purpose.

But complying with such recommendations can require major investments —

millions to hire new security teams and consultants and to buy new software. Added security spending might mean forgoing a new MRI system, or delaying the hiring of new nurses.

“Cyberthreats are knocking on your door every time you open your laptop or your phone,” said Ty Faulkner, a cyber consultant. “If you aren’t monitoring and checking your data, I question whether you are following good business processes.”

But "many of our members can’t afford the technology and tools they need at this point,” said Branzell. “It’s moving so fast that you could update everything, spend way more than you’re budgeting for, then the next wave of bad guy stuff comes up and you’re already behind again.”

"If you peer into the dark minds of a lot of hospital executives, they are rolling the dice as to where they allocate their budgets," said Clinton Mikel, an attorney with Health Law Partners.

Health care firms are spending vast sums to lure chief information security officers away from the financial and energy sector. The job description hardly existed in health care two years ago — now there are 500 just in Branzell’s organization.

Some companies are hiring security consultants on a semi-permanent basis, said Mac McMillan, co-founder and CEO of CynergisTek — one of those firms. If they don’t spend that big dough, many worry, a criminal breach of their information could result in bankruptcy levels of litigation.

Cyber insurance protects against some costs, but underwriters won’t write a policy unless the hospital system can demonstrate it is already spending plenty to defend itself.

Successful attacks are inevitable, security experts say. They talk of techniques such as compartmentalizing software, so hacks can be confined to a small area of the computer system, or programs that detect unusual computer activity within an organization, signs a bug has already penetrated the system.

“Most organizations can’t do that for themselves,” McMillan said. “More and more, people are saying to us, ‘I want a partner’ because cybercrime has become an industry.”

Medical devices: A ripe target?

The targets of attack within health care are practically limitless. "It's hard to imagine a more complex and diverse environment than a hospital," said Dave Palmer of Darktrace, a company whose technology searches for unusual behavior within networks.

"You have doctors and staff walking around with tablets, millions of dollars worth of scanners and sensitive machinery, all of it digitally integrated. You have visiting consultants there, maybe only a few days a week. Staff, porters, cleaning people."

Users may not understand that bedside devices like monitors need to be secured, said Dennis Gallitano, a leading cyber attorney. Most cyber strategies are built around detecting and keeping out bugs, but "what about tunnels through the backdoor — a fax machine or pump?"

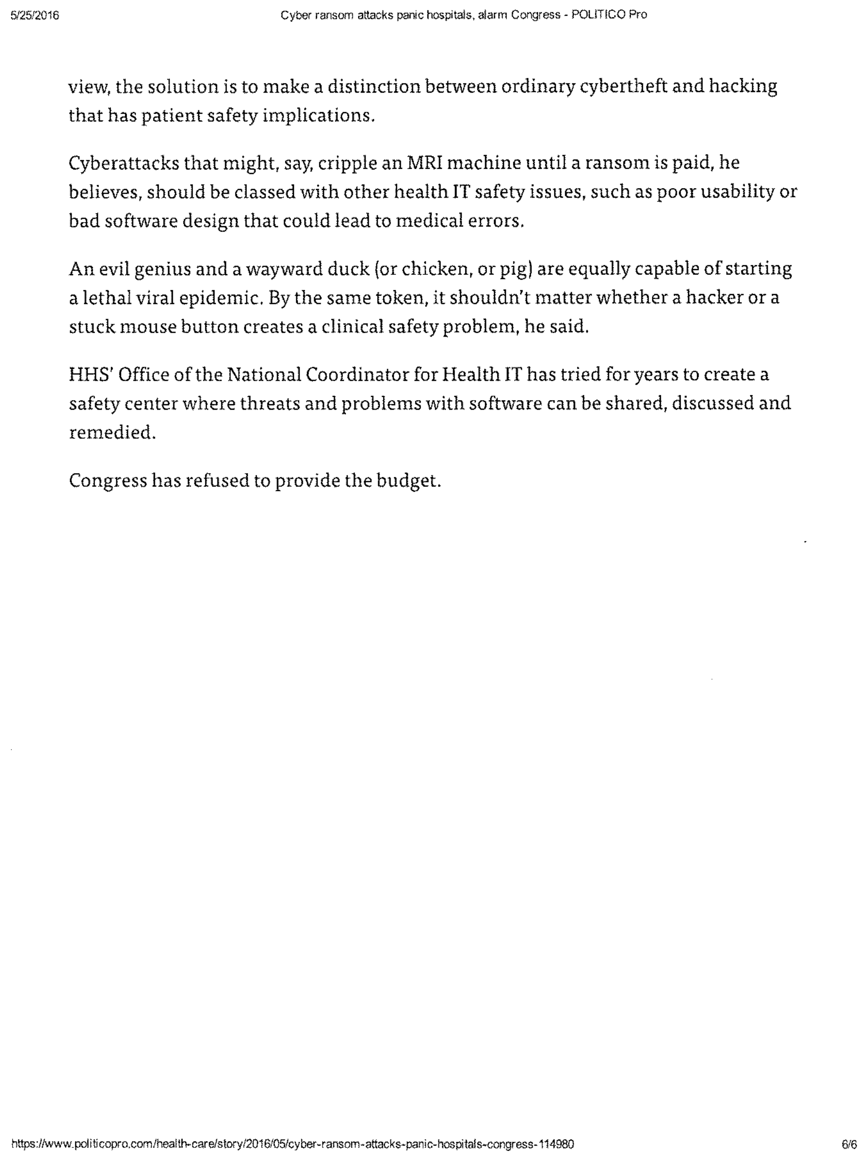
Device manufacturers are not required to meet the privacy and security standards of the Health Insurance Portability and Accountability Act (HIPAA); security experts say their protection is often lax, offering an attractive target for hackers looking for new ways into health systems. The FDA has begun working with manufacturers to improve device cybersecurity.

Security conflicts with transparency

One of the main purposes of electronic health records is to encourage information sharing among doctors, so that patients can be looked after in a more holistic way. Cyberthreats, some worry, could lead to a clampdown, because health care companies are leery of sharing data with institutions that might not be secure.

"There is very much a conflict in health care," Branzell acknowledged. "The traditional model is, 'Lock the world down.' That doesn't work in a world where we're being asked to become more and more transparent and engage with our patients ... With more patient engagement you've got people working from home on their Wi-Fi networks."

Security should not be used as an excuse to block transparency, says Fred Trotter, a hacker and data journalist who serves on HHS' Cybersecurity Task Force. In Trotter's



view, the solution is to make a distinction between ordinary cybertheft and hacking that has patient safety implications.

Cyberattacks that might, say, cripple an MRI machine until a ransom is paid, he believes, should be classed with other health IT safety issues, such as poor usability or bad software design that could lead to medical errors.

An evil genius and a wayward duck (or chicken, or pig) are equally capable of starting a lethal viral epidemic. By the same token, it shouldn't matter whether a hacker or a stuck mouse button creates a clinical safety problem, he said.

HHS' Office of the National Coordinator for Health IT has tried for years to create a safety center where threats and problems with software can be shared, discussed and remedied.

Congress has refused to provide the budget.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congreſs of the United States

Houſe of Repreſentatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515–6115
Majority (202) 225–2927
Minority (202) 225–3641

June 20, 2016

Mr. Josh Corman
Director
Cyber Statecraft Initiative
Atlantic Council
1030 15th Street, N.W.
Washington, DC 20005

Dear Mr. Corman:

Thank you for appearing before the Subcommittee on Health on May 25, 2016 to testify at the hearing entitled "Examining Cybersecurity Responsibilities at HHS."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on July 5, 2016. Your responses should be mailed to Graham Pittman, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to graham.pittman@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Joseph R. Pitts
Chairman
Subcommittee on Health

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

June 20, 2016

Mr. Josh Corman
Director
Cyber Statecraft Initiative
Atlantic Council
1030 15th Street, N.W.
Washington, DC 20005

Dear Mr. Corman:

Thank you for appearing before the Subcommittee on Health on May 25, 2016 to testify at the hearing entitled "Examining Cybersecurity Responsibilities at HHS."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on July 5, 2016. Your responses should be mailed to Graham Pittman, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to graham.pittman@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Joseph R. Pitts
Chairman
Subcommittee on Health

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

Attachment — Additional Questions for the Record

The Honorable Joseph R. Pitts

Throughout the hearing, members of the panel either made or agreed with the assertion that H.R. 5068 will not work in a vacuum; HHS must also have clear, effective, and enforced policies, procedures, and processes for ensuring that cybersecurity is a priority throughout the Department.

1. Please describe the policies, procedures, and processes that you believe HHS currently has in place for ensuring that cybersecurity is a priority throughout the Department.

A1: As an outside citizen, I lack meaningful visibility into HHS’s program. My expertise and context as a panelist was to contrast with all of my work with CISOs through the private sector and through my teaching for the CISO program at Carnegie Mellon Univesristy’s Heinze College. Anything I offer to this question would be speculative.

2. Are there policies, procedures, and processes that you believe HHS should adopt in order to be more effective with regards to cybersecurity?

A2: Every program and culture are different and involved trade-offs. My testimony was largely pointing at the difficulty in a CISO being fairly heard and acted upon. If there is a structural conflict of interest in place like reporting to a CIO – who has different (and often conflicting) incentives and measurements. As a baseline, the EO/NIST CyberSecurity Framework outlines several important program elements - but not necessarily the efficacy of its activities/controls on their own or as implemented in context.

3. Are there policies, procedures, or processes that you believe that HHS should consider reforming or removing in order to be more effective with regards to cybersecurity?

A3: Again, ss an outside citizen, I lack meaningful visibility into HHS’s program. Anything I offer to this question would be speculative. One promising and emerging practice I’d like to see considered by HHS and other parts of the US Government is the addition of Coordinated Vulnerability Disclsoure Programs. These proven programs from the private sector (an exemplar is Microsoft’s BlueHat program) invite independent, 3rd party researchers to looks for and report vulnerabilities to the affected party. This spring, the US Pentagon did a pilot “Hack the Pentagon” Boug Bounty to find weaknesses it’s websites. Such programs allow more scalable detection and discrete remediation of things the formal security programs may have missed. NTIA within Commerce has held a mutli-stakeholder program over the past year to capture and promote best practices for such programs. Additionally, the US FDA within HHS has encouraged Medical evice Manfucaturers to offer such Disclsoure Programs to maiuntain public trust and enhance Patient Safety.

Throughout the hearing, members of the panel emphasized that, in addition to its organizational structure, it is critically important the roles and responsibilities for officials within HHS in regards to cybersecurity are clear and effective.

4. Please describe the responsibilities and authorities that you believe the following HHS officials should have with regards to cybersecurity:

   - The Secretary of Health;
   A4a: Ultimate responsibility for the security of both HHS Infrastructure and the Confidentialy, Integrity, and Availability of important information and services – required to fulfill it's duties to the government and taxpayers. Make ultimate decisions where trade-offs are required between CIO and CISO – in these regards.

   - The HHS CIO;
   A4b: Factor all CyberSecurity objectives into the selection, deployment, and maintaininace of IT purchases and 3rd party relationships – in consultation with the CISO. CIO and IT teams often share operational responsibilities for instrumentation and monitoring of IT when it comes to security issues – and participate in disaster recovery, business continuity planning and exercises (for example).

   - The HHS CISO;
   A4c: Develop CyberSecurity Objectives, Programs, Policies, and Measurements, and Risk Management Functions – in consulation with executive and agency stakeholders – to support their missions. Enable, train, and consult with key stakeholders in the executive team and division leads to meet mutual targets.

   - Any other officials (such as the General Counsel, CFO, etc.).
   A4d: Consult with the CISO to identify top risk priorities and mission requriements. Bring your power and influence in support of Cyber Security and Risk Management Objectives. Ensure your parts of the organization internalize and act in accordance with thee objectives. As I indicated in my prio written testimonies, different Executive Stakeholders express different aspects of a complete program. E.g. General Counsel cares about keeping secrets secret. Procurment can enforce security criteria upon 3rd party suppliers. Etc.

In the hearing, the panel discussed the fact that, as currently drafted, H.R. 5068 makes the newly elevated CISO a presidential appointment. Concerns were raised about that, stating that it might overly politicize the position.

5. Would the position be more effective if it wasn't a presidential appointment?

A5: Given that the spirit of the H.R. 5068 was (in part) to remove any conflict of interest that affected the CISO's ability to objectively perform its required job functions, I would think this position should not be a political appointee.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115
Majority (202) 225-2927
Minority (202) 225-3641

June 20, 2016

Ms. Samantha Burch
Senior Director, Congressional Affairs
Healthcare Information & Management Systems Society
4300 Wilson Boulevard
Arlington, VA 22203

Dear Ms. Burch:

Thank you for appearing before the Subcommittee on Health on May 25, 2016 to testify at the hearing entitled "Examining Cybersecurity Responsibilities at HHS."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on July 5, 2016. Your responses should be mailed to Graham Pittman, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to graham.pittman@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Joseph R. Pitts

Joseph R. Pitts
Chairman
Subcommittee on Health

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

HIMSS
transforming health through IT

33 West Monroe St, Suite 1700
Chicago, IL 60603-5616
Tel 312 664 4467
Fax 312 664 6143
www.himss.org

July 5, 2016

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Pitts:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), thank you for the opportunity to testify before the Subcommittee at the May 25, 2016 hearing entitled "Examining Cybersecurity Responsibilities at HHS." HIMSS and our members look forward to working with you to ensure the healthcare sector has the tools, resources and structures in place to protect patients and their information from growing cyber threats.

Attached please find my responses to the follow-up questions submitted for the record. If you would like additional information, please contact me at sbburch@himss.org or 703-562-8847.

Sincerely,

Samantha Burch
Senior Director, Congressional Affairs
HIMSS North America

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

The Honorable Joseph R. Pitts

1. **Please describe the policies, procedures, and processes that you believe HHS currently has in place for ensuring that cybersecurity is a priority throughout the Department.**

The following information is based on the "Annual Report to Congress Federal Information Security Modernization Act (OMB, March 18, 2016)":

Anti-Phishing Defense and Other Defenses

- Web content filtering
- Quarantining or blocking messages to protect individual user machines and the system at large from the consequences of opening email messages infected with viruses or other nefarious programming

2. **Are there policies, procedures, and processes that you believe HHS should adopt in order to be more effective with regards to cybersecurity?**

HHS should adopt a department-wide, enterprise-level cybersecurity governance framework, which is fully implemented across the organization.

Based on the deficiencies cited in the March 2016 HHS OIG Report, "Review of the Department of Health and Human Services Compliance with the Federal Information Security Modernizations Act of 2014," the framework should have the following components:

- HHS' senior management should develop policies that address its risks with a "whole of organization" approach (i.e., taking into account risks from operational, legal, financial, and/or reputational perspectives and the confidentiality, integrity, and availability of information and assets). Additionally, regular accurate and thorough risk assessments should be conducted across the enterprise, taking into account people, processes, and technology within the enterprise and with external partners (to the extent such visibility exists). Based upon the results of the risk assessment, these results can be used to inform the policies senior management develops.
- HHS' mid-level management should add standards, baselines (i.e., minimum requirements), guidelines, and procedures to such policies. Security professionals can assist with adding such information.
- HHS' security professionals should implement the policies and associated standards, baselines, guidelines, and procedures.
- HHS' users should comply with such policies.
- At each level cited above, there should be a consistent approach to accountability to ensure compliance and full implementation of such policies. There should be formally defined, consistently applied sanctions for violations of such policies.
- At each level cited above, there should be a clear, consistent, and formalized approach to documentation. Not having a formalized documentation process and having appropriate and detailed documentation may expose HHS to potential liability for lack of due care and/or due diligence.
- At each level cited above, there should be a clear, consistent, and formalized approach to tracking and monitoring of initiatives and activities across the enterprise.

- Additionally, there should be oversight at each of these levels. What the policies state and what is done in practice should be made uniform across the Department.

HHS' senior management should provide oversight over the implementation of the policies.

- Contingency planning and disaster recovery should be addressed with a consistent, formalized approach. This should also be driven by senior management, fleshed out by mid-level management, and implemented by appropriate personnel.
- Awareness and training of workforce members across the enterprise should be mandatory to ensure that everyone understands and complies with policies, procedures, guidelines, and baselines, as appropriate.
- Finally, with all of these changes, the changes should be controlled (or managed) to control the risk (i.e., change management).

3. Are there policies, procedures, or processes that you believe that HHS should consider reforming or removing in order to be more effective with regards to cybersecurity?

The addition or enhancement of information sharing within the organization and with external parties (as emphasized in Section 405 of the Cybersecurity Act of 2015) should be encouraged, facilitated, and implemented in a formal enterprise-wide policy. Information can be shared with regard to obstacles or barriers in implementing policy or questions about how to uniformly apply policy. This feedback can be valuable and senior management and middle management, as appropriate, can modify policies and other items to make such tasks more feasible.

Information can be shared with regard to privacy and security incidents to more effectively mitigate incidents that occur. When a privacy or security incident does occur, HHS can become more resilient by using lessons learned from the incident and improving or revamping people, processes, and technology.

4. Please describe the responsibilities and authorities that you believe the following HHS officials should have with regards to cybersecurity:

Based on HIMSS' extensive experience working with private sector healthcare organizations, we the following responsibilities and authorities could apply to the roles identified below within HHS.

- **The Secretary of Health;**
  - Establish cybersecurity as a priority for the enterprise by ensuring that resources are appropriately allocated;
  - Facilitate the changing of the culture about cybersecurity throughout the enterprise;
  - Review regularly updated information about the state of cybersecurity and impacts on the Department; and,
  - Review of metrics that show progress with regard to the cybersecurity program
  - Provide ultimate oversight and accountability for the cybersecurity program and initiatives.

- **The HHS CIO;**
  - Ensure that technology is functional, operating correctly, and supports the operations of the Department;
  - Oversee the IT budget;
  - Oversee the IT lifecycle of software, hardware, and other resources;
  - Oversee the selection, vetting, and procurement of technology;
  - Oversee the inventory of IT assets and resources;
  - Oversee relationships with third party partners, vendors, and others relevant to IT operations;
  - Provide oversight to implementation of IT operational policies and procedures and ensures consistency across divisions, offices, and also throughout the enterprise; and,
  - Ensure appropriate and consistent documentation.

- **The HHS CISO;**
  - Oversee cyber threat, vulnerability, and mitigation information sharing with other Federal agencies and within the enterprise;
  - Oversee the assessment and management of risks;
  - Oversee physical, technical, and administrative security safeguards;
  - Oversee assessment and management of risks (including in view of the direction and guidance of senior management);
  - Oversee relationships with third party partners, vendors, and others relevant to cybersecurity;
  - Oversee the facilitation of information sharing about cyber threats, vulnerabilities, and mitigation information with private sector healthcare entities;
  - Oversee development of policies, procedures, baselines, and guidelines from a cybersecurity perspective;
  - Confer with senior privacy officials to safeguard the privacy of confidential or sensitive information, personally identifiable information, or classified information;
  - Confer with senior privacy officials about the handling of incidents;
  - Ensure that qualified cybersecurity personnel are hired and retained throughout the enterprise; and,
  - Develop, executes, and manages cybersecurity awareness and training programs for the entire workforce across the enterprise.

- **Any other officials (such as the General Counsel, CFO, etc.).**

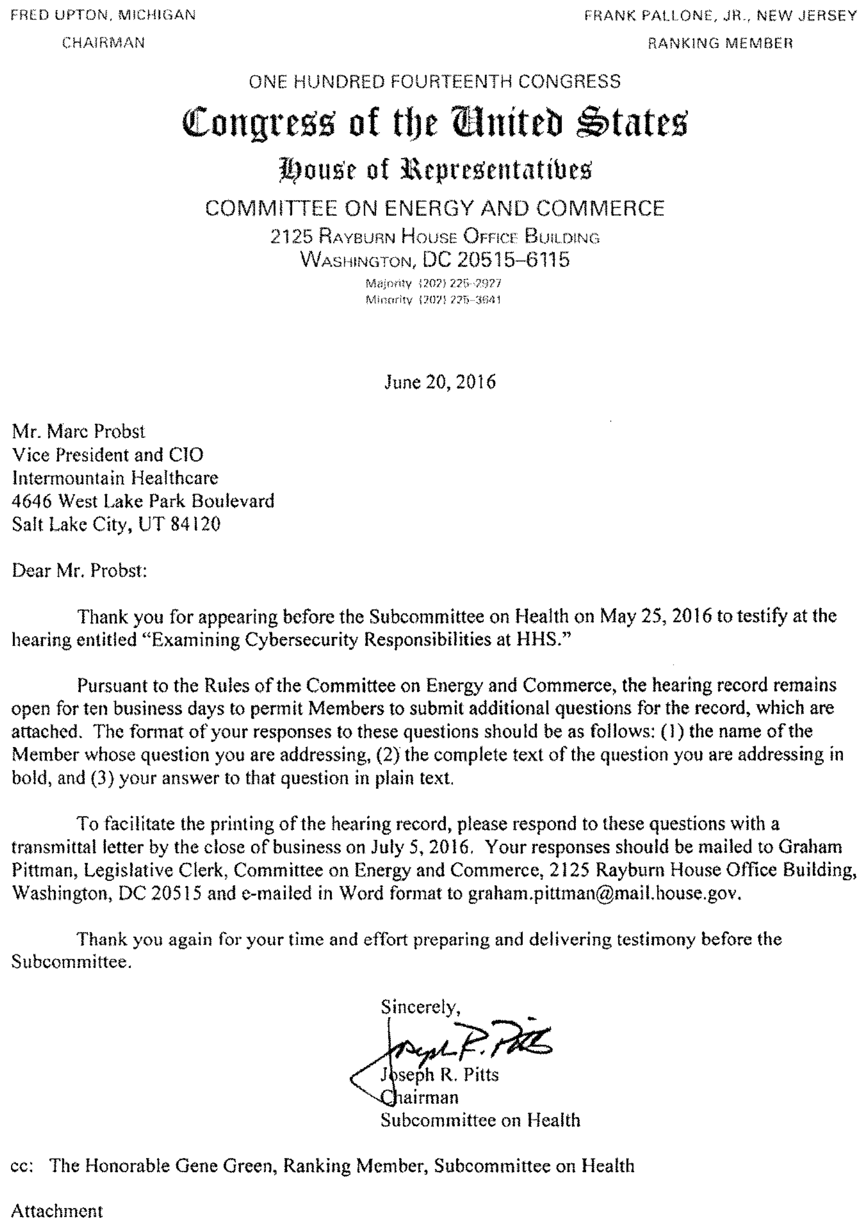
The General Counsel should work with other C-suite executives and the Secretary to ensure compliance with laws, regulations and contractual requirements. The General Counsel and staff also should also take due care and due diligence to ensure targets for enterprise-wide cybersecurity program are met and continuously monitored (including with regard to FISMA targets).

The CFO should ensure the development, execution, and oversight activities involving the budget and financial performance should include cybersecurity. The CFO should work with the CISO and CIO to ensure that all relevant factors are taken into consideration.

5. **In the hearing, the panel discussed the fact that, as currently drafted, H.R. 5068 makes the newly elevated CISO a presidential appointment. Concerns were raised about that, stating that it might overly politicize the position. Would the position be more effective if it wasn't a presidential appointment?**

Yes, the position would be more effective for a number of reasons including:

- The person would not be time-limited and policy, activities, and initiatives would not be rushed because of that time limitation.
- A person who is a permanent employee would afford continuity and less disruption to the organization.



FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congreſs of the United States
Houſe of Repreſentatives
COMMITTEE ON ENERGY AND COMMERCE
2125 Rayburn House Office Building
Washington, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 20, 2016

Mr. Marc Probst
Vice President and CIO
Intermountain Healthcare
4646 West Lake Park Boulevard
Salt Lake City, UT 84120

Dear Mr. Probst:

Thank you for appearing before the Subcommittee on Health on May 25, 2016 to testify at the hearing entitled "Examining Cybersecurity Responsibilities at HHS."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on July 5, 2016. Your responses should be mailed to Graham Pittman, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to graham.pittman@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Joseph R. Pitts
Chairman
Subcommittee on Health

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

June 30, 2016

The Honorable Joseph R. Pitts
Chairman, Subcommittee on Health
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Pitts,

Thank you for the opportunity to appear before the before the Subcommittee on Health on May 25, 2016, to testify at the hearing entitled "Examining Cybersecurity Responsibilities at HHS." CHIME and its members take very seriously their responsibility to protect their networks and patient data from cyber criminals. The hearing focused a critical and timely issue for our members. Attached please find my written responses to the questions for the record.

Sincerely,

[redacted]

Marc Probst
Vice President and Chief Information Officer, Intermountain Healthcare
Board of Trustees Chairman, College of Healthcare Information Management Executives

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

The Honorable Joseph R. Pitts

Throughout the hearing, members of the panel either made or agreed with the assertion that H.R. 5068 will not work in a vacuum; HHS must also have clear, effective, and enforced policies, procedures, and processes for ensuring that cybersecurity is a priority throughout the Department.

1. **Please describe the policies, procedures, and processes that you believe HHS currently has in place for ensuring that cybersecurity is a priority throughout the Department.**

Just as healthcare institutions must coordinate efforts to thwart cyber threats, it is vital that the Department of Health and Human Services (HHS) have a coordinated plan to address threats to the data and systems used and housed by the department. The Cybersecurity Act of 2015 calls on HHS to present to Congress within a year a report that identifies the individual who will be responsible for coordinating and leading efforts to combat cybersecurity threats. HHS must also present a plan detailing how each operational division will address cybersecurity threats in the healthcare industry, and a delineation of how personnel within each division will communicate with each other regarding efforts to address such threats.

The forthcoming coordination plan, in conjunction with the output of the Health Care Industry Cybersecurity Task Force, will be an important mechanism to evaluate current practices employed within HHS and help identify any weakness that must be addressed. Understanding these weaknesses will benefit both HHS and the industry.

In addition to the directive from the Cybersecurity Act of 2015, HHS launched an enterprise-wide information security and privacy program in fiscal year 2003 to help protect against potential information technology (IT) threats and vulnerabilities. The program ensures compliance with federal mandates and legislation, including the Federal Information Security Management Act and the President's Management Agenda. The HHS Cybersecurity Program plays an important role in protecting HHS' ability to provide mission-critical operations. In addition, the HHS Cybersecurity Program is the cornerstone of the HHS IT Strategic Plan, and an enabler for e-government success.

2. **Are there policies, procedures, and processes that you believe HHS should adopt in order to be more effective with regards to cybersecurity?**

No industry can enable perfect security; rather, organizations must enumerate and manage their risks. At a healthcare organization, the IT security team is challenged with understanding every possible avenue of attack by which a hacker might gain access to the network, including malicious malware or intrusion via a weak link in devices or part of the facility's infrastructure that receive routine electronic updates. A hacker only needs to find and exploit one weakness to penetrate a network. That's as true for HHS and its operating divisions as it is for a hospital.

In many cases, that one weakness is preying upon the behaviors of individuals through social engineering. As many studies have shown, and as many organizations that conduct penetration tests and other social engineering assessments will attest, it is impossible to prevent every human being in an organization from falling prey to such an attack. Coordination and a clear delineation of responsibilities across an organization are key tenets of an effective cybersecurity strategy, whether it is a healthcare delivery organization or the Department of Health and Human Services. Clear and consistent communication, reinforced by vigilant training programs, will allow a strategy to flourish.

We are hesitant to suggest the immediate adoption of particular policies until HHS has completed its report to Congress.

3. **Are there policies, procedures, or processes that you believe that HHS should consider reforming or removing in order to be more effective with regards to cybersecurity?**

HHS' coordination plan, which is expected to be delivered to Congress in December, should show areas for improvement in HHS' cyber protocols and procedures. That said, security must be an organizational priority for true change to take hold. Even before the coordination plan is delivered to Congress, HHS could embark on a comprehensive training program that creates a set of expectations and holds staff accountable. For instance, many healthcare organizations will routinely conduct phishing exercises to assess employee behavior and detect trouble spots.

Throughout the hearing, members of the panel emphasized that, in addition to its organizational structure, it is critically important the roles and responsibilities for officials within HHS in regards to cybersecurity are clear and effective.

4. **Please describe the responsibilities and authorities that you believe the following HHS officials should have with regards to cybersecurity:**

- **The Secretary of Health;**
- **The HHS CIO;**
- **The HHS CISO**
- **Any other officials (such as the General Counsel, CFO, etc.).**

Given the breadth and depth of cyber threats, it's paramount that all facets of the department, from the information technology department to researchers at the National Institutes of Health (NIH) to senior leadership and everyone in between, coordinate efforts to improve HHS' cyber hygiene.

- **The Secretary of Health**

Similar to a hospital and health system CEO or in some cases, members of a health system's board of directors, the secretary has a responsibility to understand, at a high level, the risks and vulnerabilities the department faces. The secretary must use his/her bully pulpit to make cybersecurity an organization priority and ensure that risk management and risk mitigation is part of an overall operational plan.

The secretary should know who within the department is responsible for the execution and implementation of the cybersecurity plan. Given that cybersecurity should not be considered solely an information technology issue, it's imperative that the secretary have regularly scheduled meetings with the chief information officer (CIO) and/or other members of the department's cybersecurity team, which should include: Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Chief Security Officer (CSO).

- **The HHS CIO**

As in healthcare delivery organizations, the CIO should manage various pieces of the department's information technology infrastructure, with responsibility over the myriad of IT and computer systems that support the department's enterprise-wide goals, including information security. Currently, the CIO advises the secretary and the Assistant Secretary for Resources and Technology (ASRT) on matters pertaining to the use of information and related technologies.

Within HHS, the Office of the Chief Information Officer should, among other responsibilities, provide assistance and guidance on the use of technology-supported business processes; investment analysis for information technology; strategic development and application of information systems and infrastructure; and, establish and execute policies to provide improved management of information resources and technology within the department.

- **The HHS CISO**

As I mentioned in my testimony, the reporting structure for CISOs varies across healthcare organizations. At Intermountain Healthcare, the CISO reports directly to me, the CIO. More important that the reporting structure is ensuring coordination and continuity of an organizatino's cybersecurity plan. Similar to the private sector, the HHS' CISO should be focused on developing and overseeing the implementation of the *technical strategy to achieve the department's security posture,* as well as managing the department's information security team. Working across information systems operations ensures that the technical components required for cybersecurity are in place and managed.

In the hearing, the panel discussed the fact that, as currently drafted, H.R. 5068 makes the newly elevated CISO a presidential appointment. Concerns were raised about that, stating that it might overly politicize the position.

5. **Would the position be more effective if it wasn't a presidential appointment?**

As a former member of the Health IT Policy Committee, a federal advisory committee created under Health Information Technology for Economic and Clinical Health Act (HITECH), I witnessed firsthand how important initiatives for improving care delivery can get bogged down in politics and bureaucracy resulting from political appointments. What's central to this conversation is the value of meaningful coordination, avoiding any unintended consequences of complex reporting structure. For instance, elevating the CISO to a presidential appointment could create tensions with other with other positions that, at least on the department's organization chart, have equal responsibilities, but are not appointed. Such a circumstance may impede the coordination and flow of information necessary to thwart cyber threats due to the nature by which an individual was selected for their position.

It is vital to fully evaluate the potential negative consequences that could result from making the HHS CISO a presidential appointment. We've seen instances where politicizing a role can hamper an agency's ability to affect change. For instance, confirmation hearings can be delayed for a variety of reasons, leading to a void in leadership. The CISO, as with the CIO, demand significant technical expertise. A presidential appointment could unnecessarily imperil the chances that qualified, rather than connected, candidates fill the office.

CHIME recommends that the CISO within the Department of Health and Human Services not be a presidentially-appointed position.

FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 Rayburn House Office Building
Washington, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 20, 2016

Mr. Mac McMillan
Chief Executive Officer
CynergisTek, Inc.
11410 Jollyville Road
Austin, TX 78759

Dear Mr. McMillan:

Thank you for appearing before the Subcommittee on Health on May 25, 2016 to testify at the hearing entitled "Examining Cybersecurity Responsibilities at HHS."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on July 5, 2016. Your responses should be mailed to Graham Pittman, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to graham.pittman@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Joseph R. Pitts

Joseph R. Pitts
Chairman
Subcommittee on Health

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

Attachment – Answers: Additional Questions for the Record

The Honorable Joseph R. Pitts

Throughout the hearing, members of the panel either made or agreed with the assertion that H.R. 5068 will not work in a vacuum; HHS must also have clear, effective, and enforced policies, procedures, and processes for ensuring that cybersecurity is a priority throughout the Department.

1. **Please describe the policies, procedures, and processes that you believe HHS currently has in place for ensuring that cybersecurity is a priority throughout the Department.**

HHS like other Departments of the Government must be compliant with the Federal Information Systems Management Act (FISMA) which uses as its basis the National Institute of Standards and Technology Cybersecurity Framework for implementing and measuring the effectiveness of its efforts to protect information. HHS with its multitude of program responsibilities and diverse information ecosystem is likely subject to many other different information security standards as well such as SAMHSA, FDA requirements, the Common Rule, etc. The NIST Cybersecurity Framework provides an effective structure for addressing the Department's many diverse regulatory security requirements. HHS has various governance structures like the CIO Council and the CTO Council where privacy and security issues are raised and vetted with senior leadership. The HHS CISO sits on the CTO Council. I am sure, but am not privy to, the existence of other policy elements of their program, but they have the basic elements of policy and framework that support the necessary procedure and processes required to manage a cybersecurity program.

2. **Are there policies, procedures, and processes that you believe HHS should adopt in order to be more effective with regards to cybersecurity?**

By using the NIST Cybersecurity Framework and the NIST Guides for information security the HHS assures that it is following a well researched and up to date set of standards and guidelines for managing cybersecurity. Like any organization managing a dynamic program with multiple elements subject to change they should be constantly reviewing their program, their policies, their procedures and processes against the latest guidelines and alerts published by NIST to insure their program is as up to date as possible. NIST publishes specific guidelines addressing areas such as encryption, cloud services, third party relationships, etc. and these should also be consulted when appropriate. Information security is a constantly changing state with influences from technology, the threat, operations and the environment that must be constantly monitored and addressed.

3. **Are there policies, procedures, or processes that you believe that HHS should consider reforming or removing in order to be more effective with regards to cybersecurity?**

I am not aware of any policies, procedures or processes that HHS should consider reforming or removing that supports their program. However HHS does have responsibility for overseeing privacy and security in healthcare and the businesses that handle protected health information under the Health Information Portability and Accountability Act (HIPAA) and its follow on legislation the HITECH Act and the Omnibus Rule. The HIPAA Security Rule, first conceived in the late 1990s and implemented in 2003 is woefully inadequate to meet the needs of the current cybersecurity environment we live and operate in today. This rule has not undergone revision since it was introduced, yet every other credible security standard whether NIST, ISO 27000, ITIL, etc. has been revised at least three or four times between 2003 and today. If there is a policy standard that HHS needs to address it is the HIPAA Security Rule. There is also I believe already a basis for doing this as many health systems already know the HIPAA Security Rule is not enough and have adopted the NIST standards to proactively improve the effectiveness of their program. To date more than 60% of healthcare follow or use NIST as the basis for their cybersecurity program. HHS should consider adopting the NIST Cybersecurity Framework across the board, not only for its own internal purposes, but for the industry as a whole to raise the standard of healthcare security.

In general organizations that place requirements on their fiscal structures for considering security in investment decisions tend to focus more on data security. The HHS CIO Council Charter describes that body's responsibilities for overseeing information technology investments and its relationship to the HHS Information Technology Investment Review Board (ITIRB) and the HHS Capital Planning and Investment Control (CPIC) policy. What is conspicuously absent, but is address in the CTO Council Charter, is reference to cybersecurity when making or reviewing information technology investments. Cybersecurity should be present at all levels of the governance structure in the Department to include the CIO Council.

Throughout the hearing, members of the panel emphasized that, in addition to its organizational structure, it is critically important the roles and responsibilities for officials within HHS in regards to cybersecurity are clear and effective.

4. **Please describe the responsibilities and authorities that you believe the following HHS officials should have with regards to cybersecurity:**

   - **The Secretary of Health;**

The Secretary of Health is and should be ultimately responsible for the protection of Departmental information assets and for promoting effective cybersecurity protections in the nations healthcare industry. They should be responsible for appointing a competent individual to serve as the HHS CISO to advise them and the leadership of HHS on cybersecurity policy and measures necessary to carry out the information security mission of the Department. They should be responsible for reporting to the Administration and to Congress on whatever basis deemed necessary regarding their

Departments efforts and status with respect to cybersecurity preparedness. They should be responsible for ensuring an effective governance structure is out in place throughout the Department to provide oversight, accountability, direction and resource support.

- **The HHS CIO;**

The HHS CIO should be responsible for implementing and delivering the necessary information services to support the operations of the Department in a manner that promotes the protection of information assets and sensitive information. They should implement the security technologies that are required to security the enterprise effectively and support security operations. They should ensure that information assets are implemented in accordance with the Departments cybersecurity policies. They should ensure that all information technology personnel are trained on the security skills required for their position and those with specific security responsibilities receive specialized training to perform their roles effectively. They should work collaboratively with the CISO to ensure that all information assets are selected, procured, implemented, tested, maintained and retired in an appropriate manner to ensure the protection of the Departments assets, operations, personnel and information.

- **The HHS CISO;**

There are many well written CISO position descriptions that detail the role and responsibilities of the CISO in an organization. What I feel is germane for this discussion is the importance of the role as the chief advisor on cybersecurity matters to the Secretary HHS. The HHS CISO is the principle with primary responsibility for overseeing the on-going activities and development, implementation, and improvement of the Department's information assurance program and compliance with Federal regulations. The HHS CISO in collaboration with the HHS CIO is responsible for ensuring that Departmental information assets and data are protected adequately. Serves as the primary cybersecurity advisor to the Secretary HHS and collaborates with other CISOs across the Federal government and industry. Maintains in depth knowledge of cybersecurity matters, standards, frameworks, technologies to inform information technology strategy and security controls. Is or appoints a member to the CIO and CTO Councils. The CISO should be designated as the senior official responsible for accrediting HHS information assets as having met and continuing to meet Departmental and Federal mandates for cybersecurity.

- **Any other officials (such as the General Counsel, CFO, etc.).**

First, let me say that every other official and employee ought to have information security responsibilities articulated in their position descriptions if for no other reason than to convey their responsibilities as system and data users. There are a number of other important positions from a policy perspective to ensure effective cybersecurity. Those include the General Counsel (GC), Human Resources, the Chief Financial Officer (CFO), the Chief Procurement Official, the Chief of Physical Security. Effective cybersecurity relies on an integrated ecosystem of controls and behaviors to be successful. These other principles in the Department are important by supporting, but not limited to, understanding and articulating risk, personnel selection, screening, accountability and training, supporting effective budget development/defense, ensuring acquisitions involving information technology are reviewed before purchased and complimentary controls are in place to physically protect information assets and data. Information security is a cultural phenomena that requires action, input, support, vigilance, etc. from the bottom up and the top down in every organization.

In the hearing, the panel discussed the fact that, as currently drafted, H.R. 5068 makes the newly elevated CISO a presidential appointment. Concerns were raised about that, stating that it might overly politicize the position.

Would the position be more effective if it wasn't a presidential appointment?

Personally I do not believe this position needs or should be a presidential appointment. The Secretary should be able to appoint his or her CISO in the same manner as they appoint the CIO. If we use the rationale that we need the CISO position appointed as a presidential appointment to ensure effective cybersecurity then we would need to treat the CIO position the same way. They are both critical to the success of the program. I believe that what is more important is the description of the position and the qualifications of the appointee.

○