STRENGTHENING U.S. CYBERSECURITY CAPABILITIES

HEARING

BEFORE THE

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

FEBRUARY 14, 2017

Serial No. 115–02

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
24–667PDF 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 SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
DANA ROHRABACHER, California
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
STEPHEN KNIGHT, California
BRIAN BABIN, Texas
BARBARA COMSTOCK, Virginia
GARY PALMER, Alabama
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DRAIN LAHOOD, Illinois
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ANDY BIGGS, Arizona
ROGER W. MARSHALL, Kansas
NEAL P. DUNN, Florida
CLAY HIGGINS, Louisiana

EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
ALAN GRAYSON, Florida
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
DONALD S. BEYER, JR., Virginia
JACKY ROSEN, Nevada
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
MARK TAKANO, California
COLLEEN HANABUSA, Hawaii
CHARLIE CRIST, Florida

Subcommittee on Research and Technology

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma
RANDY HULTGREN, Illinois
STEPHEN KNIGHT, California
DARIN LAHOOD, Illinois
RALPH LEE ABRAHAM, Louisiana
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ROGER W. MARSHALL, Kansas
LAMAR S. SMITH, Texas

DANIEL LIPINSKI, Illinois
ELIZABETH H. ESTY, Connecticut
JACKY ROSEN, Nevada
SUZANNE BONAMICI, Oregon
AMI BERA, California
DONALD S. BEYER, JR., Virginia
EDDIE BERNICE JOHNSON, Texas

CONTENTS

February 14, 2017

Opening Statements

Witnesses:

Appendix I: Additional Material for the Record

STRENGTHENING U.S. CYBERSECURITY CAPABILITIES

TUESDAY, FEBRUARY 14, 2017

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittee met, pursuant to call, at 10:08 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Barbara Comstock [Chairwoman of the Subcommittee] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6301
(202) 225-6371
www.science.house.gov

Strengthening U.S. Cybersecurity Capabilities

Tuesday, February 14, 2017
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Dr. Charles H. Romine, Director, Information Technology Lab, National Institute for Standards and Technology (NIST)

Mr. Iain Mulholland, Industry Member, Center for Strategic and International Studies (CSIS) Cyber Policy Task Force, Chief Technology Officer, Security, VMware, Inc.

Dr. Diana Burley, Executive Director and Chair, Institute for Information Infrastructure Protection (I3P), Professor, Human and Organizational Learning, The George Washington University

Mr. Gregory Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office (GAO)

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

Tuesday, February 14, 2017

TO: Members, Committee on Science, Space, and Technology

FROM: Majority Staff, Committee on Science, Space, and Technology

SUBJECT: Research and Technology Subcommittee hearing
"Strengthening U.S. Cybersecurity Capabilities"

The Subcommittee on Research and Technology of the Committee on Science, Space, and Technology will hold a hearing titled *Strengthening U.S. Cybersecurity Capabilities* on Tuesday, February 14, 2017 at 10:00 a.m. in Room 2318 of the Rayburn House Office Building.

Hearing Purpose:

The purpose of the hearing is to review and discuss cybersecurity policy recommendations provided by recent reports. These include the *Report on Securing and Growing the Digital Economy* published by the Commission on Enhancing National Cybersecurity in December 2016,[1] and *From Awareness to Action – A Cybersecurity Agenda for the 45th President*, published by the Center for Strategic and International Studies (CSIS) in January 2017.[2] The hearing will also address work conducted by the U.S. Government Accountability Office (GAO) relative to cybersecurity issues, and discuss the reports' recommendations in the context of GAO's body of work.

Witness List

- **Dr. Charles H. Romine**, Director, Information Technology Lab, National Institute of Standards and Technology (NIST)
- **Mr. Iain Mulholland**, Industry Member, CSIS Cyber Policy Task Force; Chief Technology Officer, Security, VMware, Inc.
- **Dr. Diana Burley**, Executive Director and Chair, Institute for Information Infrastructure Protection (I3P); Professor, Human and Organizational Learning, The George Washington University
- **Mr. Gregory Wilshusen**, Director, Information Security Issues, GAO

Staff Contact

For questions related to the hearing, please contact Raj Bharwani of the Majority Staff at 202-225-6371.

[1] https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.
[2] https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

Chairwoman COMSTOCK. The Committee on Science, Space, and Technology will come to order.

Without objection, the Chair is authorized to declare recesses of the Committee at any time.

Good morning, and welcome to today's hearing titled "Strengthening U.S. Cybersecurity Capabilities." I recognize myself for five minutes for an opening statement.

I want to begin by thanking everyone for attending this first hearing of the Research and Technology Subcommittee in the 115th Congress. I look forward to working with the members of the Subcommittee, some of whom are new to the Committee, while others are new to Congress, and working together on many of the issues under our jurisdiction.

The topic of cybersecurity is a familiar one for this Committee, and this Subcommittee in particular. It is also a topic of continuously growing international attention and real concern.

During the 114th Congress, the Science Committee held a dozen hearings related to cybersecurity. Some of these were triggered by notable events such as the Office of Personnel Management and Internal Revenue Service data breaches. I still remember receiving my OPM letter, and I also got one of those IRS letters, which informed me that my personal information may have been compromised or stolen by the cyber criminals behind this attack. I also chaired a hearing last year during which the IRS Commissioner testified about the breaches under his watch. It's certainly frustrating to hear that criminals used information from other cyberattacks to accurately answer questions on the IRS website to access what should have been secured information. Those criminals should not have been able to access such information, and may not have been able to access it, had the agency fully followed security guidelines provided by the National Institute of Standards and Technology.

I look forward to hearing from our witnesses today about cybersecurity recommendations to help protect U.S. information systems. These recommendations were highlighted in recent documents, which include the report published by the Commission on Enhancing National Cybersecurity and one published by the Center for Strategic and International Studies. The Government Accountability Office (GAO), which has issued countless recommendations in the area of cybersecurity for decades, is also represented at today's hearing. I am interested in hearing how the suggestions from the reports being profiled today align with GAO's body of work.

I also look forward to hearing more about what can be done to proactively address cyber workforce gaps. This Committee has been very much involved in STEM education and making sure we have that cybersecurity generation for dealing with this, and that is an important role that we need to play here in Congress, continuing to get that cyber workforce up and running, I, particularly in my district, am pleased that we have so much going on in that area and want to continue in this Subcommittee to focus on that also. You know, when I travel around my district and visit with constituents who work in this sector, a repeated concern is the increasing need for individuals with appropriate education, training, and knowledge of cybersecurity matters and being able to tackle what we know are going to be increasing problems and that we need to be on the offense on this front.

Before I yield to the Ranking Member, let me just note that I appreciate everyone's presence here today given that this is the week of the RSA Conference in San Francisco. So sorry you aren't able to be there and are here, but we truly appreciate you being able to join us here today.

[The prepared statement of Chairwoman Comstock follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
February 14, 2017

Media Contact: Kristina Baum
(202) 225-6371

Statement of Chairwoman Barbara Comstock (R-Va.)
Strengthening U.S. Cybersecurity Capabilities

Chairwoman Comstock: I want to begin by thanking everyone for attending this first hearing of the Research and Technology Subcommittee in the 115th Congress.

I look forward to working with the Members of the Subcommittee, some of whom are new to the Committee, while others are new to Congress, on the many issues under our jurisdiction.

The topic of cybersecurity is a familiar one for this Committee, and this Subcommittee in particular. It is also a topic of continuously growing international attention and concern.

During the 114th Congress, the Science Committee held a dozen hearings related to cybersecurity. Some of these were triggered by notable events such as the Office of Personnel Management (OPM) and Internal Revenue Service (IRS) data breaches. I still remember receiving my OPM letter, which informed me that my personal information may have been compromised or stolen by the cyber criminals behind this attack.

I also chaired a hearing last year during which the IRS Commissioner testified about the breaches under his watch. It was frustrating to hear that criminals used information from other cyber-attacks to accurately answer questions on the IRS website to access what should have been secured information. Those criminals should not have been able to access such information, and may not have been able to access it, had the agency fully followed security guidelines provided by the National Institute of Standards and Technology (NIST).

I look forward to hearing from our witnesses today about cybersecurity recommendations to help protect U.S. information systems. These recommendations were highlighted in recent documents, which include the report published by the Commission on Enhancing National Cybersecurity and one published by the Center for Strategic and International Studies.

The Government Accountability Office (GAO), which has issued countless recommendations in the area of cybersecurity for decades, is also represented at today's hearing. I am interested in hearing how the suggestions from the reports being profiled today align with GAO's body of work.

I also look forward to hearing more about what can be done to proactively address cyber workforce gaps. When I travel around my district and visit with constituents who work in the technology sector, a repeated concern is the increasing need for individuals with appropriate education, training, and knowledge of cybersecurity matters.

Before I yield to the Ranking Member, let me just note that I appreciate everyone's presence here today given that this is the week of the RSA Conference in San Francisco.

###

Chairwoman COMSTOCK. And I now yield to our distinguished Ranking Member, Mr. Lipinski.

Mr. LIPINSKI. Thank you, Chairwoman Comstock. Too bad we couldn't all go out to San Francisco to have a field hearing there.

But I want to thank Chairwoman Comstock and I look forward to working with you. It's good to have some continuity in the Chair of the Subcommittee. I think that will be helpful as we move forward and work together on getting some things done here on the Subcommittee, and I also look forward to working with all our returning and new members of this Research and Technology Subcommittee. I also want to thank our distinguished panel for being here today. I know some of you have been here a number of times, and we always appreciate your expertise.

Cybersecurity has long been a priority of mine in Congress. The Cybersecurity Enhancement Act of 2014, which was signed into law, began as a bill that Representative McCaul and I introduced in 2009. As pointed out in the CSIS report, cybersecurity is a topic on which nearly every Committee in Congress has something to contribute. This is a good thing and a bad thing. What we need to do is to do our best at making sure that there is collaboration and coordination across all these different committees.

Our committee is uniquely positioned to contribute meaningfully to oversight and policy development for cybersecurity because of our jurisdiction over NIST, and our oversight responsibility for STEM education and workforce training activities across the Federal government. I understand that today's hearing is likely just the first of several hearings on cybersecurity we will hold in this Congress. I understand that today's hearing is likely—well, this hearing—I got lost in my script here—this is one of several. This one is going to be a more broad overview of what we're looking at in cybersecurity.

However, sitting before us are a few of our nation's top experts on NIST's role in cybersecurity and on cybersecurity education and workforce issues, so I look forward to hearing those specific areas from our witnesses.

NIST plays a central role in the security of federal information systems. The experts at NIST develop the security standards and guidelines that all other civilian federal agencies are required to implement through the Federal Information Security Modernization Act, or FISMA. Those experts also provide technical assistance to other agencies. Furthermore, NIST led the development of the Cybersecurity Framework for Critical Infrastructure, a widely adopted set of voluntary guidelines and standards for industry, and works closely with industry to help develop tools for businesses of all sizes and from all sectors to effectively implement the Framework.

There have been some calls for an expanded role for NIST, including an expanded oversight role under FISMA. These suggestions warrant careful examination. NIST is successful in its current role in large part because of its independence as a standards and technology agency, and not a regulatory or enforcement agency. Any discussion about an expanded role must be accompanied by a discussion about increasing resources and other issues that would come up.

On the topic of education and workforce, NIST leads federal efforts through coordination of the National Initiative for Cybersecurity Education, or NICE. Another agency in our jurisdiction, the National Science Foundation, supports important programs such as the CyberCorps Scholarship for Service.

However, the gap between supply and demand for cybersecurity training in both the government and the private sector remains a challenge. All of the best policies are meaningless without the skilled workforce to implement these policies. Increasing the recruitment and retention of cybersecurity talent in our federal agencies is going to require new and creative thinking, as well as increased resources.

It is also going to require stepping back from the disparaging rhetoric aimed lately at the civil service. Federal agencies already struggle to recruit and retain top talent from the limited pool of qualified cybersecurity professionals, especially when private sector salaries are much higher. Negative remarks, combined with a federal hiring freeze, can do real damage to agencies' recruitment and retention efforts.

Before I conclude, I want to ask unanimous consent to add to the record two letters to the Committee, one from the Electronic Privacy Information Center, and the other from the National Association of Federally Insured Credit Unions.

Chairwoman COMSTOCK. Thank you. Without objection.

[The information appears in Appendix I]

Mr. LIPINSKI. Thank you, and I want to again thank the Chairwoman for holding this hearing, and the witnesses for being here, and I look forward to your testimony.

I yield back.

[The prepared statement of Mr. Lipinski follows:]

OPENING STATEMENT

Ranking Member Daniel Lipinski (D-IL)
of the Subcommittee on Research and Technology

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Strengthening U.S. Cybersecurity Capabilities"
February 14, 2017

Thank you Chairwoman Comstock. I look forward to working with you and all of the returning and new Members of the Research & Technology Subcommittee in this new Congress. Thank you also to the distinguished panel for being here this morning to share your expertise on this important topic.

Cybersecurity has long been a priority of mine in Congress. The *Cybersecurity Enhancement Act of 2014*, which was signed into law, began as a bill that Rep. McCaul and I introduced in 2009. As pointed out in the CSIS report, cybersecurity is a topic on which nearly every Committee in Congress has something to contribute. [On one hand, this presents a challenge to developing and enacting comprehensive and coherent policies. On the other hand, it presents an opportunity for coordinated policy making across the government to address this complex and pressing issue.]

Our committee is uniquely positioned to contribute meaningfully to oversight and policy development for cybersecurity because of our jurisdiction over NIST, and our oversight responsibility for STEM education and workforce training activities across the Federal government. I understand that today's hearing is likely just the first of several hearings on cybersecurity we will hold this Congress, and as such it is intentionally broad in scope. However, sitting before us are a few of our nation's top experts on NIST's role in cybersecurity and on cybersecurity education and workforce issues, so I look forward to hearing those specific areas from our witnesses.

NIST plays a central role in the security of federal information systems. The experts at NIST develop the security standards and guidelines that all other civilian federal agencies are required to implement through the Federal Information Security Modernization Act, or FISMA. Those experts also provide technical assistance to other agencies. Furthermore, NIST led the development of the Cybersecurity Framework for Critical Infrastructure, a widely adopted set of voluntary guidelines and standards for industry, and works closely with industry to help develop tools for businesses of all sizes and from all sectors to effectively implement the Framework.

There have been some calls for an expanded role for NIST, including an expanded oversight role under FISMA. These suggestions warrant careful examination. NIST is successful in its current role in large part because of its independence as a standards and technology agency, and not a regulatory or enforcement agency. Any discussion about an expanded role must be accompanied by a discussion about increasing resources.

On the topic of education and workforce, NIST leads Federal efforts through coordination of the National Initiative for Cybersecurity Education, or NICE. Another agency in our jurisdiction, the National Science Foundation, supports important programs such as the CyberCorps Scholarship for Service. However, the gap between supply and demand for cybersecurity training in both the government and the private sector remains an urgent challenge. All of the best policies are meaningless without the skilled workforce to implement those policies. Increasing the recruitment and retention of cybersecurity talent in our Federal agencies is going to require new and creative thinking, as well as increased resources. It is also going to require stepping back from the disparaging rhetoric aimed lately at the civil service. Federal agencies already struggle to recruit and retain top talent from the limited pool of qualified cybersecurity professionals, especially when private sector salaries are much higher. Negative remarks, combined with a federal hiring freeze, do real damage to agencies' recruitment and retention efforts.

Once again, I want to thank the Chairwoman for holding this hearing, and the witnesses for sharing your time and expertise with us this morning. I look forward to your testimony.

I yield back.

Chairwoman COMSTOCK. I thank the Ranking Member, and I also thank him for his comments on the importance of our cybersecurity workforce and I'll second those sentiments.

Our first witness today is Dr. Charles Romine, Director of the—oh, I'm sorry. The Ranking Member is present. I'm sorry.

Ms. JOHNSON. Thank you very much, Madam Chairwoman.

I'd like to ask for unanimous consent to enter some material in the record prior to making a statement.

Chairwoman COMSTOCK. Without objection.

Ms. JOHNSON. Thank you.

Chairwoman Comstock, I have been in Congress and on this Committee for a long time. As a matter of fact, this is the beginning of my 25th year. There are many times I have disagreed with my Republican colleagues. Sometimes we've had harsh criticisms of each other's political positions. That comes with the job description of being a Member of Congress, and I accept that. But what I will not accept is when Members or staff provide clearly misleading information about me or my colleagues to the press, the public, or anyone else.

Yesterday, a story in The Hill newspaper regarding a letter that I sent along with Mr. Lipinski and Mr. Beyer to you, Chairman Smith and Chairman LaHood about President Trump's cybersecurity practices quoted an unnamed GOP Committee aide that suggested that last Congress, Committee Democrats opposed cybersecurity hearings that were held on this Committee regarding the Office of Personnel Management, the Internal Revenue Service and the Federal Deposit Insurance Corporation because we believed that they were political and illegitimate. I want to speak—I will not speak for my colleagues but I will speak for myself. I did believe many of the hearings that were held on this Committee were politically motivated but none of them included any of the hearings mentioned by the Committee aide. If this aide had attended any of these hearings or read any of the statements by me or the Ranking Members Beyer or Lipinski, they would have understood that. Since I believe in ensuring there is an honest record of events, I would like unanimous consent to enter into the record all of the Ranking Member's statements and press releases issued by the Democrats for each of the hearings referenced by this Republican staffer just in order to set the record straight.

Chairwoman COMSTOCK. Without objection.

[The information appears in Appendix I]

Ms. JOHNSON. Thank you.

Let me thank you again and also Ranking Member Lipinski for holding the hearing today on cybersecurity, and thank you to all the witnesses for being here this morning. We have several new members on the Committee, so it is valuable to start off the year with a Cybersecurity 101 hearing.

Today's panel includes four very distinguished experts from government, the private sector, and academia, and I know it will be an interesting and informative discussion. I'm pleased that Dr. Romine is able to join us this morning. Testifying before Congress so early during a transition in administrations can be challenging for any agency official.

This is not a hearing specifically about NIST's role in cybersecurity, but I'm going to set some context with a few words about this very important but little-known agency. NIST plays a crucial role in both public and private sector cybersecurity, as we will hear about today. In fact, cybersecurity accounts for a significant fraction of NIST's total budget. However, it is but one of dozens of topics to which the hundreds of extraordinary scientists and engineers working at the NIST labs in Gaithersburg, Maryland, and Boulder, Colorado, devote their careers. NIST hosts the world leading measurement scientists, and uses that science to lead the development of technical standards for the nation. NIST scientists work closely with industry across all sectors, big and small, to advance U.S. innovation and competitiveness.

And they do all of this on what amounts to a shoestring budget. Because NIST usually exceeds expectations, there is a tendency by policymakers to ask them to do more with less. That has surely been true in the realm of cybersecurity. But I caution this Committee and the Administration not to push NIST to the breaking point. Every agency must set priorities, and there may be room even at NIST to put aside some of its work to make room for higher priority topics, including cybersecurity. I will be watching closely to ensure that that none of NIST's important work is compromised in our zeal to save a dollar here and dollar there. The costs to the nation will be much greater than the few dollars saved.

And finally, I want to bring up a troubling incident from 2013, in which the National Security Agency (NSA) secretly inserted a "back door" into a cryptographic standard being developed by NIST. There was an immediate outcry, as this sneak attack was widely recognized as a potentially slippery slope to a surveillance state. It undermined the stellar reputation and credibility of NIST in international circles and it had a negative impact on the global operations of U.S. corporations.

In the aftermath of that incident, NIST implemented new procedures to reinforce transparency and integrity in their standards development process. I want NIST to be able to consult with the intelligence agencies. Such collaboration is necessary and appropriate in the realm of cybersecurity. Both NIST and the U.S. intelligence community share special cybersecurity expertise and skills that should be shared to help defend our nation against the many cybersecurity threats that confront us. However, I will be watching out for the slightest hint that such collaborations in any way compromise NIST's independence or the integrity of their work.

With that, I want to thank the witnesses again for your time and contributions to this Committee's discussion about cybersecurity, and I yield back.

I thank you, Madam Chair.

[The prepared statement of Ms. Johnson follows:]

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Strengthening U.S. Cybersecurity Capabilities"
February 14, 2017

Thank you Chairwoman Comstock and Ranking Member Lipinski for holding this hearing on cybersecurity. And thank you to the witnesses for being here this morning. We have several new Members on the Committee, so it is valuable to start off the year with a "Cybersecurity 101" hearing. Today's panel includes four very distinguished experts from government, the private sector, and academia, and I know it will be an interesting and informative discussion.

I'm pleased Dr. Romine is able to join us this morning. Testifying before Congress so early during a transition in administrations can be challenging for any agency official. This is not a hearing specifically about NIST's role in cybersecurity, but I'm going to set some context with a few words about this very important but little known agency.

NIST plays a crucial role in both public and private sector cybersecurity, as we will hear about today. In fact, cybersecurity accounts for a significant fraction of NIST's total budget. However, it is but one of dozens of topics to which the hundreds of extraordinary scientists and engineers working at the NIST labs in Gaithersburg, Maryland and Boulder, Colorado devote their careers. NIST hosts the world leading measurement scientists, and uses that science to lead the development of technical standards for the nation. NIST scientists work closely with industry across all sectors, big and small, to advance U.S. innovation and competitiveness. And they do all of this on what amounts to a shoestring budget.

Because NIST usually exceeds expectations, there is a tendency by policymakers to ask them to do more with less. That has surely been true in the realm of cybersecurity. But I caution this Committee and the Administration not to push NIST to the breaking point. Every agency must set priorities, and there may be room even at NIST to put aside some of its work to make room for higher priority topics, including cybersecurity. I will be watching closely to ensure that that none of NIST's important work is compromised in our zeal to save a dollar here and dollar there. The costs to the nation will be much greater than the few dollars saved.

Finally, I want to bring up a troubling incident from 2013, in which the National Security Agency (NSA) secretly inserted a "back door" into a cryptographic standard being developed by NIST. There was an immediate outcry, as this sneak attack was widely recognized as a potentially slippery slope to a surveillance state. It undermined the stellar reputation and credibility of NIST in international circles and it had a negative impact on the global operations of U.S. corporations. In the aftermath of that incident, NIST implemented new procedures to reinforce transparency and integrity in their standards development process.

I want NIST to be able to consult with the intelligence agencies – such collaboration is necessary and appropriate in the realm of cybersecurity. Both NIST and the U.S. intelligence community share special cybersecurity expertise and skills that should be shared to help defend our nation against the many cybersecurity threats that confront us. However, I will be watching out for the slightest hint that such collaborations in any way compromise NIST's independence or the integrity of their work.

With that, I want to thank the witnesses again for your time and contributions to this Committee's discussion about cybersecurity, and I yield back.

Chairwoman COMSTOCK. Thank you.

Our first witness today is Dr. Charles Romine, Director of the Information Technology Lab at the National Institutes of Standards and Technology. This program develops and disseminates standards for security and reliability of information systems including cybersecurity standards and guidelines for federal agencies. Dr. Romine has previously served as a Senior Policy Analyst at the White House Office of Science and Technology Policy and as a Program Manager at the Department of Energy's Advanced Scientific Computing Research Office. Dr. Romine received his bachelor's degree in mathematics and his Ph.D. in applied mathematics from the University of Virginia.

Our second witness today is Mr. Iain Mulholland, Industry Member of the Center for Strategic and International Studies Cybersecurity Task Force and Chief Technology Officer of Security for VMware, Inc. A 20-year veteran of the software security space, Mr. Mulholland was an early member of the Microsoft Trustworthy Computing Group where he led the Microsoft Security Response Center. Mr. Mulholland is also a member of the U.S. Delegation to the Wassenaar Plenary in Austria in charge of negotiating international cybersecurity protocols. Mr. Mulholland has received degrees from the Royal Military Academy in the United Kingdom as well as from Stanford University Graduate School of Business' Executive Leadership Program.

Our third witness today is Dr. Diana Burley, Executive Director and Chair of the Institute for Information Infrastructure Protection, and Professor of Human and Organizational Learning at the George Washington University. Prior to joining GW, Dr. Burley managed a multimillion-dollar computer science education and research portfolio and led the CyberCorps Program for the National Science Foundation. Dr. Burley holds a B.A. in economics from the Catholic University of America, M.S. in public management and policy, M.S. in organization science, and Ph.D. in organization science and information technology from Carnegie Mellon University, where she studied as a Woodrow Wilson Foundation fellow.

Our final witness today is Mr. Gregory Wilshusen, Director of Information Security Issues at the U.S. Government Accountability Office. Prior to joining GAO in 1997, he was a Senior Systems Analyst at the Department of Education. He received his bachelor's degree in business administration from the University of Missouri and his master of science and information management from George Washington University.

Thank you all for joining us this morning, and now I'll hear five minutes from Dr. Romine.

TESTIMONY OF DR. CHARLES H. ROMINE, DIRECTOR, INFORMATION TECHNOLOGY LAB, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Dr. ROMINE. Chairwoman Comstock, Ranking Member Lipinski, and Mrs. Johnson, and Members of the Subcommittee, thank you for the opportunity to discuss NIST's activities that help strengthen the nation's cybersecurity capabilities.

In the area of cybersecurity, NIST has worked with federal agencies, industry and academia since 1972. Our role to research, develop and deploy information security standards and technology to protect the federal government's information systems against the threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987, broadened through the Federal Information Security Management Act of 2002, and reaffirmed in the Federal Information Security Modernization Act of 2014, or FISMA.

In addition, the Cybersecurity Enhancement Act of 2014 authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

Recently, the independent bipartisan Commission on Enhancing National Cybersecurity released its report, which provides detailed recommendations to strengthen cybersecurity in both the public and the private sectors. NIST is active in many areas addressed by the Commission report.

Three years ago, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity, or the "Framework," which was created through collaboration between industry and government, and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Last month, NIST released a draft update to the Framework for public comment. The Framework continues to be voluntarily implemented by industry and adopted by infrastructure sectors, and this is contributing to reducing cyber-risks to our nation's critical infrastructure.

NIST works with stakeholders to cultivate trust in the Internet of Things, or IoT. NIST performs fundamental research, contributes to the development of consensus standards, and issues guidance that addresses security of IoT.

NIST's applied research for IoT security addresses market-focused applications such as healthcare, vehicles and transportation, smart home, and manufacturing. NIST carries out its responsibilities under FISMA through Federal Information Processing Standards and associated guidelines and practices. NIST provides management, operational, and technical security guidelines for federal agencies covering a broad range of topics. NIST stresses that the authorization of a system by a management official is an important quality control under FISMA. By authorizing operation of a system, the manager accepts the associated risk, formally assuming responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

NIST is considering additional steps to assist federal agencies, including how best to align the Cybersecurity Framework with our FISMA suite of standards and guidelines. Applying the Cybersecurity Framework across the federal government complements and enhances rather than duplicates or conflicts with the existing statute, executive direction, policy and standards.

NIST is active in other areas identified in the Commission report, such as authentication and identity management, privacy, and cybersecurity education, training and workforce development. NIST recognizes that it has an essential role to play in helping industry, consumers and government to counter cyber threats and strengthen the nation's cybersecurity capabilities.

NIST is extremely proud of its role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices and the robust collaborations with its federal government partners, private sector collaborators, and international colleagues.

Thank you for the opportunity to testify today on NIST's work in cybersecurity, and I'd be delighted to answer any questions that you may have.

[The prepared statement of Dr. Romine follows:]

Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Research and Technology

"Strengthening U.S. Cybersecurity Capabilities"

February 14, 2017

Introduction

Chairwoman Comstock, Mrs. Johnson, and members of the Subcommittee, I am Dr. Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss NIST's key roles in cybersecurity. Specifically, today I will discuss NIST's activities that help strengthen the Nation's cybersecurity capabilities.

The Role of NIST in Cybersecurity

With programs focused on national priorities from the Smart Grid and electronic health records to forensics, atomic clocks, advanced nanomaterials, computer chips and more, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop and deploy information security standards and technology to protect the federal government's information systems against threats to the confidentiality, integrity and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. § 3541[1]) and reaffirmed in the Federal Information Security Modernization Act of 2014 (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

Cybersecurity Commission

The Commission on Enhancing National Cybersecurity was established by Executive Order 13718 in February of last year, as a limited-duration, independent, bipartisan advisory committee within the Department of Commerce. The stated goals for the Commission were to enhance cybersecurity awareness and protections at all levels of government, business, and society; to protect privacy, to ensure public safety and economic and national security; and to empower Americans to take better control of their digital security. The Executive Order charged the Commission to produce and to publish a final report, after which it would be terminated.

On December 2, 2016, the Commission released its report, which provides detailed short- and long-term recommendations to strengthen cybersecurity in both the public and private sectors, while protecting privacy, fostering innovation and ensuring

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

economic and national security. NIST provided support to the commissioners as they consulted technical and policy experts, solicited input from the public through open hearings and a request for information, reviewed existing literature, and technical input during development of the final report.

The report emphasizes the need for collaborations between the public and private sectors, as well as international engagement. It also discusses the role consumers must play in enhancing our digital security. The report categorizes its recommendations within six overarching imperatives:

- Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks;
- Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy;
- Prepare Consumers to Thrive in a Digital Age;
- Build Cybersecurity Workforce Capabilities;
- Better Equip Government to Function Effectively and Securely in the Digital Age; and
- Ensure an Open, Fair, Competitive, and Secure Global Digital Economy.

NIST is active in several of these imperatives, which are addressed below.

Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks

Cybersecurity Framework

Three years ago, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity (Framework) in accordance with Section 7 of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The Framework, created through collaboration between industry and government, consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The voluntary, risk-based prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Since the release of the Framework, NIST has strengthened its collaborations with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders to raise awareness about the Framework, encourage use by organizations across and supporting the critical infrastructure, and develop implementation guides and resources.

Last month, NIST released a draft update to the Framework incorporating feedback received since the release of Framework version 1.0, comments from a December 2015 Request for Information, and from a 2016 Cybersecurity Framework Workshop. Draft Version 1.1 of the Framework, for which NIST is seeking public comments through April 10 of this year, provides new details on managing supply chain risks, clarifies key terms, and introduces measurement methods for cybersecurity. Key to the continuing success of the Framework is that it is not regulatory or mandatory in nature, but rather, is voluntarily implemented by industry and voluntarily adopted by infrastructure sectors, contributing to reducing cyber-risks to our Nation's critical infrastructure.

Cybersecurity for the Internet of Things

NIST works with stakeholders across industry, academia, and organizations that develop international standards and governments to cultivate trust in the Internet of Things (IoT). NIST performs fundamental research, contributes to the development of consensus standards, and issues guidance that address security for IoT in areas such as: Lightweight Encryption; RFID (Radio-Frequency Identification) and Bluetooth Security; BIOS Integrity; Industrial Control Systems Security; Blockchain; and Verifiable Time. NIST's applied research for IoT security addresses market-focused applications such as Health Information Technology, Vehicle/Transportation, Smart Home, and Manufacturing. For example, NIST's National Cybersecurity Center of Excellence (NCCoE) engineers are working with the healthcare community to address wireless infusion pump security in hospital environments. NIST is also working with the smart home industry to explore authentication and privacy preserving data sharing of IoT devices in a home environment and with the automotive industry toward integration of security, safety, resilience, reliability, and privacy in connected vehicle design and testing.There are many other NIST projects that cross-cut with IoT research, such as the Cybersecurity Framework, the National Vulnerability Database (already extended to include IoT devices and known IoT vulnerabilities), Supply Chain Risk Management for Information and Communication Technology, and guidance on systems security engineering (NIST Special Publication 800-160).

Authentication and Identity Management

Identity and access management processes are key elements of many of the cybersecurity technologies identified above, and are necessary to the effective specification and application of these technologies to counter cyber-threats. Authentication of people, information, and system components underlies the selection, application, and management of cybersecurity technical, procedural and management controls.

NIST develops best practices to support user digital identities, building on decades of research in technology areas that support authentication and identity management. Recently, NIST published for comment a major revision to NIST Special Publication 800-63, now titled *Digital Identity Guidelines*. The guidelines cover remote authentication of users (such as employees or contractors) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, and related assertions.

NIST is working to accelerate adoption of identity and access management technologies that expand the use of digital Personal Identity Verification credentials to mobile devices and private sector organizations. One example includes implementation of a centralized system to authenticate and control individuals' access to IT and operational resources of electrical generation and distribution systems. NIST is also researching requirements for standards and best practices for digital device identity for IoT devices and working with industry to support implementation of those standards and recommendations.

Privacy

NIST provides guidance and tools for organizations to address privacy risk by designing privacy into their systems from the beginning. Last month, NIST released Internal Report (NIST IR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. NIST collaborated with stakeholders in the public and private sectors, academia, and civil society organizations to develop a foundational framework to support privacy engineering and risk management. The report also provides a platform for integrating privacy into NIST's cybersecurity activities and programs, including the Cybersecurity Framework, Internet of Things, identity management, and the NCCoE. Aligned with the NIST mission, protecting privacy is good for innovation and U.S. competiveness in the digital economy, improving our quality of life.

Build Cybersecurity Workforce Capabilities

National Initiative for Cybersecurity Education

As the cybersecurity threat and technology environment evolves, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain, and continuously improve upon current cybersecurity practices, including in our Nation's critical infrastructure.

In 2008, the National Initiative for Cybersecurity Education (NICE), a public-private collaboration among government, academia, and industry, was established to enhance the overall cybersecurity capabilities of the U.S. The NICE program seeks to energize and promote a robust ecosystem for cybersecurity education, training, and workforce development. As the lead agency for this initiative, NIST works with more than 20 federal departments and agencies, as well as with industry and academia, to ensure a digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

In November 2016, NIST released the draft *NICE Cybersecurity Workforce Framework*, to help our Nation more effectively identify, recruit, develop, and maintain its cybersecurity talent. The framework provides a common language to categorize and describe cybersecurity work that will help organizations build a strong labor staff to protect systems and data. The NICE Challenge Project, funded by NIST and developed and maintained by California State University, San Bernardino, creates virtual challenges to test students and professionals on their ability to perform NICE Framework tasks and exhibit their knowledge, skills, and abilities.

In 2016, CyberSeek, an interactive online tool designed to help close the cybersecurity skills gap, was released to the public. CyberSeek, developed by CompTIA and Burning Glass, with funding from NIST, provides detailed, actionable data about supply and demand in the cybersecurity job market. CyberSeek includes an interactive map that indicates relative concentrations of cybersecurity job postings and worker supply. The Career Pathway portal of CyberSeek provides information on different types of cybersecurity positions to help students, job seekers, and education and training providers. The Career Pathway portal features information on common job titles, salaries, in-demand skills, education and certifications related to careers in cybersecurity, as well as pathways to reaching the mid- to advanced-level career positions.

NIST is also piloting the establishment of Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development in five communities[2] across the U.S. The RAMPS work to bring together K-12 schools, community colleges, universities, training providers, economic development organizations, local and state government, and employers to coordinate regional activities addressing the cybersecurity workforce shortage and expand their local economy.

Better Equip Government to Function Effectively and Securely in the Digital Age

Enterprise Risk Management

NIST carries out its responsibilities under both the Federal Information Security Management and Modernization Acts (FISMA) through the creation of a series of Federal Information Processing Standards (FIPS) and associated guidelines and practices. Under these laws, federal agencies are required to implement NIST's FIPS. NIST provides management, operational, and technical security guidelines for federal agencies covering a broad range of topics, such as protecting the confidentiality of Controlled Unclassified Information while residing in nonfederal information systems and organizations, BIOS management and measurement, key management and derivation, media sanitization, electronic authentication, and security automation.

NIST has a series of specific responsibilities with respect to federal agency information and information systems, other than National Security Systems, under both the Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act of 2014, including the development of:

- A standard for categorizing information to be used by all federal agencies. The categories are based on the potential impact of harm to the organization if the information or information systems are compromised; and

[2] Albany, New York; the Virginia Tidewater region; the Cincinnati-Dayton Corridor of Ohio; Colorado Springs, Colorado; and Phoenix, Arizona

- Minimum security requirements (*i.e.*, management, operational, and technical controls), for each information category.

In support of FISMA implementation, in recent years NIST has strengthened its collaboration with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems, through the Joint Task Force Transformation Initiative, which continues to develop key cybersecurity guidelines for protecting federal information and information systems.

This collaboration allows for a broad-based and comprehensive set of safeguards and countermeasures for information systems. This unified framework provides a standardized method for expressing security at all levels, from operational implementation to compliance reporting. It allows for an environment of information-sharing and interconnections among these communities and significantly reduces costs, time, and resources needed for finite sets of systems and administrators to report on cybersecurity to multiple authorities.

NIST provides standards, guidelines, and tools for agencies to test and assess their security and then to continuously monitor their implementation and new risks. This process is essential to ensure security baselines are initially implemented correctly, and remains pertinent even as technologies, threats, and missions continuously evolve.

Under FISMA, NIST does not assess, audit, or test agency security implementations and has no oversight authority. Congress recognized that placing such responsibilities on NIST would impede and ultimately defeat its ability to work with federal agency and private sector stakeholders to develop standards, guidelines, and practices in the open, transparent, and collaborative manner Congress intended.

Accordingly, compliance and oversight authority resides with other agencies, such as the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). Federal agency heads, in coordination with their Chief Information Officers and Senior Agency Information Security Officers, report the security status of their information systems to OMB in accordance with annual FISMA reporting guidance. In addition, agency Inspectors General provide an independent assessment of the security status of federal information systems, also reporting results to OMB annually.

NIST's statutory role as the developer—but not the enforcer—of standards and guidelines under FISMA has ensured NIST's ongoing ability to engage freely and positively with federal agencies on the implementation challenges and issues they experience in using these standards and guidelines. NIST meets frequently with agencies and holds regular Federal Security Manager Forums to discuss these issues, our standards and guidance, share lessons learned, and gain insights into methods and means to continually improve our standards, guidelines, and practices.

NIST is actively considering additional steps to assist federal agency cybersecurity practices, including ways in which Federal agencies might take advantage of the voluntary Cybersecurity Framework in implementing NIST's FISMA suite of standards, guidelines and best practices. Thoughtful application of the risk-based approach of the Cybersecurity Framework across the federal government could complement and enhance agency efforts to implement their programs. NIST will continue to seek to minimize the burden placed upon implementing departments and agencies by building from existing evaluation and reporting regimes, and encouraging common and comparable evaluation of cybersecurity capabilities across federal departments and agencies, given the diversity of missions, requirements and risk environments.

The President signed the American Innovation and Competitiveness Act (Public Law 114-329), which passed both Houses of the 114th Congress with bipartisan support, and amended the NIST Organic Act to include new requirements for research and analysis on the information security and challenges faced by the Federal government. NIST looks forward to working with this Congress and its stakeholders in government and industry on implementing these important provisions.

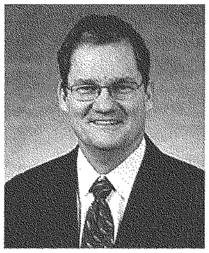
Conclusion

NIST recognizes that it has an essential role to play in helping industry, consumers and government to counter cyber-threats and enhance the security of the Nation's cyberinfrastructure and capabilities. The outputs from its cybersecurity portfolio are applicable to a wide variety of users, from small and medium enterprises to large private and public organizations, including federal government agencies and companies involved with critical infrastructure.

NIST is extremely proud of its role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, guidelines, and best practices, and of the robust collaborations enjoyed with its federal government partners, private sector collaborators, and international colleagues.

Thank you for the opportunity to testify today on NIST's work in cybersecurity. I would be happy to answer any questions you may have.

Charles H. Romine



Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $150 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the Nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:
Ph.D. in Applied Mathematics from the University of Virginia

B.A. in Mathematics from the University of Virginia.

Chairwoman COMSTOCK. Thank you, Doctor.

And now we'll hear from Mr. Mulholland.

TESTIMONY OF MR. IAIN MULHOLLAND, INDUSTRY MEMBER, CSIS CYBER POLICY TASK FORCE; CHIEF TECHNOLOGY OFFICER, SECURITY, VMWARE, INC.

Mr. MULHOLLAND. Chairwoman Comstock, Ranking Member Lipinski, Mrs. Johnson, other Members of the Committee, thank you for the opportunity to testify today.

I'm Iain Mulholland, a member of the Center for Strategic and International Studies Cyber Policy Task Force and the Chief Technology Officer for Security at VMware.

VMware is the fourth largest software company in the world with 2016 revenues of over $7 billion and over 19,000 employees globally.

The U.S. Government is dependent on a vast cyber world of interconnected networks, data centers, cloud, mobile platforms, and other assets. Because we require cyber infrastructure to perform the modern-day functions of government, sophisticated and aggressive cyber-attacks perpetuated by criminal entities and foreign government agencies represent a clear and present national security threat to the U.S. Government.

We are also experiencing an unprecedented level of cyber-attacks and sophistication in the private sector. The reality is that global technology companies like VMware not only receive an unprecedented amount of information in regards to cyber threats from inside the U.S. but we also receive a large number from overseas as well. The fact is, with data moving across borders instantly, the digital devices and technologies associated with this ecosystem and therefore with cybersecurity are not confined to physical borders.

In order to continue to provide world-class secure services, we must be able to act on a moment's notice whether that information is coming from the U.S. or from abroad. We must have the tools and resources on hand to act immediately.

Building on the 2009 Commission on Cybersecurity, the Center for Strategic and International Studies established the Cyber Policy Task Force to lay out practical steps for policy, resources and organization that the new Administration can use to build better cybersecurity. In the eight years since that report was published, there has been much activity and an exponential increase in attention to cybersecurity. However, we are still at risk and there's still much that this new Administration can do.

Specifically, CSIS believes that there are five core areas that require renewed focus. Firstly, the development of a new international strategy based on partnerships with like-minded nations to improve the ability of deterring attackers.

Secondly, there must be a serious effort to reduce cybercrime to build international cooperation to fight botnets and sophisticated financial crime. Part of this effort must be to penalize countries that won't cooperate in the effort to reduce and control cybercrime.

Thirdly, we must prepare our critical infrastructures and services for attack and improve cyber hygiene. Greater use of shared, managed and cloud services can make government agencies more secure.

Further, we must identify where federal action and resource issues such as research or workforce development is necessary. And finally, we must streamline White House bureaucracy, increase oversight of federal cybersecurity, and clarify the rules of DOD and other agencies. A stronger DHS is crucial, and the new Administration must strengthen DHS's role in cybersecurity.

Promoting good cyber hygiene should also be a key standard that helps agencies, consumers, and businesses better protect their information and networks from hackers. One of the best ways for the federal government to be proactive is by deploying microsegmentation technology that offers the ability to segment their networks in the event of a breach. Let's use the example of the cybersecurity breach at OPM. The nature of the security breach at OPM was not particularly unique. Hackers were able to penetrate perimeter network security systems and gain access to OPM and Department of Interior systems where they were free to roam around the internal networks and steal sensitive data over a period of months. In order to effectively prevent an attacker from moving freely around the network, agencies must compartmentalize their network perimeters by adding zero trust or microsegmented networks within the data center. A zero-trust environment prevents unauthorized lateral movement within a data center by establishing automated governance rules that manage the movement of users and data between systems and applications.

Lastly, I'd like to touch on another topic that is important to securing the cyber ecosystem, the internet of things. As we saw from the distributed denial-of-service attacks in October, there are security vulnerabilities that must be addressed to advance the IOT economy. A way to better secure the IOT ecosystem is by ensuring flexible and isolated connection points through secure managed infrastructure such as edge systems, which include but are not limited to IOT gateways.

As Congress and the Administration continue to work on policies to promote the IOT economy, we believe that some consideration should be given to developing some rules of the road, standards for IOT moving forward. Among others, we would agree with the CSIS recommendation calling on NIST and other federal agencies to cooperate with industry stakeholders to develop a set of standards and principles for IOT security.

Lastly, another security issue looming that could have significant impact on the cyber ecosystem is the 2013 Wassenaar Arrangement. I've included more on this topic in my written testimony. My hope is that the new Administration will continue to view this as a leadership opportunity for the U.S. to ship international cyber norms and support ongoing renegotiations at the Wassenaar Arrangement. The continued U.S. renegotiation efforts in partnership with the U.S. technology industry and bipartisan support from Congress can ensure a signed Wassenaar cyber agreement that enhances our nation's cyber posture and ultimately strengthens our defense against attacks.

Thank you for the opportunity to testify today, and I look forward to answering the Committee's questions.

[The prepared statement of Mr. Mulholland follows:]

Testimony for the Record

Iain Mulholland

Industry Member, Center for Strategic and International Studies

(CSIS) Cyber Policy Take Force;

Chief Technology Officer for

Security, VMware, Inc.

Before the

U.S. House of Representatives

Committee on Science and Technology Subcommittee on
Research and Technology

"Strengthening U.S. Cybersecurity Capabilities"

February 14, 2017

Chairwoman Comstock and Ranking Member and Members of the Committees, thank you for the opportunity to testify today at this important hearing. I am Iain Mulholland, an industry member for the Center for Strategic and International Studies (CSIS) Cyber Policy Task Force; and Chief Technology Officer for Security at VMware Inc. I have nearly 20 years of experience in the product security field, including establishing VMware's Product Security Group in 2011. Before VMware, I worked for a number of leading technology companies, including Microsoft, where in 2002, I was a founding member of the company's Trustworthy Computing Group.

My current employer, VMware, is a leading provider of software-defined solutions that increase the operation efficiency and security of data centers across the globe. Currently, VMware, is the fourth largest software company in the world with 2016 revenues of over $7 billion and over 19,000 employees. We are headquartered in Silicon Valley with 140 offices throughout the world, that serve more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. In addition to VMware's work throughout commercial markets, VMware remains committed to serving all sectors of the U.S. Government; including the Department of Defense, Civilian agencies, and the Intelligence Community, as well as state and local governments.

We are committed to enabling both government and commercial organizations with the ability to respond to their dynamic business needs, whether they utilize on premise datacenters, the cloud, or personal computers and mobile devices. VMware is providing enhanced security to government and commercial customers globally through its pioneering role in redefining how we build and secure networks, data centers, computers and devices.

Cybersecurity Policy

The U.S. Government is dependent on a vast cyber world of interconnected IT networks, data centers, the Cloud, mobile platforms, and other assets. Individual agencies rely on this cyber infrastructure to perform almost every mission critical function within their purview, from national defense and natural disaster response to postal services and the constitutionally mandated Census. In many cases, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. The widespread adoption and use of cyber-systems has reaped immeasurable benefits for the country through increased government responsiveness, agency effectiveness, worker productivity, and a host of other economic efficiencies and returns.

Because we require cyber infrastructure to perform the modern-day functions of government, sophisticated and aggressive cyber-attacks perpetuated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. As you know, there have been well-publicized cyber-attacks, including one of the largest cyber-attacks on a U.S. agency, the Office of Personnel Management (OPM), which suffered one of the most damaging breaches of information ever on government workers. As this Committee knows, the OPM breach and the other federal agency attacks, have compromised the personal data and security of over 21 million current and former federal employees and has likely compromised our national security, national defense, and national intelligence posture(s). These breaches have put our nation's blood and treasure at risk.

We are also experiencing an unprecedented level of cyber-attacks and sophistication in the private sector. The reality is that global technology companies, like VMware, not only receive an unprecedented amount of information in regards to cyber threats from inside the U.S., but we also receive a large number from overseas as well. The fact is, with data moving across borders instantly, the digital devices and technologies associated with the ecosystem, and therefore cybersecurity, is not confined to physical borders. In order to continue to provide world-class secure enterprise software and services and ensure customer safety, we must be able to act on a moment's notice, whether that information is coming from the U.S. or abroad. We must have the tools and resources on hand to act immediately.

Building on the 2009 Commission on Cybersecurity, the Center for Strategic and International Security established the Cyber Policy Task Force to lay out practical steps for policy, resources and organization that the next Administration can use to build better cybersecurity. The goals for a national approach to better cybersecurity remain largely the same: to create a secure and stable digital environment that supports continued economic growth, while protecting personal freedoms and national security. The requirements for implementation also remain the same: central direction and leadership from the White House to create and implement a comprehensive and coordinated approach to cybersecurity.

In the eight years since that report was published, there has been much activity and an exponential increase in attention to cybersecurity, however, we are still at risk and there is much for this current Administration to do.

Specifically, CSIS believes that there are five core areas that require renewed focus:

- First, the development of a new international strategy based on partnerships with like-minded nations, to improve the ability of deterring attackers, by developing a full range of response and countermeasures that go beyond the threat of military action.

- Secondly, there must be a serious effort to reduce cybercrime, with consistent Cabinet level support, to build international cooperation to fight botnets and sophisticated financial crime. Part of this effort must be to penalize countries that won't cooperate in the effort to reduce and control cybercrime.

- Thirdly, we must prepare our critical infrastructures and services for attack and improve "cyber hygiene." The new Administration should use incentives when possible, but be ready to regulate if incentives don't work. Greater use of shared, managed and cloud services can make government agencies more secure.

- Furthermore, we must identify where Federal action in resource issues, such as research or workforce development, is necessary, since many of these efforts are best left to the private sector. We don't need a cyber "Manhattan Project."

- And finally, we must streamline White House bureaucracy, increase oversight of Federal cybersecurity by creating a special GAO office, and clarify the roles of DOD and other agencies. A stronger DHS is crucial, and the new Administration must either strengthen DHS move the cybersecurity mission.

To build on the theme of increasing the cyber role of DHS, in the President's Commission on Enhancing National Cybersecurity Report published in December, one of the recommendations (5.1) was to consolidate basic network operations in the Federal Government. I agree with this recommendation, but only if network architecture is done the correct way with the proper security. In President Obama's Cybersecurity National Action Plan (CNAP), he expanded the Department of Homeland Security's EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs. As the Committee knows, these two programs were designed to detect, prevent and mitigate cyber incidents on the Federal Government's Civilian networks.

Originally conceived as a three-phased program, the FY17 Department of Homeland Security Budget request expanded the CDM program to add a Phase 4 in order to address the ever-changing cybersecurity landscape. This expands on CDM Phase 3, which primarily focuses on boundary protection, including data loss prevention, and incident response. CDM Phase 3 provides Federal civilian departments and agencies with the capability of identifying and protecting against anomalous activity inside Federal networks, as well as alerting security personnel for expedited remediation. CDM Phase 4 will expand the program to include additional tools and services that protect sensitive and high value asset data **within** agency networks.

These tools and services include programming that mimics current data stores (data masking), encodes data during its transfer (encryption), creates multiple compartments within a system for data storage (micro-segmentation), and only allows individuals with specific credentials to access and manipulate specific data (digital rights management), as well as deploys, secures, monitors, integrates and manages mobile devices, such as smartphones, tablets and laptops, in the workplace (mobile device management).

Microsegmentation Policy

I'd like to take a minute to highlight microsegmentation, a key part of the CDM Phase 4 program and explain why I believe it must be continued, expanded and accelerated to fully secure government networks.

VMware testified before this Committee last year to discuss the best practices that the government could adopt to lessen cyber threats. Let's take the Office of Personnel Management (OPM) breach as an example again. As is apparent from publicized accounts, the nature of the security breach at OPM is not particularly unique. Hackers were able to penetrate perimeter network security systems and subsequently gain access to OPM systems, where they were free to roam around the internal network and steal sensitive data over a period of several months. Hackers typically use this attack methodology because traditional perimeter-centric security systems are structurally designed to be "doors" to the network. These doors serve to allow authorized users access to networked systems and to prevent unauthorized users from getting inside a network. However, structurally the perimeter is the single point of failure (a single perimeter: firewall + additional security systems like intrusion prevention or advanced attack detection) that must be breached in order to enter the data center network. Once the intruder has penetrated perimeter security, there is no simple means to stop malicious activity within the data center without extreme disruption to the agency's mission. In many cases, the response from agencies and network security vendors is to add more security technology to the perimeter – which ignores the structural issue.

VMware submits three salient points for consideration:

1) Every recent agency breach has had one thing in common: the attacker, once inside the perimeter security, has been able to move freely around the agency's network.
2) Perimeter-centric cyber security policies, mandates, and techniques are necessary, but alone they are insufficient and ineffective in protecting U.S. Government cyber assets.
3) These cyber-attacks will continue – but we can greatly increase our ability to prevent them, and limit the damage and severity of the attacks when they do.

There are lots of perimeter-centric technologies that are designed to stop an attacker from getting inside a network – clearly this approach is not sufficient to combat today's cyber-attacks. Perimeter-centric security solutions are analogous to a locked door that can only be accessed with a key. The primary function of the door is to deny initial unauthorized entry by anyone that does not have a key. However, once the door is forced open (hacked or breached), the unauthorized actor is free to move throughout (laterally) unabated.

In order to effectively prevent an Attacker from moving freely around the network, agencies must compartmentalize their networks by creating "zero-trust" or "micro-segmented" network environments within the data center. A zero-trust environment prevents unauthorized lateral movement within the data center by establishing automated governance rules that manage the movement of users and data between business systems and/or applications within the data center network. When a user or system "breaks the rules", the potential threat incident is compartmentalized and security staff can take any appropriate remediation actions. To build on the analogy above, compartmentalization is equivalent to securing each interior room with locks. Only those with the appropriate keys can move freely within the data center. The magnitude of a perimeter security breach, or break-in, is significantly mitigated by limiting the intruder's ability to move around freely within the house.

In an era of constrained resources and imminent threat, the old perimeter based approach is insufficient and untimely. Congress last year did not fully fund CDM Phase 4 due to budget constraints. We would urge this Committee's strong support for full and accelerated funding for the Einstein and CDM programs.

IoT Security

I'd also like to touch on another topic that is important to securing the cyber eco-system, the Internet-of-Things (IoT).

We are at the cusp of the Internet-of-Things, the Internet of Everything, where we have an intelligent world connected in almost every aspect of our daily lives. From our health care to manufacturing to banking to home monitoring, and now into "smart cities", transportation and the list goes on. IoT has been called by some as "the next Industrial Revolution." In fact, several recent studies, including a recent Business Insider survey, estimate that "there will be 34 billion devices connected to the Internet by 2020, up from 10 billion in 2015. IoT devices will account for 24 billion, while traditional computing devices (i.e. smartphones, tablets, smartwatches, etc) will comprise of 10 billion."

Due to this increasingly interconnected economy, there is no doubt that "security" is the linchpin for the advancement of IoT technologies. We have seen the impact and vulnerabilities from the October DDoS attack that targeted many older, outdated devices, devices that did not utilize any of the industry's standard best practices for cybersecurity.

Consumers, businesses and Government need to feel confident that IoT technologies are secure and their privacy is protected. At VMware, we have launched Liota (Little IoT Agent), a vendor neutral Open Source software development kit for building secure IoT gateway data and control applications.

A way to secure the IoT ecosystem is by ensuring flexible and isolated connection points through secure manageable infrastructure, such as edge systems, which include, but not limited to, IoT gateways. Whenever an IoT device connects to the Internet, whether by itself or through an IoT gateway, that system needs to be manageable, deployed responsibly with a proper initial configuration, and maintained at the current state of best-security-practices available throughout the complete lifetime of the device.

IoT gateways are an integral part of the IoT infrastructure. They bridge, but also decouple, the physical IoT devices from management components in data centers. This bridge allows data and control to move freely and securely from the device to the cloud or data center. We will need secure IoT Gateways to ensure data and information are secured as it moves through the IoT pipeline.

As Congress and the Administration continue to work on policies promoting the IoT economy, we believe that some consideration should be given to developing some rules of the road type standards for IoT moving forward. Absent any Federal action around IoT, standards could be developed in divergent and potentially disruptive ways. Among others, we would agree with a CSIS recommendation calling on NIST and other federal agencies to cooperate with industry stakeholders in order to develop a set of standards and principles for IoT security.

Wassennaar

Another cybersecurity issue looming that could have a significant impact on the cyber ecosystem is the 2012 Wassenaar Arrangement.

The Wassenaar Arrangement was originally established over 20 years ago and now includes 41 nations to promote transparency and responsibility in transfers of conventional arms and dual-use goods and technologies. In 2013, the Wassenaar Plenary, seemingly expanded its original mission beyond regulating technologies that could be incorporated into conventional weapon systems, to include regulating the export of certain types of equipment, software and technology used to distribute or produce malicious "intrusion software." We know that the two capabilities demand two separate and unique skill sets. Regulating conventional weapons and arms requires a very unique expertise, much different from the expertise required to develop, code and patch software.

In short, the 2013 Wassenaar rules would severely impact the ability of the U.S. technology industry to test and share code used to test for security vulnerabilities in our products, services and global infrastructure. This would lead to less secure products and ultimately, less security for customers and the global cyber ecosystem.

Last year, to their credit, the U.S. government recognized that it needed private sector technologists at the negotiating table to help renegotiate the "software intrusion" provisions included in the 2013 Wassenaar Arrangement. I was invited to join the U.S. Delegation in Vienna during the June and September Wassenaar Sessions with the goal of providing U.S. technology and security industry expertise directly at the negotiating table. This was the first time that the U.S. Delegation included non-government cyber experts at the September meeting, due to niche knowledge we provide as security practitioners.

That said, the new Administration faces an ever-increasing amount of challenges in securing cyberspace. Attacks are on the rise and massive numbers of interconnected devices threaten to overwhelm Internet defenders. Cyber export control agreements have been drafted in the past several years, and the importance of getting them right affects not just national security, but the entire global Internet ecosystem. Getting them wrong means crippling Internet defenders.

It is my hope that the new Administration will continue to view this as a leadership opportunity for the U.S. to shape international cyber norms and support the ongoing renegotiations on the Wassenaar Arrangement. The continued US renegotiation efforts, in partnership with the U.S. technology industry and bipartisan support from Congress, can ensure a sound Wassenaar Cyber Agreement that enhances our nation's cyber posture and ultimately strengthens our defense against attacks.

Summary

As I mentioned in my testimony, the global digital ecosystem is experiencing an unprecedented level of cyberattacks and sophistication. In order to secure and adequately protect our customers, products, services and networks against these highly sophisticated entities we must utilize every security tool we have in the toolbox. As laid out in my testimony, CSIS proposes a series of recommendations that Congress and the Administration should consider to reduce the threat of cybersecurity on federal and commercial networks.

Promoting good cyber hygiene should also be a key standard that helps agencies, consumers and businesses better protect their information and networks from hackers. One of the best ways for the Federal Government to be pro-active is by deploying microsegmentation technologies that offer the ability to segment their networks in the event of a breach.

Additionally, as part of enhancing the global cyber eco-system, we must ensure that devices and technologies associated with the Internet-of-Things (IoT) are secure for consumers, businesses and the federal government. Security is the key principle that will enable and advance further adoption in IoT. Congress and the Administration should look to develop reasonable standards around IoT security moving forward.

Lastly, I would like to encourage the new Administration to continue to seek reasonable improvements to the 2013 Wassenaar Arrangement. The U.S. has an opportunity to demonstrate global leadership to craft new international cyber agreements in the future. The new Administration should continue the negotiating efforts at Wassenaar moving forward.

I appreciate the opportunity to share my thoughts on this very important issue. We applaud the leadership and vision of the Chairmen and Ranking Members for holding this hearing. CSIS and VMware look forward to continuing to participate in efforts to find solutions to help resolve this issue. Thank you again for the opportunity.

Chairwoman COMSTOCK. Thank you.

And now we will hear from Dr. Burley.

TESTIMONY OF DR. DIANA BURLEY, EXECUTIVE DIRECTOR AND CHAIR, INSTITUTE FOR INFORMATION INFRASTRUCTURE PROTECTION (I3P); PROFESSOR, HUMAN AND ORGANIZATIONAL LEARNING, THE GEORGE WASHINGTON UNIVERSITY

Dr. BURLEY. Good morning. Chairwoman Comstock, Ranking Member Lipinski, and Mrs. Johnson, Members of the Committee, I am honored to appear before you today to discuss strategies for strengthening U.S. cybersecurity capabilities.

Recommendations from the recent reports serving as the foundation of this Committee hearing highlight the critical importance of developing a cybersecurity workforce of sufficient quality and quantity to meet the global threat environment. The workforce need is acute and immediate with a projected shortfall of nearly 1.5 million professionals by the year 2020.

Yet despite significant effort and steady progress, the gap between supply and demand is widening. Of the recommendations offered in the recent reports, I will briefly address two.

The first, to develop a comprehensive cybersecurity education and workforce development model that standardizes interdisciplinary curricula, that serves as a foundation for accreditation, and integrates with existing programs and taxonomies. To implement this recommendation, I suggest that the federal government leverage the work of the Association for Computing Machinery, the ACM Joint Task Force on Cybersecurity Education. I serve as Co-Chair of this task force, and our work, which is developing the first set of global curricular guidelines in cybersecurity education, structuring the cybersecurity discipline and providing comprehensive and flexible curricular guidance, will be complete late this year.

Several points drive my recommendation. First, with over 100,000 members, the ACM is the largest computing society in the world, and the framework is being developed by global subject-matter experts across academia, government and industry. The ACM has nearly 50 years of experience developing curricular guidance, and the document will be endorsed by major computing societies, the ACM, the IEEE Computer Society, the Association for Information Systems, and the International Federation for Information Processing.

The framework is grounded in both the interdisciplinary nature of cybersecurity and the inherently technical foundation of the field. It facilitates the alignment between curricular content and workforce frameworks including the National Cybersecurity Workforce Framework developed through the U.S. National Initiative for Cybersecurity Education, and it forms the foundation for emerging accreditation standards currently under development by ABET.

The second recommendation from the reports is to add new credentialing requirements and to develop a network of credentialing associations. The call for additional credentialing requirements is not new. I support the need to ensure cybersecurity professionals maintain the highest level of competency but caution against blanket professionalization requirements that do not consider differences in occupational needs. Cybersecurity is a broad field with many occupations and the needs of those occupations must be considered separately. I co-chaired the 2013 National Research Council Committee on Professionalizing the nation's Cybersecurity Workforce that addressed this issue. As we state in our report, before new credentialing requirements are added, workforce developers should review specific occupational characteristics, identify the associated workforce deficiencies, and consider the tradeoffs associated with implementing additional requirements. I urge the federal government to continue to catalyze activities and to leverage existing multisector stakeholder groups like the Institute for Information Infrastructure Protection (The I3P) to integrate, accelerate and guide existing cybersecurity workforce development initiatives. These initiatives should leverage existing and scalable models, emphasize both evidence-based short-term interventions that address immediate needs, and strategic long-term initiatives that address the entire ecosystem; expand the pipeline by engaging a broad cross-section of society to include women, ethnic groups typically underrepresented in this workforce, veterans, and even special-needs populations who possess targeted skill sets, to lengthen the pipeline by engaging students early in their education, and including K–12 teachers who will largely influence those students' choices.

A coordinated and comprehensive cybersecurity workforce development strategy that supports our ability to scale is a critical success factor for strengthening U.S. cybersecurity capabilities.

Again, I am honored to appear before the Committee, and I look forward to your questions. Thank you.

[The prepared statement of Dr. Burley follows:]

TESTIMONY OF

Dr. Diana L. Burley

Professor, Human and Organizational Learning
Executive Director, Institute for Information Infrastructure Protection
The George Washington University
Washington, DC

BEFORE THE

United States House of Representatives
Committee on Science, Space & Technology
Subcommittee on Research and Technology

HEARING ON

Strengthening U.S. Cybersecurity Capabilities

February 14, 2017

Rayburn House Office Building
Washington, DC

Chairwoman Comstock, Vice Chairman Abraham, Ranking Member Johnson, members of the Committee, I am honored to appear before you today to discuss strategies for strengthening U.S. cybersecurity capabilities as our nation faces the a global threat environment where cybercrime damage is projected to exceed $2 trillion by 2019.[1]

My name is Diana Burley. I am professor of human & organizational learning and the executive director and chair of the Institute for Information Infrastructure Protection[2] (I3P) at The George Washington University (GW).

For more than 15 years, I have worked to build the nation's cybersecurity workforce by leading workforce development initiatives, defining best practices in cybersecurity education, and informing policy and practice through rigorous research and analysis. I have authored nearly 75 publications on the subject and have been honored as both the cybersecurity educator of the year and the government leader of the year; as well as a top influencer in information security careers. In short, my experiences across government, academia and industry provide me with a unique vantage point from which to offer the committee insight and recommendations on building the nation's cybersecurity workforce.

In my remarks today I will:

- Provide background and describe the current cybersecurity workforce context;
- Discuss workforce development recommendations offered in the January 2017 CSIS Cyber Policy Task Force report and the December 2016 report of the Commission on Enhancing National Cybersecurity; and
- Suggest actionable steps toward meeting the national need for a cybersecurity workforce capable of meeting the evolving threat.

Taken together, my recommendations support a holistic approach to building the nation's cybersecurity workforce – one that includes both evidence-based short-term interventions that address immediate needs, and strategic long-term initiatives that address the entire ecosystem of educational, professional and environmental challenges.

Institute for Information Infrastructure Protection

The I3P is a national consortium of leading academic institutions, national laboratories, and non-profit research organizations. The I3P is housed at The George Washington University where I manage the consortium in collaboration with SRI International and an executive committee currently comprised of representatives from Johns Hopkins University Applied Physics Laboratory, Dartmouth College, the MITRE Corporation, and the University of California, Davis. In my role as executive director and chair I work with

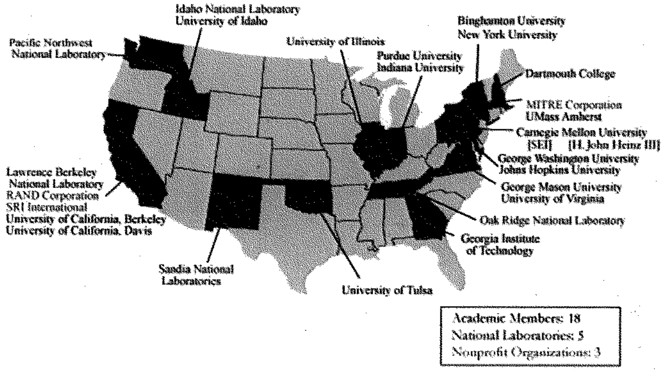
[1] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
[2] I3P website: http://www.thei3p.org
[2] I3P website: http://www.thei3p.org

our executive committee to establish strategic priorities, engage with project sponsors, launch and manage research projects, and advise stakeholders on research results.

Since its' founding in 2002 at Dartmouth College, the I3P has been a cornerstone in cybersecurity research and development. The I3P brings together researchers, government officials, and industry representatives to address cybersecurity challenges affecting the nation's critical infrastructure. Drawing from its member institutions, the I3P assembles multi-disciplinary and multi-institutional research teams that bring in-depth analysis to complex cybersecurity challenges. The I3P's impact on cybersecurity research, policy, and practice has taken many forms, including:

- **49 national workshops** that convened cybersecurity subject matter experts across academia, government and industry to address challenges related to security the nation's critical information infrastructure.
- **65+ journal papers** resulting from I3P driven research projects (many of these projects were sponsored by the Department of Homeland Security, the National Institute of Standards and Technology, and the National Science Foundation).
- **366+ technical reports, workshop and conference proceedings, and Congressional testimonies** produced by I3P researchers and disseminated to national (and in many instances, global) stakeholders.
- **12 tools/technology transfers** between academic institutions, national laboratories, non-profit research institutions, and government agencies.
- **19 postdoctoral research fellowships** that advanced scientific discovery and dissemination by linking researchers across academia, government and industry.

The 26-member I3P consortium includes 18 academic research institutions, 5 national laboratories, and 3 nonprofit research organizations – a roster that brings intellectual breadth and depth to the analysis of cybersecurity challenges.


Idaho National Laboratory
University of Idaho
Pacific Northwest National Laboratory
University of Illinois
Purdue University
Indiana University
Binghamton University
New York University
Dartmouth College
MITRE Corporation
UMass Amherst
Carnegie Mellon University
[SEI] [H. John Heinz III]
George Washington University
Johns Hopkins University
George Mason University
University of Virginia
Oak Ridge National Laboratory
Georgia Institute of Technology
Lawrence Berkeley National Laboratory
RAND Corporation
SRI International
University of California, Berkeley
University of California, Davis
Sandia National Laboratories
University of Tulsa
Academic Members: 18
National Laboratories: 5
Nonprofit Organizations: 3

The Cybersecurity Workforce Context

As evidenced by this hearing today, building a highly capable cybersecurity workforce remains a top national priority. To meet this critical workforce need, the U.S. federal government sponsors several major initiatives.

The U.S. National Science Foundation Scholarship for Service: Cyber Corps program provides scholarships to students who will join the federal cybersecurity workforce and capacity building funds to academic institutions developing cybersecurity programs. I led this program from 2004-2007. During that period, the federal government was challenged with building a cybersecurity workforce that had little structure, uncertain priorities, and limited awareness of the nature of the threat or specific workforce needs. The federal government also faced significant challenges in attracting young professionals to public service. In addition to these demand-side challenges, academic institutions tasked with providing a supply of new professionals, were largely developing programs alone. With the exception of the National Security Agency (NSA) Centers of Academic Excellence (CAE) [3] program, which provides curricular content for programs in information assurance, academic institutions had little guidance on how to develop cybersecurity programs. Since that time, federal efforts led by the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE)[4] have established a workforce framework with work roles and career pathways, assisted in the development of workforce priorities, raised awareness of workforce and educational needs, and contributed to the generation of curricular resources to aid in program development.

These initiatives are, in large part, responsible for the steady increase the number of cybersecurity professionals entering the national workforce. Yet, while these federal programs serve as a major driver of the cybersecurity workforce, they have not been sufficient to address the growing demand. In fact, despite significant efforts to increase the size and quality of the workforce, the U.S. still faces a projected shortfall of nearly 1.5 million cybersecurity-related professionals by 2020[5]. The workforce need is acute, immediate, and the gap between supply and demand is growing.

Recent Recommendations to Build the Cybersecurity Workforce

Recent reports by the CSIS Cyber Policy Task Force and the Commission on Enhancing National Cybersecurity recognize this critical need and identify cybersecurity workforce development as a critical success factor for strengthening U.S. cybersecurity capabilities.

[3] NSA Centers of Academic Excellence Program: https://www.nsa.gov/ia/academic_outreach/nat_cae/

[4] National Initiative for Cybersecurity Education: http://csrc.nist.gov/nice/about.html

[5] See, for example, CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

Specifically, the January 2017 CSIS report, "From Awareness to Action: A Cybersecurity Agenda for the 45th President[6]," recommends:

> "The next administration should develop and implement an ambitious education and workforce model for cybersecurity, with a system for accrediting training and educational institutions; a taxonomy of cybersecurity roles and the skills that practitioners must demonstrate to claim competence in each specialty; and a robust network of professional credentialing entities."

A Comprehensive Model

The call for a comprehensive cybersecurity education and workforce development model that standardizes interdisciplinary curricula, serves as a foundation for accreditation efforts, integrates with existing programs, and provides the taxonomy of work roles, is echoed in recommendation 4.1 of the Commission on Enhancing National Cybersecurity report[7].

In fact, academic institutions are also calling for a comprehensive curricular model. Institutions across the spectrum of computing disciplines are launching initiatives to establish cybersecurity programs and need curricular guidance based on a holistic view of the cybersecurity field, the specific demands of the base computing discipline, and the relationship between the curriculum and cybersecurity workforce frameworks.

The Association for Computing Machinery (ACM) Joint Task Force on Cybersecurity Education (JTF)[8] is developing the curricular model called for by these groups. As the first set of global curricular guidelines in cybersecurity education, Cybersecurity 2017 (CSEC2017) will provide:

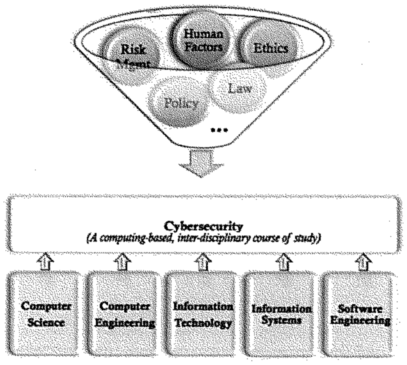
- Comprehensive and flexible curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level.
- A curricular volume that structures the cybersecurity discipline and provides guidance to institutions seeking to develop or modify a broad range of programs rather than a prescriptive document to support a single program type.

I serve as the CSEC2017 task force co-chair. The development process is well underway and the curricular volume will be published in late 2017. **I strongly urge the federal government to leverage this effort in the implementation of the recent recommendations for several key reasons.**

[6] CSIS report: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf
[7] Commission on Enhancing National Cybersecurity: https://www.nist.gov/cybercommission
[8] ACM Joint Task Force: http://CSEC2017.org

First, the CSEC2017 is being developed by global subject matter experts across academia, government and industry; and the professional societies leading this effort have nearly 50 years of experience developing curricular guidance. With over 100,000 members, the ACM is the largest global computing society. For nearly five decades, starting with Computer Science 1968[9], the ACM has collaborated with other professional and scientific societies to establish curricular guidelines for academic program development in the computing disciplines[10]. Currently, ACM curricular volumes provide guidance in computer science, computer engineering, information systems, information technology, and software engineering. The curricular recommendations produced by this task force will be endorsed by major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS)[11], Association for Information Systems Special Interest Group on Security (AIS SIGSEC)[12], the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)[13], and the Cyber Education Project (CEP)[14].

Second, the model is grounded in both the interdisciplinary nature of cybersecurity and the inherently technical foundation of the field. Cybersecurity is emerging as an identifiable discipline. While cybersecurity is an interdisciplinary course of study; including aspects of law, policy, human factors, ethics, and risk management; it is fundamentally a computing-based discipline. As such, and as depicted below, academic programs in cybersecurity are both informed by the inter-disciplinary content, and driven by the needs and perspectives of the computing discipline that forms the programmatic foundation.



[9] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197.
[10] ACM Computing Disciplines Overview: http://acm.org/education/curricula-recommendations
[11] IEEE CS website: https://www.computer.org/
[12] AIS SIGSEC website: http://aisnet.org/group/SIGSEC
[13] IFIP WG 11.8 website: https://www.ifiptc11.org/wg118
[14] Cyber Education Project website: http://cybereducationproject.org/about/

Cybersecurity programs require curricular content that includes: (1) the theoretical and conceptual knowledge essential to understanding the discipline and; (2) opportunities to develop the practical skills that will support the application of that knowledge. The content included in any cybersecurity program is requires a delicate balance of breadth, depth, along with an alignment to workforce needs. It also demands a structure that simultaneously provides for consistency across programs of similar types while allowing for flexibility necessitated by both local needs and advancements in the body of knowledge.

Third, the CSEC2017 model organizes curricular content, facilitates the alignment between curricular content and workforce frameworks, and forms the foundation of emerging accreditation standards. The CSEC2017 joint task force is actively coordinating with workforce framework developers within the federal government in order to provide a bridge between the curricular content and specific work roles. In addition, members of the task force also serve as leaders in the Accreditation Board for Engineering and Technology (ABET) process to develop accreditation criteria for both computer science-based and engineering-based cybersecurity degree programs.

Credentialing

The CSIS and Commission reports also assert the need for additional professionalization requirements; advanced training, skill-based demonstrations, and a network of credentialing associations all have been advanced as important components of a comprehensive workforce development strategy.

The call for additional credentialing requirements is not new. Although I strongly support the need to ensure cybersecurity professionals have and maintain the highest level of competency, I also caution against blanket professionalization requirements that do not consider differences in occupational needs. In 2013, I co-chaired the U.S. National Research Council Committee on Professionalizing the Nation's Cybersecurity Workforce[15]. Our report, sponsored by the Department of Homeland Security, highlighted the breadth of the field and provided criteria for decision-makers on whether, when, and how to assess the need for additional professional requirements. We argue that before professionalization activities such as licensure, certifications, or skill-based exams are undertaken, an occupation must have well-defined characteristics: stable knowledge and skill requirements, stable job roles, occupational boundaries, and career ladders. Further, the specific workforce deficiencies to be remedied by the professionalization mechanism must be identified and aligned with the intervention.

As a final step to determining if additional credentialing requirements are appropriate, the tradeoffs associated with additional requirements must be considered:

- *Do the benefits of a given professionalization measure outweigh the potential supply restrictions resulting from the additional barriers to entry?*

[15] Professionalizing the Nation's Cybersecurity Workforce: https://www.nap.edu/read/18446/chapter/1

- *Does the potential to provide additional information about a candidate outweigh the risks of false certainty about who is actually best suited for a job?*
- *Do the benefits of establishing the standards needed for professionalization outweigh the risks of:*
    - *Obsolescence (when the knowledge or skills associated with the standard are out-of-date by the time a standard is agreed on) and*
    - *Ossification (when the establishment of a standard inhibits further development by workers of their skills and knowledge)?*

It is important to note that professionalization can serve as a magnet that attracts people to the occupation, as a funnel that restricts the supply of people entering the occupation, or as a sieve that filters people out of the occupation based on increased requirements.[16]

Given the significant workforce shortages, a thoughtful approach to additional credentialing requirements must be taken. The danger of increased requirements leading to people exiting the field is particularly important given the increasingly integrated nature of cybersecurity work roles. The Commission on Enhancing National Cybersecurity report highlights this point, asserting that "cybersecurity work roles and responsibilities are increasingly being integrated into a growing array of jobs at all levels with nearly all organizations.[17]" Individuals performing these hybrid roles will likely be subject to an abundance of requirements. While additional requirements associated with additional responsibilities will most certainly be expected, workforce development framers should be careful not to unnecessarily overload professionals.

I urge the federal government to consider the recommendations put forth in the National Research Council Professionalizing the Nation's Cybersecurity Workforce: Criteria for Decision-Making report before implementing additional professionalization and credentialing requirements.

Building the Workforce Pipeline

Developing the K-12 pipeline is a key strategy for building a cybersecurity workforce of sufficient capacity and capability to address current and emerging threats. K-12 educators (teachers, counselors, and administrators) are a critical factor in supporting student participation in cybersecurity career development activities (e.g. high school computer science curricula, cybersecurity competitions and clubs). As such, cybersecurity educators provide an increasing number of professional development opportunities for K-12 educators. These opportunities typically take the form of summer boot camps, workshops and access to resources.

[16] Diana L. Burley, Jon Eisenberg, and Seymour E. Goodman. 2014. Would cybersecurity professionalization help address the cybersecurity crisis?. *Commun. ACM* 57, 2 (February 2014), 24-27. DOI: https://doi.org/10.1145/2556936

[17] cite quote

While helpful, these professional development efforts leave major gaps. First, they primarily target computer science or technically oriented teachers; leaving out the vast majority of K-12 teachers and administrators. Second, they rely on the participation of self-selected teachers who have the time, interest and pre-requisite knowledge to take advantage of the opportunities. Third, teachers have limited support for integrating the cybersecurity content into their courses. Fourth, the current approach is primarily focused on 'raising awareness' of cybersecurity topics for the vast majority of K-12 teachers, counselors, and administrators. While awareness is important, as the primary interface with the students we want enter the cybersecurity career pipeline, K-12 educators need more than post-degree professional development. They need cybersecurity educational opportunities that are integrated into their formal educational degree programs.

I recommend that the federal government collaborate with post-secondary colleges of education to develop and disseminate curricular guidance and resources for teachers, administrators, and other school staff members to provide a continuum of learning experiences which result in the development of actual cybersecurity skills and a portfolio of teacher-developed resources to support the integration of cybersecurity and cybersecurity career awareness into broad teaching practice.

Raising Awareness

Both reports call on the new administration to implement programs that will raise awareness and engagement among the general citizenry. In this context, the term "engagement" is key.

I recommend that cybersecurity awareness programs be reconstituted to emphasize the behavioral changes that depend on participant engagement. Raising awareness of cybersecurity threats is necessary but behavioral change relies on participant understanding of the impact of their actions.

Broadening Participation

Efforts to attract women, members of underrepresented minority groups, and veterans to the cybersecurity field are growing. These types of programs should be expanded to consider other special populations. For instance, several programs that focus on individuals with desired cognitive traits for specific work roles are being piloted to target potentially well-qualified entrants who think critically, rapidly recognize patterns, efficiently analyze quantitative data, and focus precisely: the exact profile of many cognitively able individuals with autism. At GW, we are launching the CyberBlue^{TM} initiative – a collaboration between the I3P and the Autism and Neurodevelopmental Disorders Institute (AND), as a bold, scalable solution that uses one social challenge to solve another.[18] I recommend that the federal government encourage the development and implementation of creative solutions such as CyberBlue^{TM} that expand the cybersecurity workforce pipeline beyond traditional populations.

[18] CyberBlue^{TM} video introduction: https://youtu.be/oJhzM4ttW-E

The field also suffers from a lack of leaders. Strategies to increase the supply of mid-level and senior-level employees with the cybersecurity experience and capabilities are critical.

I support the recommendations offered to build an executive cyber corps equipped with knowledge of technical cybersecurity concepts, the organizational and behavioral phenomena that will impact the successful implementation of cybersecurity initiatives, and advanced research and analytical skills that will allow them to adapt strategies in the face of evolving and increasingly complex threats.

Summary

Despite significant efforts to increase the size and quality of the workforce, a persistent and growing gap between supply and demand for skilled cybersecurity professionals exists. Strengthening U.S. cybersecurity capabilities requires a comprehensive and coordinated effort to build the cybersecurity workforce.

While workforce development experts assert the need to quickly surge the cybersecurity workforce, the recommendations implemented by the federal government must address both short- and long-term needs. A holistic approach to building the nation's cybersecurity workforce must include both evidence-based short-term interventions that address immediate needs, and strategic long-term initiatives that address the entire ecosystem of educational, professional and environmental challenges.

Actions implemented as a result of these recommendations should be empirically based, sustainable and scalable. Current initiatives are constrained by limited resources and a lack of models. These limitations prohibit the type of scaling which will be necessary if these programs are to meet an ever-growing societal need for a cadre of cybersecurity professionals.

The needs are immediate and the challenges are broad. So broad, in fact, that, as then NSA Director Admiral Michael Rogers said to the House (Select) Intelligence Committee in 2014, "It is going to take a true partnership between the private sector, the government, and academia to address [them]."[19]

I urge the federal government to leverage existing multi-sector stakeholder groups – consortia like the I3P, to integrate, accelerate, and guide existing cybersecurity workforce development activities that address both short- and long-term needs.

[19] https://www.nsa.gov/news-features/speeches-testimonies/testimonies/adm-rogers-testimony-20nov2014.shtml

Strengthening U.S. Cybersecurity Capabilities
Summary Testimony of Dr. Diana L. Burley

Strengthening U.S. cybersecurity capabilities requires a comprehensive and coordinated effort to build the cybersecurity workforce. Despite significant efforts to build the workforce, the gap between supply and demand persists. The workforce need is acute and immediate with a projected shortfall of nearly 1.5 million by 2020.

Of the recommendations offered in the recent reports by the Commission to Enhance National Cybersecurity and the CSIS Cyber Policy Task Force, I will address two:

Summary Recommendation 1: Develop a comprehensive cybersecurity education and workforce development model that standardizes interdisciplinary curricula, serves as a foundation for accreditation, and integrates with existing programs and taxonomies.

Comment: The Association for Computing Machinery (ACM) Joint Task Force on Cybersecurity Education is developing this type of model. As the first set of global curricular guidelines in cybersecurity education, CSEC2017 will structure the cybersecurity discipline, and provide comprehensive and flexible curricular guidance. I co-chair the CSEC2017 task force and the volume will be published in late 2017.

- The ACM has nearly 50 years of experience developing curricular guidance.
- The CSEC2017 is being developed by global subject matter experts across academia, government and industry; and will be endorsed by major computing societies: ACM, IEEE Computer Society, Association for Information Systems, and the International Federation for Information Processing.
- The model is grounded in both the interdisciplinary nature of cybersecurity and the inherently technical foundation of the field. It facilitates the alignment between curricular content and workforce frameworks, and forms the foundation of emerging accreditation standards.

Summary Recommendation 2: Add new credentialing requirements such as advanced training, skill-based demonstrations; and develop a network of credentialing associations.

Comment: The call for additional credentialing requirements is not new. I support the need to ensure cybersecurity professionals maintain the highest level of competency, but caution against blanket professionalization requirements that do not consider differences in occupational needs. Cybersecurity is a broad field with many occupations and the needs of each occupation must be considered separately. I co-chaired the 2013 National Research Council Committee on Professionalizing the Nation's Cybersecurity Workforce that addressed this issue. Before professionalization activities such as certifications or skill-based exams are undertaken, consider the occupational characteristics, specific workforce deficiencies, and the trade-offs associated with additional requirements.

To meet the growing societal need for a cadre of cybersecurity professionals, initiatives should address both short- and long-term needs; be empirically based and scalable; engage a broad cross-section of society; and target entry-, mid- and senior-level professionals. I urge the federal government to leverage existing multi-sector stakeholder groups – consortia like the I3P, to integrate, accelerate, and guide existing cybersecurity workforce development activities.

Diana L. Burley, Ph.D.

Diana L. Burley, Ph.D. is executive director and chair of the Institute for Information Infrastructure Protection (I3P) and full professor of human & organizational learning at The George Washington University. She is a globally recognized cybersecurity expert who currently co-chairs the ACM Joint Task Force on Cybersecurity Education. Dr. Burley was selected as the 2016 Woman of Influence-Public Sector/Academia by the Executive Women's Forum in Information Security, Risk Management and Privacy; and in 2014, she was named the Cybersecurity Educator of the Year and as one of the Top Ten Influencers in information security careers. In 2013, she served as co-Chair of the US National Research Council Committee on Professionalizing the Nation's Cybersecurity Workforce. Dr. Burley has written nearly 75 publications on cybersecurity, information sharing, and IT-enabled change.

Prior to joining GW, she managed a multi-million dollar computer science education and research portfolio and led the Cyber Corps program for the National Science Foundation. She is the sole recipient of both educator of the year and government leader of the year awards from the Colloquium for Information Systems Security Education and has been honored by the Federal CIO Council for her work on developing the federal cyber security workforce. She served two appointments on the Cyber Security Advisory Committee of the Virginia General Assembly Joint Commission on Technology & Science (2012, 2013) and has secured nearly $10 million in sponsored project support. Dr. Burley is a widely sought after speaker on cybersecurity workforce development, critical information infrastructure protection and the evolving cybersecurity landscape.

She holds a BA in Economics from the Catholic University of America; M.S. in Public Management and Policy, M.S. in Organization Science, and Ph.D. in Organization Science and Information Technology from Carnegie Mellon University where she studied as a Woodrow Wilson Foundation Fellow.

LinkedIn: http://www.linkedin.com/in/dianaburley
Twitter: @dianaburley

Chairwoman COMSTOCK. Thank you, Doctor.

And now we'll hear from Mr. Wilshusen.

TESTIMONY OF MR. GREGORY WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GAO

Mr. WILSHUSEN. Chairwoman Comstock, Ranking Member Lipinski, Mrs. Johnson, and Members of the Subcommittee, thank you for the opportunity to discuss ways to strengthen U.S. cybersecurity.

As recent cybersecurity attacks have illustrated, the need for robust and effective cybersecurity has never been greater. Today I will provide an overview of our work related to cybersecurity posture of the federal government and the nation's critical infrastructure.

At your request, I will also identify areas of consistency between our recommendations and those made in recent reports by the Commission on Enhancing National Cybersecurity and CSIS.

Before I do, if I may, I'd like to recognize for the record Mike Gilmore, Kush Malhotra, Nancy Glover, and Scott Pettis for their significant contributions to helping develop my written statement.

Madam Chairwoman, GAO has consistently identified shortcomings in the federal government's approach to protecting its computer systems. This year marks the 20th anniversary of GAO designating federal information security as a government-wide high-risk area. We expanded this area to include the protection of cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information, or PII, in 2015. Federal agencies in our nation's critical infrastructures are dependent upon computerized systems, networks and electronic data to carry out operations yet these systems and networks are inherently at risk and cyber threats continue to evolve and become more sophisticated. While agencies in previous Administrations have acted to improve the protections over systems supporting federal operations of critical infrastructure, the government needs to take additional actions to bolster U.S. cybersecurity. These include effectively implementing risk-based entity-wide information security programs consistently and over time improving its cyber incident detection, response and mitigation capabilities, enhancing its cybersecurity workforce planning and training efforts, expanding efforts to fortify cybersecurity of the nation's critical infrastructures, and better overseeing protection of personally identifiable information.

Over the last several years, GAO has made about 2,500 recommendations aimed at improving the security of federal systems and information. We have identified how agencies can tighten technical security controls, fully implement information security programs, and better protect the privacy of PII held on their systems. Many agencies continue to be challenged in safeguarding their computer systems and information, in part because many of these recommendations have not yet been implemented. As of January 2017, about 1,000 of our recommendations had not been implemented.

Regarding recommendations made by the Cybersecurity Commission and CSIS, several are generally consistent with or similar to previous GAO recommendations. In particular, certain recommendations pertaining to the establishing of an international cybersecurity strategy, protecting critical cyber infrastructure, promoting use of the NIST Cybersecurity Framework, prioritizing cyber research and expanding cybersecurity workforces share common traits.

In summary, the dependence upon the federal government and the national critical infrastructure on information and communications technologies makes them potentially vulnerable to a wide and evolving array of cyber-based threats. Securing these technologies is vital to the nation's security, prosperity and well-being. Nevertheless, the security over these systems is inconsistent and additional actions are needed to address ongoing cybersecurity and privacy challenges. We at GAO will continue to work with the Congress and federal agencies to address these challenges and strengthen our nation's cybersecurity capabilities.

Chairwoman Comstock, Ranking Member Lipinski, members of the Subcommittee, this concludes my statement, and I'd be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony

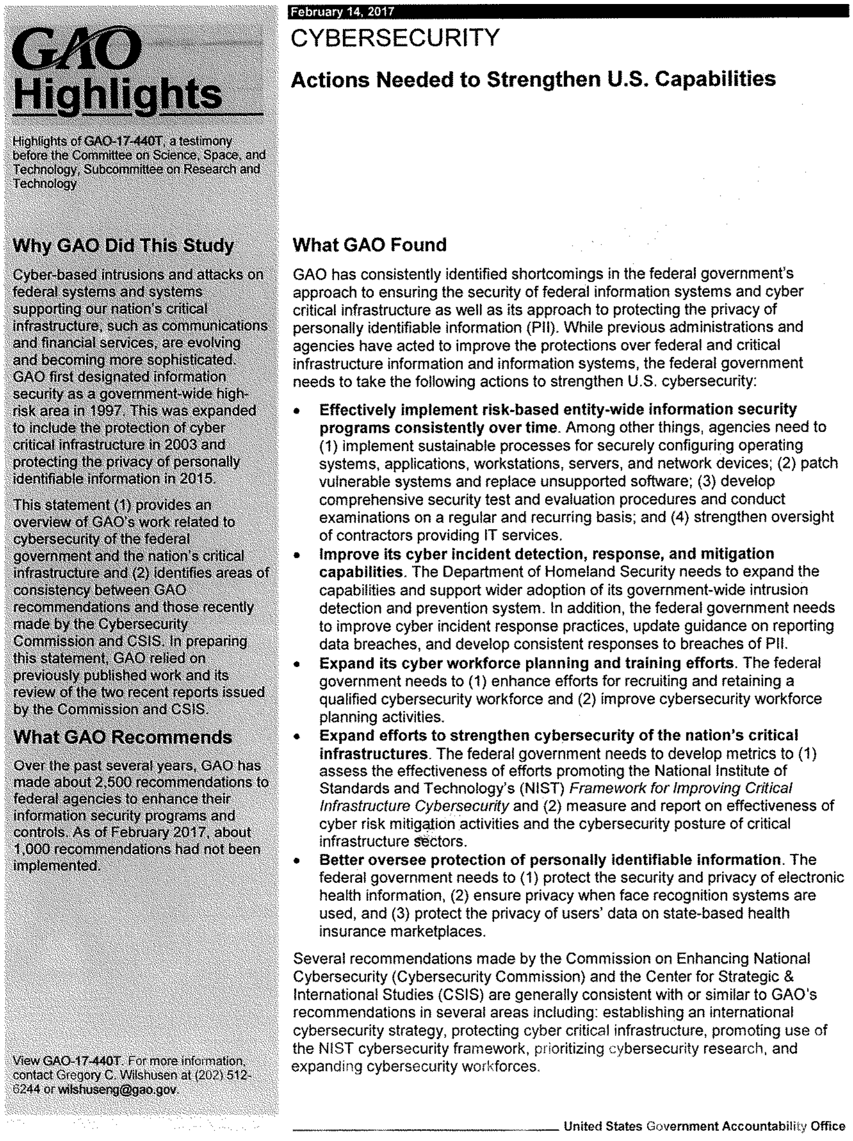
Before the Committee on Science, Space, and Technology, Subcommittee on Research and Technology

For Release on Delivery
Expected at 10 a.m EST
Tuesday, February 14, 2017

CYBERSECURITY

Actions Needed to Strengthen U.S. Capabilities

Statement of Gregory C. Wilshusen, Director,
Information Security Issues



GAO Highlights

Highlights of GAO-17-440T, a testimony before the Committee on Science, Space, and Technology, Subcommittee on Research and Technology

February 14, 2017

CYBERSECURITY

Actions Needed to Strengthen U.S. Capabilities

Why GAO Did This Study

Cyber-based intrusions and attacks on federal systems and systems supporting our nation's critical infrastructure, such as communications and financial services, are evolving and becoming more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include the protection of cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

This statement (1) provides an overview of GAO's work related to cybersecurity of the federal government and the nation's critical infrastructure and (2) identifies areas of consistency between GAO recommendations and those recently made by the Cybersecurity Commission and CSIS. In preparing this statement, GAO relied on previously published work and its review of the two recent reports issued by the Commission and CSIS.

What GAO Recommends

Over the past several years, GAO has made about 2,500 recommendations to federal agencies to enhance their information security programs and controls. As of February 2017, about 1,000 recommendations had not been implemented.

View GAO-17-440T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has consistently identified shortcomings in the federal government's approach to ensuring the security of federal information systems and cyber critical infrastructure as well as its approach to protecting the privacy of personally identifiable information (PII). While previous administrations and agencies have acted to improve the protections over federal and critical infrastructure information and information systems, the federal government needs to take the following actions to strengthen U.S. cybersecurity:

- **Effectively implement risk-based entity-wide information security programs consistently over time**. Among other things, agencies need to (1) implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices; (2) patch vulnerable systems and replace unsupported software; (3) develop comprehensive security test and evaluation procedures and conduct examinations on a regular and recurring basis; and (4) strengthen oversight of contractors providing IT services.
- **Improve its cyber incident detection, response, and mitigation capabilities**. The Department of Homeland Security needs to expand the capabilities and support wider adoption of its government-wide intrusion detection and prevention system. In addition, the federal government needs to improve cyber incident response practices, update guidance on reporting data breaches, and develop consistent responses to breaches of PII.
- **Expand its cyber workforce planning and training efforts**. The federal government needs to (1) enhance efforts for recruiting and retaining a qualified cybersecurity workforce and (2) improve cybersecurity workforce planning activities.
- **Expand efforts to strengthen cybersecurity of the nation's critical infrastructures**. The federal government needs to develop metrics to (1) assess the effectiveness of efforts promoting the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* and (2) measure and report on effectiveness of cyber risk mitigation activities and the cybersecurity posture of critical infrastructure sectors.
- **Better oversee protection of personally identifiable information**. The federal government needs to (1) protect the security and privacy of electronic health information, (2) ensure privacy when face recognition systems are used, and (3) protect the privacy of users' data on state-based health insurance marketplaces.

Several recommendations made by the Commission on Enhancing National Cybersecurity (Cybersecurity Commission) and the Center for Strategic & International Studies (CSIS) are generally consistent with or similar to GAO's recommendations in several areas including: establishing an international cybersecurity strategy, protecting cyber critical infrastructure, promoting use of the NIST cybersecurity framework, prioritizing cybersecurity research, and expanding cybersecurity workforces.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee:

Thank you for the opportunity to appear before you to discuss issues related to strengthening U.S. cybersecurity capabilities. As recent cyberattacks have illustrated, the need for robust and effective cybersecurity has never been greater.

Today, I will provide an overview of our work related to the cybersecurity posture of the federal government and the nation's critical infrastructure,[1] and federal efforts to protect the privacy of personally identifiable information (PII).[2] At your request, I will also identify areas of consistency between our cybersecurity-related recommendations and those made in recent reports by the President's Commission on Enhancing National Cybersecurity (Cybersecurity Commission)[3] and the Center for Strategic & International Studies (CSIS).[4]

My statement is based on our previously published work addressing cybersecurity efforts and our review of the two recent reports issued by the Cybersecurity Commission and CSIS. The GAO reports cited in this statement contain detailed discussions of the scope of the work and the methodology used to carry it out.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate

[1] Critical infrastructure includes systems and assets so vital to the United States that incapacitating or destroying them would have a debilitating effect on national security. Mostly owned and operated by the private sector, these critical infrastructures are grouped by the following industries or "sectors": chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology (IT); nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[2] PII is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

[3] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy* (December 1, 2016).

[4] Center for Strategic & International Studies, *From Awareness to Action: A Cybersecurity Agenda for the 45th President* (Washington, D.C.: January 2017).

evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Federal agencies and our nation's critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective controls could have a significant impact on a broad array of government operations and assets. For example,

- resources, such as payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes, including the launching of attacks on others;
- sensitive information, such as intellectual property, national security data, and PII such as taxpayer data, Social Security records, and medical records could be inappropriately added, deleted, read, copied, disclosed, or modified for purposes such as espionage, identity theft, or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- entity missions could be undermined by embarrassing incidents that result in diminished confidence in the entity's ability to conduct operations and fulfill its responsibilities.

Federal information systems and networks are inherently at risk. They are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the myriad of operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. For example, the national vulnerability database maintained by the National Institute of Standards and Technology (NIST) has identified 82,384 publicly known cybersecurity vulnerabilities and exposures as of February 9, 2017, with more being added each day.[5] Federal systems and networks are also often interconnected with other internal and external systems and networks including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface.

In addition, cyber threats to systems supporting the federal government and critical infrastructure are evolving and becoming more sophisticated. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, foreign nations—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks.

Risks to cyber assets can originate from unintentional and intentional threats. These include insider threats from disaffected or careless employees and business partners, escalating and emerging threats from around the globe, the steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks. Ineffectively protecting cyber assets can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security, economic well-being, and public health and safety.

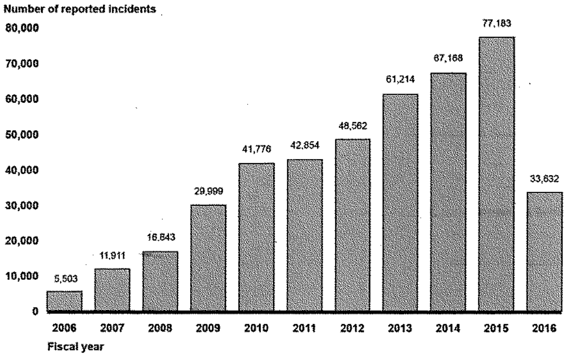
Until fiscal year 2016, the number of information security incidents reported by federal agencies to the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT)[6] had steadily increased each year. From fiscal year 2006 through fiscal year 2015, reported security incidents increased from 5,503 to 77,183, an increase of 1,303 percent. However, the number of reported incidents

[5] The national vulnerability database is the U.S. government repository of standards based vulnerability management data. The database includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

[6] US-CERT, a branch of DHS's National Cybersecurity and Communications Integration Center, is a central Federal information security incident center that compiles and analyzes information about incidents that threaten information security. Federal agencies are required to report such incidents to US-CERT.

decreased by 56 percent in fiscal year 2016 to 33,632, as shown in figure 1.

Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2016



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2016.

An official from DHS's National Cybersecurity and Communications Integration Center stated that the decrease in reported incidents for fiscal year 2016 was likely due to revised incident reporting requirements that no longer require agencies to report non-cyber incidents or attempted scans or probes of agency networks. The official also cited the expanded use of the National Cybersecurity Protection System[7] to detect or block potentially malicious network traffic entering networks at federal agencies as another possible reason for fewer reported incidents.

Safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—has been a long-standing concern. GAO first designated

[7] The National Cybersecurity Protection System is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing. See GAO-16-294 for results of GAO's review of this system.

information security as a government-wide high-risk area[8] in 1997; it then expanded this high risk area to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of PII in 2015.[9]

Over the last several years, GAO has made about 2,500 recommendations to agencies aimed at improving the security of federal systems and information. These recommendations identified actions for agencies to take to strengthen technical security controls over their computer networks and systems. They also include recommendations for agencies to fully implement aspects of their information security programs, as mandated by the *Federal Information Security Modernization Act* (FISMA) of 2014 and its predecessor, the *Federal Information Security Management Act of 2002*,[10] as well as to protect the privacy of PII held on their systems. Nevertheless, many agencies continue to be challenged in safeguarding their information systems and information, in part because many of these recommendations have not been implemented. As of February 2017, about 1,000 of our information security-related recommendations had not been implemented.

Action Is Needed to Address Ongoing Cybersecurity and Privacy Challenges

Our work has identified the need for improvements in the federal government's approach to cybersecurity of its systems and those supporting the nation's critical infrastructures and in protecting the privacy of PII. While previous administrations and agencies have acted to improve the protections over the information and information systems supporting federal operations and U.S. critical infrastructure, additional actions are needed.

Federal agencies need to effectively implement risk-based entity-wide information security programs consistently over time. Since the first FISMA was enacted in 2002, agencies have been challenged to fully

[8] GAO designates agencies and program areas as high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or when they are most in need of transformation.

[9] See GAO, *High-Risk List: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[10] The *Federal Information Security Modernization Act of 2014* (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, Dec. 17, 2002). As used here, FISMA refers both to FISMA 2014 and those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

and effectively develop, document, and implement the entity-wide information security program required by FISMA to protect the information and information systems that support their operations and assets, including those provided or managed by another agency or contractor. For example, as of February 7, 2017, 19 of 23 federal agencies covered by the *Chief Financial Officers Act* (CFO Act)[11] that had issued their required annual financial reports for fiscal year 2016[12] reported that information security control deficiencies were either a material weakness or significant deficiency[13] in internal controls over financial reporting for fiscal year 2016. In addition, inspectors general at 20 of the 23 agencies identified information security as a major management challenge for their agencies.

Further, in light of these challenges, we have identified a number of actions to assist agencies in implementing their information security programs.

- *Enhance capabilities to effectively identify cyber threats to agency systems and information.* A key activity for assessing cybersecurity risk and selecting appropriate mitigating controls is the identification of cyber threats to computer networks, systems, and information. In 2016, we reported on several factors that agencies identified as impairing their ability to identify these threats to a great or moderate extent. The impairments included an inability to recruit and retain

[11] Twenty-four agencies are covered by the CFO Act: Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management (OPM); Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[12] As February 7, 2017, 23 of the 24 CFO Act agencies had issued their annual financial report for fiscal year 2016. The Department of Defense has not issued its annual financial report for fiscal year 2016.

[13] A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a deficiency, or combination of deficiencies, in internal that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

personnel with the appropriate skills, rapidly changing threats, continuous changes in technology, and a lack of government-wide information sharing mechanisms.[14] Addressing these impairments will enhance the ability of agencies to identify the threats to their systems and information and be in a better position to select and implement appropriate countermeasures.

- *Implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices.* We routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations, servers, and network devices. Agencies were not always aware of the insecure settings that introduced risk to the computing environment. Establishing strong configuration standards and implementing sustainable processes for monitoring and enabling configuration settings will strengthen the security posture of federal agencies.
- *Patch vulnerable systems and replace unsupported software.* Federal agencies consistently fail to apply critical security patches on their systems in a timely manner, sometimes doing so years after the patch becomes available. We also consistently identify instances where agencies use software that is no longer supported by their vendors. These shortcomings often place agency systems and information at significant risk of compromise, since many successful cyberattacks exploit known vulnerabilities associated with software products. Using vendor-supported and patched software will help to reduce this risk.
- *Develop comprehensive security test and evaluation procedures and conduct examinations on a regular and recurring basis.* Federal agencies we reviewed often did not test or evaluate their information security controls in a comprehensive manner. The evaluations were sometimes based on interviews and document reviews, limited in scope, and did not identify many of the security vulnerabilities that our examinations identified. Conducting in-depth security evaluations that examine the effectiveness of security processes and technical controls is essential for effectively identifying system vulnerabilities that place agency systems and information at risk.
- *Strengthen oversight of contractors providing IT services.* As demonstrated by the OPM data breach of 2015, cyber attackers can sometimes gain entry to agency systems and information through the

[14] GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

agency's contractors or business partners. Accordingly, agencies need to assure that their contractors and partners are adequately protecting the agency's information and systems. In August 2014, we reported that five of six selected agencies were inconsistent in overseeing the execution and review of security assessments that were intended to determine the effectiveness of contractor implementation of security controls, resulting in security lapses.[15] In 2016, agency chief information security officers (CISOs) we surveyed reported that they were challenged to a large or moderate extent in overseeing their IT contractors and receiving security data from the contractors. This challenge diminished their ability to assess how well agency information maintained by the contractors is protected.[16] Effectively overseeing and reviewing the security controls implemented by contractors and other parties is essential to ensuring that the agency's information is properly safeguarded.

We have several ongoing and planned audit engagements that will continue to assess the effectiveness of agency actions to implement information security programs. These engagements include in-depth assessments of information security programs at individual agencies including OPM and the Centers for Disease Control and Prevention as well as our biennial review of the adequacy of agencies' information security policies and practices and their compliance with the provisions of FISMA.

Also, on an annual basis, we evaluate information security controls over financial systems and information at seven agencies and incorporate the audit results of agency offices of inspector general during our annual audit of the consolidated financial statements of the federal government. In addition, we are currently conducting an assessment of the Federal Risk Authorization and Management Program and have plans to review cyber risk management practices and continuous monitoring programs at federal agencies.

The federal government needs to improve its cyber incident detection, response, and mitigation capabilities. Even agencies or organizations with strong security can fall victim to information security

[15] GAO, Information Security: Agencies Need to Improve Oversight of Contractor Controls, GAO-14-612, (Washington, D.C.: Aug. 8, 2014).

[16] GAO, Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

incidents due to the existence of previously unknown vulnerabilities that are exploited by attackers to intrude into an agency's information systems. Accordingly, agencies need to have effective mechanisms for detecting, responding to, and recovering from such incidents. We have previously identified various actions that could assist the federal government in building its capabilities for detecting, responding to, and recovering from security incidents.

- *Expand capabilities, improve planning, and support wider adoption of the government-wide intrusion detection and prevention system.* In January 2016, we reported that DHS's National Cybersecurity Protection System (NCPS) had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information. In addition, adoption of these capabilities at federal agencies was limited. We noted that expanding NCPS's capabilities for detecting and preventing malicious traffic, defining requirements for future capabilities, and developing network routing guidance could increase assurance of the system's effectiveness in detecting and preventing computer intrusions and support wider adoption by agencies.[17]
- *Improve cyber incident response practices at federal agencies.* In April 2014 we reported that 24 major federal agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[18] For example, six agencies reviewed had not determined the impact of incidents or taken actions to address the underlying control weaknesses that allowed the incidents to occur, in part because they had not developed comprehensive policies, plans, and procedures for responding to security incidents, and had not tested their incident response capabilities. By developing comprehensive incident response policies, plans, and procedures for responding to incidents and effectively overseeing response activities, agencies will have increased assurance that they will effectively respond to cyber incidents.
- *Update federal guidance on reporting data breaches and develop consistent responses to breaches of PII.* As we reported in December 2013, eight agencies that we reviewed did not consistently implement

[17] GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System,* GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

[18] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices,* GAO-14-354 (Washington, D.C.: April 30, 2014).

policies and procedures for responding to breaches of PII.[19] For example, none of the agencies had documented the evaluation of incidents and lessons learned. In addition, we noted that OMB guidance calling for agencies to report each PII-related incident—even those with inherently low risk to the individuals affected—within 1 hour of discovery may cause agencies to expend resources to meet reporting requirements that provide little value and divert time and attention from responding to breaches. We recommended that OMB update it guidance on federal agencies' responses to a PII-related data breach and that the agencies we reviewed take steps to improve their response to data breaches involving PII. Updating guidance and consistently implementing breach response practices will improve the effectiveness of governmentwide and agency data breach response programs.

GAO routinely evaluates agencies' intrusion detection, response, and mitigation activities during audits of agency information security controls and programs. We plan to continue to do so during ongoing and future engagements. In addition, the *Cybersecurity Act of 2015*[20] contains a provision for us to study and publish a report by December 2018 on the effectiveness of the approach and strategy of the federal government to secure agency information systems, including the intrusion detection and prevention capabilities and the government's intrusion assessment plan.

The federal government needs to expand its cyber workforce planning and training efforts. Ensuring that the government has a sufficient number of cybersecurity professionals with the right skills and that its overall workforce is aware of information security responsibilities remains an ongoing challenge.

- *Enhance efforts for recruiting and retaining a qualified cybersecurity workforce.* This has been a long-standing dilemma for the federal government. In 2013, agency chief information officers and experts we surveyed cited weaknesses in education, awareness, and workforce planning as a root cause in hindering improvements in the

[19] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

[20] *The Cybersecurity Act of 2015* was enacted as *Division N of the Consolidated Appropriations Act, 2016*, Pub. L. No. 114-113, Dec. 18, 2015.

nation's cybersecurity posture.[21] Several experts also noted that the cybersecurity workforce was inadequate, both in numbers and training. They cited challenges such as the lack of role-based qualification standards and difficulties in retaining cyber professionals. In 2016, agency chief information security officers we surveyed cited difficulties related to having sufficient staff; recruiting, hiring, and retaining security personnel; and ensuring that security personnel have appropriate skills and expertise as posing challenges to their abilities to carry out their responsibilities effectively.[22]

- *Improve cybersecurity workforce planning activities at federal agencies.* In November 2011, we reported that only five of eight selected agencies had developed workforce plans that addressed cybersecurity.[23] Further, all eight agencies reported challenges with filling cybersecurity positions, and only three of the eight had a department-wide training program for their cybersecurity workforce.

GAO has two current engagements to further review cybersecurity workforce issues in the federal government. T*he Homeland Security Cybersecurity Workforce Assessment Act of 2014*[24] contains a provision for us to monitor, analyze, and report by December 2017 on the Department of Homeland Security's implementation of the National Cybersecurity Workforce Measurement Initiative. In addition, the *Cybersecurity Act of 2015* calls for us to monitor, analyze, and submit a report by December 2018 on the implementation of this initiative and the identification of cyber-related work roles of critical need by federal agencies.

The federal government needs to expand efforts to strengthen cybersecurity of the nation's critical infrastructures. U.S. critical infrastructures such as financial institutions, energy production and transmission facilities, and communications networks, are vital to the U.S. security, economy, and public health and safety. Similar to federal

[21] GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb 14, 2013).

[22] GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

[23] GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

[24] *Homeland Security Cybersecurity Workforce Assessment Act of 2014*, Pub. L. No. 113-277, (Dec. 18, 2014).

systems, the systems supporting critical infrastructures face an evolving array of cyber-based threats. To help secure infrastructure cyber assets—most of which is owned and operated by the private sector—federal policy and the *National Infrastructure Protection Plan*[25] provide for a public-private partnership in which federal agencies support or assist their private sector partners in securing systems supporting critical infrastructure. We have identified the following actions that can assist agencies in performing these vital services.

- *Develop metrics to assess the effectiveness of efforts promoting the NIST cybersecurity framework.* In December 2015, we reported that NIST and other agencies had promoted the adoption of the *Framework for Improving Critical Infrastructure Cybersecurity* to critical infrastructure owners and operators and other organizations.[26] Toward this end, DHS established the Critical Infrastructure Cyber Community Voluntary Program to encourage entities to adopt the framework. However, DHS had not developed metrics to measure the success of its activities and programs. In addition, DHS and the General Services Administration had not determined whether to develop tailored guidance for implementing the framework in government facilities sector as other agencies had done for their respective sectors. DHS concurred with our recommendation to develop metrics, but has not indicated that it has taken action, and DHS and the General Services Administration concurred with our recommendation to determine whether tailored guidance was needed.
- *Develop metrics to measure and report on the effectiveness of cyber risk mitigation activities and the cybersecurity posture of critical infrastructure sectors.* In November 2015, we reported that all eight sector-specific agencies reviewed had determined the significance of cyber risk to the nation's critical infrastructures and had taken actions to mitigate cyber risks and vulnerabilities for their respective sectors.[27] However, not all sector-specific agencies had metrics to measure and report on the effectiveness of all their activities to mitigate cyber risks

[25] DHS, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, (December 2013).

[26] GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015).

[27] GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

or their sectors' cybersecurity posture. We recommended that agencies lacking metrics develop them and determine how to overcome any challenges to reporting the results of their activities to mitigate cyber risks. Four of the agencies explicitly agreed with our recommendations and identified planned or on-going efforts to implement performance metrics; however, they have not yet provided metrics or reports of outcomes.

GAO has several ongoing and planned engagements that will touch on the cybersecurity of national critical infrastructures. Among these engagements, our study of the "Internet of things" addresses the security and privacy implications of this phenomenon. In addition, the *Cybersecurity Enhancement Act of 2014*[28] contains a provision for us to assess the extent to which critical infrastructure sectors have adopted a voluntary cybersecurity framework to reduce cyber risks and the success of such a framework for protecting critical infrastructure against cyber threats. We also plan to review the cybersecurity of oil and gas pipeline control systems and the Department of Homeland Security's efforts to share cyber information with federal and non-federal entities.

The federal government needs to better oversee protection of PII. Regarding PII, advancements in technology, such as new search technology and data analytics software for searching and collecting information, have made it easier for individuals and organizations to correlate data and track it across large and numerous databases. In addition, lower data storage costs have made it less expensive to store vast amounts of data. Also, ubiquitous Internet and cellular connectivity make it easier to track individuals by allowing easy access to information pinpointing their locations. These advances—combined with the increasing sophistication of hackers and others with malicious intent, and the extent to which both federal agencies and private companies collect sensitive information about individuals—have increased the risk of PII being exposed and compromised. Our work has identified the following actions that need to be taken to better protect the privacy of personal information.

- *Protect the security and privacy of electronic health information.* In August 2016, we reported that guidance for securing electronic health information issued by Department of Health and Human Services (HHS) did not address all key controls called for by other federal

[28] *Cybersecurity Enhancement Act of 2014,* Pub. L. No. 113-274, (Dec. 18, 2014).

cybersecurity guidance.[29] In addition, this department's oversight efforts did not always offer pertinent technical guidance and did not always follow up on corrective actions when investigative cases were closed. HHS generally concurred with the five recommendations we made and stated that it would take actions to implement them.

- *Ensure privacy when face recognition systems are used.* In May 2016, we reported[30] that the Department of Justice had not been timely in publishing and updating privacy documentation for the Federal Bureau of Investigation's (FBI) use of face recognition technology.[31] Publishing such documents in a timely manner would better assure the public that the FBI is evaluating risks to privacy when implementing systems. Also, the FBI had taken limited steps to determine whether the face recognition system it was using was sufficiently accurate. We recommended that the department ensure required privacy-related documents are published and that the FBI test and review face recognition systems to ensure that they are sufficiently accurate. Of the six recommendations we made, the Department of Justice agreed with one, partially agreed with two, and disagreed with three. The agency has not yet provided information about the actions it has taken to address the recommendations.
- *Protect the privacy of users' data on state-based marketplaces.* In March 2016, we reported on weaknesses in technical controls for the "data hub" that the Centers for Medicare and Medicaid Services (CMS) uses to exchange information between its health insurance marketplace and external partners.[32] We also identified significant weaknesses in the controls in place at three selected state-based

[29] GAO, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight*, GAO-16-771 (Washington, D.C.: Aug. 26, 2016).

[30] GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016).

[31] Face recognition technology uses biometrics—the automated recognition of individuals based on their biological and behavioral characteristics—to identify the identity of individuals based on a comparison of a photograph of an unknown person against a database of photographs of known persons. Specifically, the technology extracts features from the faces and puts them into a format—often referred to as a faceprint—that can be used for verification, among other things. Once the faceprint has been created, the technology can use a face recognition algorithm to compare the faceprints against each other to produce a single score value that represents the degree of similarity between the two faces.

[32] GAO, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls*, GAO-16-265 (Washington, D.C.: Mar. 23, 2016).

marketplaces established to carry out provisions of the *Patient Protection and Affordable Care Act*.[33] We recommended that CMS define procedures for overseeing the security of state-based marketplaces and require continuous monitoring of state marketplace controls. HHS concurred with our recommendations and stated it has taken or plans to take actions to address these recommendations.

GAO has several ongoing and planned reviews that address actions intended to protect the privacy of PII. For example, we are assessing agency efforts and government-wide initiatives to reduce or eliminate the use of Social Security numbers. In addition, the *Cybersecurity Act of 2015* calls for us to review and report by December 2018 on agency policies and actions taken by the federal government to remove PII from shared cyber threat indicators or defensive measures. Further, the *21st Century Cures Act of 2016* requires us to review and report by December 2018 on the policies and activities of the Office of the National Coordinator for Health Information Technology to ensure appropriate matching to protect patient privacy and security with respect to electronic health records.[34]

Several Recommendations Made by the Cybersecurity Commission and CSIS Are Generally Consistent with GAO's Recommendations for Improving Cybersecurity

Recent reports by the Cybersecurity Commission and CSIS identify topical areas and numerous recommendations for the new administration to consider as it develops and implements cybersecurity strategy and policy. In its study, the Commission focused on 10 cybersecurity topics including international issues, critical infrastructure, cybersecurity research and development, cybersecurity workforce, and the Internet of Things. CSIS addressed similar topics and identified five major issues related to international strategy, securing government agencies and critical infrastructure, cybersecurity research and workforce development, cybercrime, and defending cyberspace.

Over the last several years, GAO has reviewed many of the areas covered by the Commission and CSIS reports. Our conclusions and recommendations are generally directed to specific agencies and may be more limited in scope than the recommendations of the Commission and CSIS. Nevertheless, several of our recommendations are generally

[33] Pub. L. No. 111-148, 124 Stat. 119 (Mar. 23, 2010), as amended by the *Health Care and Education Reconciliation Act of 2010*, Pub. L. No. 111-152,124 Stat.1029 (Mar. 30, 2010).

[34] *21st Century Cures Act of 2016*, Pub L. No. 114-255, Div. A, Title IV, Sec. 4007 (December 13, 2016).

consistent with or similar to recommendations made by the Commission and CSIS in the following areas:

- *International cybersecurity strategy.* In July 2010, we identified a number of challenges confronting U.S. involvement in global cybersecurity and governance.[35] These include developing a comprehensive national strategy; ensuring international standards and policies do not pose unnecessary barriers to U.S. trade; participating in international cyber-incident response and appropriately sharing information without jeopardizing national security; investigating and prosecuting transnational cybercrime; and contending with differing laws and norms of behavior. We made five recommendations to the administration's cybersecurity coordinator to address these challenges, to include developing a comprehensive national global cyberspace strategy and defining cyberspace norms. In their recent reports, the Commission and CSIS also identified actions for enhancing international cybersecurity strategy and policies and agreeing on norms of behavior with like-minded nations.
- *Protecting cyber critical infrastructure.* In November 2015, we reported that sector specific agencies—federal agencies that are responsible for collaborating with their private sector counterparts in their assigned critical infrastructure sectors—were acting to address sector cyber risk by sharing information, supporting incident response activities, and providing technical assistance. However, they had not developed metrics to measure and improve the effectiveness of their cyber risk mitigation activities or their sectors' cybersecurity posture.[36] We recommended that the agencies develop performance metrics to monitor and improve the effectiveness of their cyber risk mitigation activities. In their recent reports, the Commission and CSIS also identified actions for enhancing the public-private partnership, including improving information sharing, incident response capabilities, and cyber risk management practices.
- *Promoting Use of the NIST Cybersecurity Framework.* In December 2015, we reported that NIST had developed a set of voluntary standards and procedures for enhancing cybersecurity of critical infrastructure, known as the *Framework for Improving Critical*

[35] GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

[36] GAO, Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress, GAO-16-79, (Washington, D.C.: Nov. 19, 2015).

Infrastructure Cybersecurity. We also reported that although DHS had established a program dedicated to encouraging the framework's adoption, it had not established metrics to assess the effectiveness of these efforts. We recommended that DHS develop metrics for measuring the effectiveness of efforts to promote and support the framework. Similarly, both the Commission and CSIS have recommended actions to promote and measure use of the framework.

- *Prioritizing cybersecurity research and development (R&D).* In June 2010, we reported that the federal government lacked a prioritized national R&D agenda and a data repository to track research and development projects and funding, as required by law.[37] We recommended that the Office of Science and Technology Policy (OSTP) take several steps, including developing a comprehensive national R&D agenda that identifies priorities for short-term, mid-term, and long-term complex R&D projects and is guided by input from the public and private sectors. Similarly, in its report, the Commission stated that OSTP, as part of an overall R&D agenda, should lead the development of an integrated government-private-sector cybersecurity roadmap for developing defensible systems.
- *Expanding cybersecurity workforce capabilities.* As discussed earlier in this statement, we have reported that ensuring that the government has a sufficient number of cybersecurity professionals with the right skills and that its overall workforce is aware of information security responsibilities remains an ongoing challenge. Consistent with this view, the Commission and CSIS have identified actions to address improving the nation's cybersecurity workforce, including increasing the number of cybersecurity practitioners; implementing a range of education and training programs at the federal, state, and local levels; providing incentives for individuals to enter the workforce; and allocating additional funds at key departments for cybersecurity education and training programs.
- *Combatting cybercrime.* In June 2007, we identified a number of challenges impeding public and private entities efforts in mitigating cybercrime, including working in a borderless environment[38] with laws

[37] GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development*, GAO-10-466 (Washington, D.C.: June 3, 2010).

[38] Cybercriminals are not hampered by physical proximity or borders. Cybercriminals can be physically located in one nation or state, direct their crime through computers in multiple nations or states, and store evidence of the crime on computers in yet another nation or state.

of multiple jurisdictions.[39] We stated that efforts to investigate and prosecute cybercrime are complicated by the multiplicity of laws and procedures that govern in the various nations and states where victims may be found, and the conflicting priorities and varying degrees of expertise of law enforcement authorities in those jurisdictions. In addition, laws used to address cybercrime differ across states and nations. For example, an act that is illegal in the United States may be legal in another nation or not directly addressed in the other nation's laws. Developing countries, for example, may lack cybercrime laws and enforcement procedures. In its recent report, CSIS stated that many countries still do not have adequate cybercrime laws and recommended that (1) countries that refuse to cooperate with law enforcement should be penalized in some way and (2) methods be found to address the concerns of countries not willing to sign an existing treaty addressing cybercrime.

In summary, the dependence of the federal government and the nation's critical infrastructure on computerized information systems and electronic data makes them potentially vulnerable to a wide and evolving array of cyber-based threats. Securing these systems and data is vital to the nation's security, prosperity, and well-being. Nevertheless, the security over these systems is inconsistent and additional actions are needed to address ongoing cybersecurity and privacy challenges. Specifically, federal agencies need to address control deficiencies and fully implement organization-wide information security programs, cyber incident response and mitigation efforts needs to be improved across the government, maintaining a qualified cybersecurity workforce needs to be a priority, efforts to bolster the cybersecurity of the nation's critical infrastructure needs to be strengthened, and the privacy of PII needs to be better protected. Several recommendations made by the Commission and CSIS are generally consistent with previous recommendations made by GAO and warrant close consideration.

Chairwoman Comstock, Ranking Member Lipinski, and Members of the Subcommittee, this concludes my statement. I would be happy to respond to your questions.

[39] GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Michael Gilmore, Nancy Glover, and Kush Malhotra.

Related GAO Products

GAO, *Cybersecurity: DHS's National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely*, GAO-17-163 (Washington, D.C.: Feb. 1, 2017).

GAO, *Federal Information Security: Actions Needed to Address Challenges*, GAO-16-885T (Washington, D.C.: Sept. 19, 2016).

GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686. (Washington, D.C.: Aug. 26, 2016).

GAO, *Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight*, GAO-16-771 (Washington, D.C.: Aug. 26, 2016).

GAO, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, GAO-16-267 (Washington, D.C.: May 16, 2016) (Reissued August 3, 2016).

GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

GAO, *Healthcare.gov: Actions Needed to Enhance Information Security and Privacy Controls*, GAO-16-265 (Washington, D.C.: Mar. 23, 2016).

GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

GAO, *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, GAO-16-152 (Washington, D.C.: Dec. 17, 2015).

GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79, (Washington, D.C.: Nov. 19, 2015).

GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010).

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.

Biography

Gregory Wilshusen is Director of Information Security Issues at GAO, where he leads cybersecurity and privacy-related studies and audits of the federal government and critical infrastructure. He has over 30 years of auditing, financial management, and information systems experience. Prior to joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions. He was a senior systems analyst at the Department of Education. He also served as the Controller for the North Carolina Department of Environment, Health, and Natural Resources, and held senior auditing positions at Irving Burton Associates, Inc. and the U.S. Army Audit Agency. He's a certified public accountant, certified internal auditor, and certified information systems auditor. He holds a B.S. degree in business administration (accounting) from the University of Missouri and an M.S. in information management from George Washington University's School of Engineering and Applied Sciences.

Chairwoman COMSTOCK. Thank you.

I'll now yield myself five minutes, and I appreciate the witnesses' testimony.

Mr. Wilshusen, as you noted, 1,000 of the recommendations have not been implemented. That's about 40 percent. What are some of the most common reasons for that lack of implementation, and what steps might Congress take to help encourage agencies to implement these recommendations?

Mr. WILSHUSEN. Well, I think the recommendations in some instances require a longer period of time to actually implement consistently throughout the organization, and that may be one factor. Another factor is that agencies often will close a recommendation as implemented when they may have a plan to implement the recommendations and not when they take the action needed to implement the recommendation across the enterprise. We often find that when we go back to an agency that has indicated that it has implemented the recs. We go out and re-test the systems across the organization, the conditions still exist. They may have implemented it on a couple of the systems but not throughout the organization. So that's another factor.

Chairwoman COMSTOCK. Should there be some self-testing then on that so you have your plan and then you have tests that each agency is doing on their own, or do you have recommended policies on that front?

Mr. WILSHUSEN. Right, most definitely. In fact, FISMA requires agencies to test and evaluate the security of their systems frequently, at least once a year, to assure that their controls are adequately implemented, but——

Chairwoman COMSTOCK. But that is not being done?

Mr. WILSHUSEN. Well, it may be done but we have also found that agencies' security tests and evaluation processes may not be that comprehensive. In some cases, they may rely on interviews or document reviews but not dig down to look to see how systems and their settings are actually configured. That's vital with information security because so many controls, particularly the technical security controls, are implemented in the systems that have to be configured in a certain way. So that's one of the key areas that we consistently find as a reason for these outstanding recommendations.

Chairwoman COMSTOCK. Thank you.

And Dr. Burley, I really appreciate your focus on the need for education, and 1.5 million jobs you said are needed?

Dr. BURLEY. Yes.

Chairwoman COMSTOCK. And so that certainly is a good growth area that people should be focused on, appreciate GW's focus on that and many of our universities in the region.

What type of practices even earlier on can get people into the pipeline? To get young students in this can we be focusing on really in earlier grades to make this really be kind of a lifestyle and understanding that this is something that everybody needs to be engaged in?

Dr. BURLEY. I think that there are two different approaches that we can take. One is certainly getting students into the technology areas earlier - so teaching them how to code and to understand what that means. Moving computer science down into the K-12 classrooms is critical. But we also need to focus on more general skills like analytical ability, critical thinking, communication, those types of skills, teamwork, team building. All of those different skill sets are critical for cybersecurity professionals and so we need to consider those as well.

Chairwoman COMSTOCK. And even for people who aren't going into that field, I mean, obviously, with 1.5 million jobs needed, that is a good field for them to go into, but what type of—should there be classes maybe in grades for qualification for just basic understanding for people even who aren't in the field?

Dr. BURLEY. Absolutely. So you're talking about awareness programs?

Chairwoman COMSTOCK. Yes.

Dr. BURLEY. We certainly need to make sure that everyone understands what cybersecurity is, and what role they play as individuals in that workforce. Not all of the cybersecurity careers are solely focused on only doing cybersecurity. There are a lot of what we consider to be hybrid roles so that if someone is going into healthcare, they may have an opportunity to work with electronic medical records or need to understand privacy considerations and so it is very important that the awareness programs aren't just general blanket broad awareness programs but that they also contain elements that specifically link cybersecurity concepts and ideas to all of the disciplines across the curriculum as early as we possibly can do it.

Chairwoman COMSTOCK. So it sounds like we need something akin to a continuing education program for everybody in various fields on the need to be aware of this, and Mr. Mulholland, I noticed you're nodding too. If you wanted to——

Mr. MULHOLLAND. Yeah, if I could just add to that, you know, as someone who hires and over the last 20 years has hired many, many security engineers, certainly I would support, you know, enhancement of skills. We find it incredibly difficult to hire well-qualified security engineers, but also more broadly in some of the software security programs that we run, I end up spending a lot of time just teaching known security software developers about security. I would love to see basic security skills to be part of every computer science degree, you know, in the curriculum moving forward so I can invest my time in being proactive and defending rather than having to teach all of my known security colleagues about the basics of security.

Chairwoman COMSTOCK. Excellent. Thank you all, and I now yield to Mr. Lipinski for five minutes.

Mr. LIPINSKI. I want to thank you all for your testimony, and just very briefly, education, workforce. Dr. Burley, you were speaking about that. I just want to say that as Co-Chair of the STEM Ed Caucus, I think there's more that we need to be doing to encourage STEM education. Next week is National Engineers Week. I know one of those days is Introduce a Girl to Engineering Day and there's a lunch up here tomorrow about that. We need to get as many people as we can into the pipeline. And also, we need to have general education on things like cyber hygiene.

I wanted to—there's so many things we could talk about. I have some questions for the record. But I wanted to ask Mr. Mulholland, you had spoken a little bit about the internet of things and what needs to—you started touching on what needs to be done. Both the Commission and the CSIS focused on security of IOT devices, and in his testimony, Dr. Romine discussed the steps NIST is already taking to address security for IOT in different sectors.

Now, I assume that the CSIS task force took into account the efforts already underway at NIST to develop security standards. Would you have any thoughts on how NIST should prioritize their IOT work in the next couple years given limited resources?

Mr. MULHOLLAND. You know, I think all of us in the CSIS cyber task force felt that IOT is really critical in terms of priorities. The speed and acceleration of things is quite phenomenal, and the spectrum that they cover is quite considerable. If you look at, you know, IOT as a concept, it is not necessarily new. We've had industrial control systems for a very long time in the power and the energy sectors but if you look at—you know, I'm wearing a watch today that's probably as powerful as my iPhone was ten years ago—the proliferation of these devices is critical, and I think NIST's involvement in setting some basic rules of the road are going to be critical, particularly actually in the consumer segment around how these devices are actually manufactured and supported over the lifecycle of those.

Mr. LIPINSKI. Anything—nothing more specific on where you would direct NIST to go?

Mr. MULHOLLAND. I think that there are a couple of specific areas. I think first of all, you need to look at it from a sector-specific point of view. If you look at industrial control systems, for example, or healthcare advices or manufacturing, certainly I think some of the work NIST has already done should be accelerated around how do we actually connect these systems through things like internet gateways and edge-type devices, what are, you know, appropriate architectures and controls for those.

But I think the other area that can't be forgotten is the consumer side. If we look at the attacks in October last year, that was predominantly consumer devices where there really aren't any standards or any recommendations around how a consumer device should be developed or, you know, some basic kind of frameworks for how it should be supported over its lifecycle. If we don't look at that full spectrum, you know, much more prescriptive around, you know, more kind of manufacturing, industrial, but also a consumer, then we're going to continue to see attacks like that.

Mr. LIPINSKI. Thank you. And since we're going down that road, let me finish with a question about privacy.

Last week, Vizeo agreed to pay $2.2 million settlement for charges that TVs collected owners' information without their knowledge. We have devices like Amazon Echo, Google Home, all these listening devices that are proliferating. We have facial recognition technologies that are getting better and better. So the issue of privacy, cybersecurity, privacy is also very important. Are there any recommendations that any of you have for how the Science Committee or Congress in general should thoughtfully address both the cybersecurity and privacy issues and balancing them?

Mr. MULHOLLAND. So certainly at CSIS, we made a set of recommendations again specifically around the definition of PII and some recommendations that NIST should revisit the definition both on kind of reestablishing a baseline but also on an ongoing basis. I think what is considered PII historically is rapidly, rapidly evolving. One of the things that we discussed quite a lot about was that five years ago, none of us would have considered that we'd have a device in our pocket that is tracking every move or we might have a television that's listening to our every conversation, and you know, the data that those devices create does not necessarily fit under the traditional definition of PII. So we had a recommendation that NIST should specifically look at what the definition of PII is but see that as a moving target that needs to be so that we can set some acceptable norms around, you know, privacy and private information.

Mr. LIPINSKI. All right. Thank you.

I yield back.

Chairwoman COMSTOCK. Thank you.

I recognize Mr. Webster for five minutes.

Mr. WEBSTER. Thank you, Madam Chair.

I have a question, I believe, for Dr. Romine. So we have this—if we looked at the negative side of cybersecurity and all the things that are happening, the attacks from other governments and even in the private sector and things that are all going on, it seems like just from what I've heard today that that's an issue that's moving at light speed, and yet we're not here in this body known for moving at snail speed, and I guess my question is, you had testified that there have been three modifications in 30 years of the document that pretty much tells you what you should be doing and how you should be doing it, and so we're walking along and yet we have something moving three times ten to the eighth meters per second. And so my question, I believe, is there an infrastructure that you're a part of and others that are part of who have testified—we've got this whole list of acronyms of organizations that are working on this. Is that infrastructure that's there combined fast enough and good enough to catch it?

Dr. ROMINE. Thank you for the question. Let me address it in this way. One of the reasons that NIST is as effective as it is in this space is our deep and longstanding partnerships with the private sector, the folks who are moving at light speed, and so I think the idea that we maintain that connection with them, that we provide input to them on priorities that the federal government has, that they provide us with a partnership working collaboratively on solving some of these really challenging technical problems in security, frankly I think is the only way that we can maintain the kind of pace and to anticipate some of the challenges that we have down the road to remain relevant.

We have deep technical expertise ourselves but we rely entirely on that connection that we have with industry and with academia to maintain our awareness and engagement at the speed that's necessary.

Mr. WEBSTER. Do you think that there is too many or too few kingdoms that are addressing this issue, or do they—maybe if there are too many, are they bleeding over into each other and maybe doing things that the other might be doing?

Dr. ROMINE. Well, I'm not exactly sure how to interpret your question but——

Mr. WEBSTER. I'm only looking at the structure to see if this is the right structure or there should be something else.

Dr. ROMINE. Oh, I see.

Mr. WEBSTER. That's what I'm thinking about.

Dr. ROMINE. Right. Yes, I can really address only NIST's role with regard to how we provide guidance and standards in this space, and I think the statutory role that we have is essential for us. It's—you alluded to the fact that there——

Mr. WEBSTER. Is it more defensive in that the agency—let's say the federal agencies, do they have to come to you before you give them or are you aggressive in——

Dr. ROMINE. No, we have partnerships. I alluded to the partnerships with the private sector but we also have strong engagement in the public sector as well with other federal agencies and even with state and local governments in some cases.

From my perspective, you alluded to the fact that there are only three updates to the governing legislation of FISMA in the last 30 years. I view that in many ways as a strength because the legislation actually sets the structure, the very high-level components, and if that were to change rapidly, I think it would be much more difficult for us. Whereas putting the structures in place and providing roles and responsibilities clearly in legislation gives us the opportunity to then operate effectively in that structure.

Mr. WEBSTER. Thank you very much. That was helpful.

I yield back.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. Bera for five minutes.

Mr. BERA. Thank you, Madam Chairwoman, and the Ranking Member.

You know, just listening to the testimony, Mr. Mulholland, in your opening statement, you talked about how cyber-attacks represent a clear and present security threat, and I think each of you, you know, alluded to the sense that the federal government is pretty vulnerable to cyber-attacks. Would any of you dispute that statement? So we've got vulnerabilities there.

I think, Dr. Burley, in your opening statement, you talked about the workforce need being acute and immediate, and I think you mentioned over a million jobs, maybe 1.5 million vacancies. Now, that's not just federal government, that's the need that exists in the private sector, and so there's this acute need, and unfortunately, I would bet that it's going to get worse before it gets better because we're not training that workforce.

If we look at the federal government, maybe Mr. Wilshusen, I would imagine we've got critical hiring needs in the federal government that we can't fill. Would that be correct? In the thousands?

Mr. WILSHUSEN. I hesitate to give a specific number but with the work we've done and the surveys where we've gone out to the agencies, it was pretty much across the board that they all felt they were very challenged to attract and retain the cyber skill sets that they needed.

Mr. BERA. So we recognize we're vulnerable as the federal government. We've got critical vacancies and needs that we need to hire for. We understand that our salaries, you know, compared to just looking at simple rules of supply and demand cannot compete with what folks in the private sector may be paying so we have difficulty retaining and recruiting those individuals. Would that be an accurate statement? So that, you know, obviously is a critical need, and a critical security need. Recently a few weeks ago, the President signed a broad, sweeping federal Executive Order freezing the hiring of federal employees. Do we know if these critical IT, critical cybersecurity jobs are exempt from that federal order, Dr. Romine?

Dr. ROMINE. We're seeking clarification on that now just to make certain because we do want to know whether we're going to be able to continue to recruit in this space.

Mr. BERA. I mean, I guess I would go on the record along with my colleagues in a bipartisan way that, you know, we ought to send a strong message to the Administration that these are clearly critical jobs that need to be filled that are in our national security interest and we would provide you with whatever support you need might in that clarification, but my sense is, if it's already hard enough to recruit these individuals and hard enough to retain these individuals, let's not make it any more difficult, and, you know, that broad order in my mind is making us less secure and certainly it's worrisome.

You know, maybe, Mr. Wilshusen, if we were thinking about strategies to recruit and retain some of these individuals, we've introduced a couple bills. One was the Tech Corps Act in the last Congress which would try to work with universities to help offset the cost of tuition. I'm a physician by training. Much as doctors can go back and fill critical needs and serve their country and community, perhaps that's one idea. You know, we've also considered prioritizing hiring of veterans and getting them into quick technical training skills—we know they're already patriotic—in order to fill some of these needs. What would be some other ideas that could help us fill these needs?

Mr. WILSHUSEN. Well, I think the one you mentioned too about reimbursement of student—well, one of the things would be reimbursement of student loans. That's one that we use at GAO, and it's a very useful and effective way of helping to recruit staff, particularly in the IT security realm where we perform these IT audits. So that has been very helpful in being able to reimburse and help those individuals to pay off their student loans would be one thing.

Another, of course, is just the focus on the civic responsibility and I would say the satisfaction of doing federal work. That's been very effective for us as well because of the type of work that we do.

Mr. BERA. Dr. Romine, do you have any suggestions?

Dr. ROMINE. I agree with Mr. Wilshusen that one of the secret weapons we have in recruiting top-notch staff is the fact that our mission is so compelling and interesting and we work in a really terrific place. I'm guessing GAO would make that same claim.

So people who do feel a sense that they want to contribute through public service, we're able to be competitive with that segment of the population.

I also want to point out one of the things that really needs to be understood well is that cybersecurity as it's currently constituted is interdisciplinary, and by that I mean people from economists, sociologists, psychologists, electrical engineers, computer scientists, across the board, these folks have roles to play in cybersecurity that are really compelling, and so we find that we're able to attract those folks.

Mr. BERA. I realize I'm out of time so I'll yield back.

Chairwoman COMSTOCK. And I now recognize Mr. Abraham for five minutes, the new Vice Chair of the Subcommittee. Welcome.

Mr. ABRAHAM. Thank you, Mrs. Chair.

Mr. Wilshusen, as far as—give me the advantages and disadvantages from your perspective as an auditor, when the federal government and the private sector, they take the same approach, in this case using NIST Cybersecurity Framework for securing their information and information systems, the good, the bad, the uglies?

Mr. WILSHUSEN. Well, one of the benefits of the NIST Cybersecurity Framework is its flexibility. The way that it can be used by different organizations, whether they're federal government organizations or private sector organizations who apply the techniques. The guidance in that document is very useful. Certainly, over the years NIST has issued a complete and comprehensive set of cybersecurity guidelines and standards that could be used by the private sector and indeed many do. They certainly are required for the federal agencies. We use that criteria in our audits, and we think that NIST does a very good job of identifying those.

Mr. ABRAHAM. Mr. Mulholland, your take on the advantages and disadvantages of taking that same approach?

Mr. MULHOLLAND. Well, I would actually second that the NIST Framework, even within the private sector is still seen as being a very compelling standard. There are many standards out there, and NIST is certainly one of the most compelling.

I'll add a different spin to my answer, though, which is that because it is a compelling framework, it actually means it's software manufacturers like ourselves who actually build our software so that it can conform to the standard and make implementing the standard a little easier for people who are using our software. So by having that kind of standard somehow float to the top actually, you know, a rising tide lifts all boats, so to speak.

Mr. ABRAHAM. Let me stay with you, Mr. Mulholland. In your testimony, you said that there may be a need to increase federal oversight or increase oversight of the federal cybersecurity by creating a special GAO office, would you elaborate on that? What does that entail?

Mr. MULHOLLAND. That's certainly one of the CSIS recommendations that I'm less familiar with so I'll defer to my written testimony if that's okay.

Mr. ABRAHAM. Mr. Wilshusen, give me your take on that. I'll ping pong between you guys.

Mr. WILSHUSEN. Okay. Well, with respect to GAO assessing agencies' implementation of cybersecurity, that's something we do already. One of our roles is to provide and help Congress provide the oversight over federal agencies' implementations of cybersecurity. So that recommendation in terms of having GAO conduct reviews is something that we do and we'll continue to do.

Mr. ABRAHAM. Mrs. Chairman, I yield back.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. Beyer for five minutes.

Mr. BEYER. Thank you, Chairman Comstock.

Last week, Ranking Members Lipinski and Johnson and I sent a letter to Chairmen Smith, LaHood and Comstock calling on them to investigate President Trump's cybersecurity practices, and my friend, Chairman Smith, was quoted in the press as saying that this is hypocritical since we didn't support the Committee's investigation of Hillary Clinton's email server. I just want to highlight a few facts.

Number one is that by the time Science Committee launched its investigation of former Secretary Hillary Clinton's emails, three government agencies—the FBI, the State, Inspector General, et cetera—had already completed investigations of Clinton's emails and five other Congressional committees were investigating the same issue, and the Committee essentially dropped all interest in Hillary Clinton's emails right after the presidential election.

There's also a quote in The Hill yesterday from an anonymous Science Committee staffer claiming Science Committee Democrats refused to support past investigations into cyber hacks, specifically mentioning the OPM hack and breaches at the FDIC, and I'd like to submit two documents for the record that dispute these alternative facts. The first is my letter to Chairman Smith, which requested the hearing into the OPM hack, and the second was any opening statement—my opening statement from the FDIC hearing in which I voiced explicit support for the inquiry into the FDIC breaches. I also don't remember any of the Democrats defending Secretary Clinton's email server.

And I believe really that members of both parties are deeply concerned about cybersecurity, and I look forward to continuing to work together with my Republican friends on this.

This past week, the Trump Administration revised and then delayed the release of a new Executive Order on cybersecurity. It was reported that the Chief Information Security Officer in charge of cybersecurity for the White House and the President was fired. As I pointed out in the letter with Ranking Members Johnson and Lipinski, in the few short weeks in office, President Trump and some of his senior staff appear to be struggling with implementing proper and appropriate cybersecurity practices. The President still apparently uses his easily hackable personal cell phone, his Android, not an iPhone, which of course opens it up to the foreigners who could use foreign intelligence services who can tracking location, can log keystrokes, could use the camera.

The official Twitter account has been linked to unsecure private Gmail account, and just this weekend it was widely reported that the President held conversations and reviewed documents about the North Korean missile launch in the middle of Mar-a-Lago's restaurant, potentially within earshot of waiters and fellow diners, and according to eyewitnesses and pictures we've all seen, aides used their phones as flashlights to illuminate the documents, which could let hackers if they had compromised these phones to read the materials because the phones' cameras were pointed right at them.

So these actions give the appearance that the Trump Administration's cybersecurity policies are in disarray and that the personal cybersecurity practices of the President and senior staff are both unwise and insecure. And by the way, if we're concerned—you know, the security of the President's Twitter account is not trivial. I mean, his tweets have given rise to a drop in Toyota stock, the Mexican peso to devalue, the best subscription day ever on Vanity Fair, the scuttling of the Mexican president's trip to the United States.

So Dr. Burley, could you speak to this issue, particularly about how effective cybersecurity policy requires buy-in from the top of the organizational chart, whether it's from a CEO or agency head or even the President of the United States?

Dr. BURLEY. Thank you for that question. I would say two things. One, certainly when we're dealing with cybersecurity culture within any organization, it is important that all levels of the organization buy in and employees are certainly driven by what the top of the organization pushes forward.

With regard to awareness and understanding how our individual behavior impacts the security of our enterprise and our personal security, I would say that this is something we need to address in the redevelopment of cybersecurity awareness programs. We need to move beyond simply trying to make people aware of the issues and move toward helping them understand what their particular behavior does in terms of making a situation more or less secure, and that's something that needs to happen across all levels of organizations and even starting with some of the programs that we were talking about earlier in terms of going down into the K–12 range because awareness is one thing but understanding the implications of your behavior that then lead to behavioral changes is another matter.

Mr. BEYER. Thank you very much.

And Dr. Romine, we know how powerful the President's Twitter account is. It's an important way for him to communicate. What should the Administration do to secure his important Twitter account?

Dr. ROMINE. Well, that verges on a certain oversight function in a specific case like this, and NIST is a non-regulatory agency with no oversight role or capabilities. I think the oversight typically for federal cybersecurity rests with the Inspectors General, with the GAO and with OMB who has the policy lever for ensuring cybersecurity of systems. So beyond that, I don't think I can really comment.

Mr. BEYER. Madam Chair, I yield back.

Chairwoman COMSTOCK. Thank you, and I'd also like to enter into the record Chairman Smith's letter responding to Mr. Beyer's letter, and I'm sure he welcomes your newfound interest in oversight, and you obviously have a role on the Oversight Subcommittee and this Committee, but I would like to also enter into the record Mr. Beyer's August 22nd, 2016, press release that was critical of the full Committee and the email investigation and your quote here, “The House Science Committee must focus on its role promoting science and ensuring that America is the global leader in research and development rather than scoring cheap political points.” And I’d also enter into the record an October 2016 interview that was on a local TV show which was critical of the FBI Director in that regard also.

[The information appears in Appendix I]

Chairwoman COMSTOCK. I will now yield five minutes to Mr. LaHood, the Chairman of the Oversight Subcommittee.

Mr. LAHOOD. Thank you, Madam Chair, and I want to thank the witnesses for being here today and for your valuable testimony.

I do want to make a couple observations in response to my friend Mr. Beyer. I would first say that there’s no evidence that President Trump is using his personal phone. In contrast to what was said, the New York Times has reported that he traded in his Android phone for a secure encrypted device authorized by the Secret Service, which is protocol for all Presidents, and he is abiding by that protocol by having an authorized phone.

I would also dispute the assertion that somehow the allegations of what occurred with former Secretary of State Hillary Clinton which was brought up, you know, in that case, I think it is really apples and oranges in terms of the activity that went on there and the allegations there. You know, the FBI in that case found multiple violations of federal law on national security, cybersecurity and criminal statutes. The FBI Director said in his press conference that there were violations of federal law there. There’s currently an active Department of Justice investigation and a grand jury looking into that, and I think the underlying circumstances and facts there are completely different than a Twitter account. And let’s remember, Twitter is by its nature a service meant to provide information to the public, and there is again no information that somehow the tweets that are being put out by the President are done by a private phone. They can clearly be done by a secure, authorized phone, and I think we live in a unique age with technology. The fact that the President communicates every day with 20 to 25 million people by Twitter in an unfiltered, raw manner I think is unique, but that’s the age that we live in now. But to make the comparison to what happened with Hillary Clinton I think is really disingenuous to this discussion, and I think the facts bear that out.

I guess in looking at our hearing here today and how we can improve on cybersecurity at the federal level, I’m very interested, and I’ve talked about this in previous hearings, looking at the private sector and what has been beneficial in the private sector, what has worked there, and public-private partnerships specifically, and I guess I would start with Mr. Mulholland.

In looking at the private sector, how do we look at metrics or effective strategies that have worked, Mr. Mulholland, that we can implement, learn from, and then how do we—how do we in an effective way put together a framework or metrics to judge that moving forward?

Mr. MULHOLLAND. Thank you for the question. I think in terms of metrics, we can have metrics for metrics sake, or we can have metrics that are actually measuring outcomes. I think in the private sector, actually to refer back to something that Dr. Burley mentioned earlier, we've moved from basic awareness to understanding. So sometimes metrics can be the kind of outcome of a checklist of items that people can complete without necessarily actually understanding what they're doing or why they're doing it. So certainly in the private sector, we've moved from, you know, predominantly checklists to really focusing on what outcomes are on how do you measure and use metrics to measure those outcomes. So specific examples might be actually looking at what are our threat models so what is the actual threat that we are subject to and then focusing and prioritizing around that. So for example, we're a Silicon Valley-based technology company. A big threat to us is the theft of intellectual property so a lot of the metrics and a lot of the outcomes we're looking at is, how do we protect our intellectual property. Perhaps some other pieces of data are less important to us than, you know, the lifeblood of our company. So we focus our metrics on outcomes and not so much on checklists for checklists' sake.

Mr. LAHOOD. Thank you for that.

The Cybersecurity Commission report recommends that the President issue a national cybersecurity strategy within the first six months of the Administration. I guess, Mr. Wilshusen, what might you—I guess what might you wish to see reflected in that strategy and what advice would you give?

Mr. WILSHUSEN. Well, I think a couple things. One would be just to come to an agreement on what the norms of behavior should be within the cybersecurity realm across the various different nations. As you know, norms differ in many different ways across nations. Coming to some sort of understanding of what's acceptable behavior, what is not when using the internet and cyberspace would be one of those areas that should be discussed.

And also how to go about raising that discussion with the different nations who have different values and mores would be another key area as part of that strategy.

Mr. LAHOOD. Thank you.

Those are all my questions. Thank you.

Chairwoman COMSTOCK. And I now yield five minutes to Ms. Rosen, a new member of the Committee.

Ms. ROSEN. Thank you, Madam Chairwoman.

I have to tell you that I started my career as a computer programmer in the 1970s with a card deck and a mainframe, and oh, how I long for those days when no one could break into the system. It was very difficult. We had a phone with a modem. Remember that was the only way in? And there weren't the possibility for attacks in those kinds of ways.

So I couldn't agree more that we need to have the analytical and teach the analytical and critical thinking skills that are needed of course to move us forward in all jobs across all platforms for this sector and that as you so eloquently said, the computer industry, engineering sciences, we have to take a multifactorial approach to be able to dynamically respond across all platforms to the challenges that we're facing, and nobody knows this better than you, and like I said, as I wrote software trying to keep that secure and safe, so I have a different perspective maybe than some people on this panel. I could talk to you all all day.

But what I find most important, as I started as a woman in technology in the 1970s, it's still not so popular but more popular. How do we teach and train—how do we promote the education? First of all, I think it starts with our teachers and our educators. How do we get them trained to inspire the students that understand that computers and all these things are very creative? It's not dull and boring. It's extremely creative and innovative. And then teachers can take those to our schools K–12 and above.

And then also my second part of the question is the general public when you begin to talk about computer things, our eyes roll back. They don't want to hear about cyber hygiene. They don't get it. They just want to use their social media, Twitter or Facebook or whatever. How do we educate the public about how easy it is for them to be used as a target into things with phishing and all those? How do we make them—give them the buy-in to do something?

Dr. BURLEY. Well, with your first question, thank you. I would say that we have to target all of the K–12 teachers instead of just focusing on those who have self-identified as being interested in computer science or in cybersecurity. So I would say that we need to start to work with the schools and colleges of education so that when the teachers are in their developmental process that they begin to understand cybersecurity concepts and that they understand how to integrate those concepts into what they're doing in their fifth-grade English classroom or what they're doing in ninth grade biology because there is an aspect of cybersecurity that pervades across the curriculum. But in order for the teachers to be able to do that, we have to educate them as such, so I would say that that's a part of what we need to do and focusing on them.

The other thing with regard to getting more women and young girls into STEM in general and certainly cybersecurity is in role models, understanding that there are people who look like them and who do this job and what that really means. We talk about cybersecurity as if it is one thing when it's really not, and so—but we do ourselves a disservice because we don't really help people to understand what it means and what it can mean to be a cybersecurity professional. So we need to do a better job of that. And I would say that that also adds into this notion of the general public and awareness and understanding. That we're not talking about something that only people down in the corner are doing or that those guys over there will keep us safe but that we really understand as individuals what our role is, how we interact with things, that we understand the tradeoffs that come along with convenience so that we understand what we're giving up when we're getting something, and as a society we don't really have that understanding and so we need to do more to educate the public on what those tradeoffs are and what their role is in making sure that they are safe and that collectively the society is safe.

Ms. ROSEN. Thank you. I appreciate that.

I yield back.

Chairwoman COMSTOCK. Thank you, and I now recognize Mr. Marshall for five minutes, and welcome to the Committee, our new member from Kansas.

Mr. MARSHALL. Thank you so much, Chairman.

I'm a physician and had the pleasure of leading a hospital and a group of physicians through meaningful stages 1 and 2, been using an electronic medical record now for a couple years. I'm intrigued with the value. Someone here in the review mentioned that medical record is worth ten times more than some other records you would hack. What brings the value to people? What's in there that brings value to start with? And I'm not sure who could answer that question the best.

Mr. MULHOLLAND. If I can clarify, do you mean in terms of the value of a medical record versus, say, a tax record or a credit card?

Mr. MARSHALL. I guess so. In one of the testimonies, someone said that the—on the black market, it would be worth ten times than other type of record.

Mr. WILSHUSEN. What I would say is that one of the benefits with electronic health records and information is the fact that the accessibility of that information not only to patients if they're able to access it but to other healthcare providers can help to assure that the treatments, the drugs prescribed to particular patients, you know, if they have a full view of the individual's overall health records that that can be very positive and beneficial to the healthcare of that individual.

But at the same time, what we have found in our audits of reviewing the security and the privacy controls over that information is that while the Centers for Medicaid and Medicare Services have come up with guidelines for that through HIPAA and the security and privacy rules, the actual use and implementation of controls on certain health information technology has not been adequately reviewed in some respects to assure that those capabilities have been designed into the technology and that in fact at some of the healthcare providers that that information and those controls are effectively implemented.

Mr. MARSHALL. Yeah, I guess——

Mr. WILSHUSEN. I'm not sure if——

Mr. MARSHALL. —I'm not explaining my question very well. I certainly understand about physician-to-physician transfer of records and that we used to go from one page of information, now it's 40 pages and it's almost a worthless piece of document. My question is on the black market. When people are hacking medical records, what makes it ten times more valuable than a credit card or other things they hack into? What do they do with it?

Mr. MULHOLLAND. I think I'll take an attempt at that. Something like a medical record, to your point about, you know, the 40 pages of information, that's going to contain a lot of effective metadata that perhaps would not be available in, you know, just a credit card-type hack or whatever, so, you know, you're going to be able to get a person— probably be able to get a person's Social Security number, their date of birth, their address, so that can be used for other attacks. You might then be able to use that to hack a person's credit card details or their tax return, but also you're going to have a list of medical conditions that can be used for, you know, extortion purposes in the most extreme case but also basic things like prescription fraud. You can see who is the—you know, does the patient have any controlled substances prescribed to them, where their pharmacy is, and you've also got all the information to be able to impersonate that person and potentially go and steal their records. So it's a little bit of a goldmine. You've got a lot of information in the same place that can be very valuable used——

Mr. MARSHALL. I mean, my big—one of my bigger concerns would be Medicare fraud, Medicaid fraud, people pretending like they're a physician. They've got this person's health record and they bill Medicare and Medicaid for procedures never done. Are we seeing much of that now or how big of an issue do you think it actually is today?

Mr. MULHOLLAND. I can't personally speak to that but it's certainly very feasible with the information available.

Mr. MARSHALL. Okay. When someone made the statement that it was ten times more valuable to have that record than other, say, a credit card record, is it ten times 10 cents? Is it ten times a dollar? Give me a—what's a black-market value of something like this?

Mr. MULHOLLAND. Well, I can't tell you the exact value of a Medicare record—or sorry, a medical record but I will tell you to calibrate that credit card information goes for cents. It is that much of a commodity. So your credit card details are probably, you know, worth 10 or 20 cents.

Mr. MARSHALL. And this might be theoretically then worth $10 or $20. If you could hack into my physician's office and I have 5,000 records there that it might be worth 5,000 times $10 to somebody?

Mr. MULHOLLAND. Conceivably. I couldn't give you an exact figure, but yes.

Mr. MARSHALL. Thank you. I yield back.

Chairwoman COMSTOCK. Thank you. I now recognize Ms. Bonamici for five minutes.

Ms. BONAMICI. Thank you very much, Chair Comstock and Ranking Member Lipinski, and thank you to our witnesses for testifying today. I've been in a hearing in the Education and Workforce Committee, which explains my absence for the beginning of this, but I did read your testimony and really am particularly concerned that we are falling short when it comes to developing adequate cybersecurity personnel both in quantity and quality, and I know that the NIST report recommends that federal programs supporting education at all levels should incorporate cybersecurity awareness for students as they're introduced to and provided with internet-based devices, and I know this has been discussed already here this morning but I really want to emphasize that especially with my concerns about education and workforce issues as well that these programs be developed as the report says and focused on children as early as preschool and throughout elementary school, and we also need programs to better prepare our teachers, and I know that that's been discussed.

So I wanted to talk a little bit about the tremendous potential for community and technical colleges, community colleges to have an increased role in preparing the workforce. What more can we be doing to create an environment that supports this? And then also if you'll address public-private partnerships as well. My State of Oregon has been working on a Center for Cyber Excellence, which is a collaboration with private sector as well as our universities and community colleges. So can you talk about what sorts of roles community and technical colleges can play as well as public-private partnership?

Dr. Burley, I'll start with you.

Dr. BURLEY. Community and technical colleges play an incredibly important role in developing the cybersecurity workforce. They are often more flexible than four-year institutions and so they're able to integrate curriculum a little bit faster. They are often where we turn to for more of the hands-on technical training that we are not necessarily as equipped to provide as rapidly in the four-year space but it really is a collaboration across all of the different levels of the academy because while the community and technical colleges are possibly able to help us develop technical skill sets a little bit faster, there are other aspects that perhaps they are not as well versed in doing and so we really have to continue to enable and push partnerships across all the levels of academia, and that also gets to your second question about the public-private partnership. Because we're dealing with an environment where the needs are very broad and very rapidly evolving, it is critical that all of the different sectors play a role and collaborate to make sure that the programs that we're developing have all of the different components that are necessary and that we are really getting at holistically looking at the development of the workforce, and it's not a situation where we can simply focus on one part of the ecosystem at the expense of another because we'll only grow a portion of the workforce.

Ms. BONAMICI. I'm going to ask the others to respond as well, but before I do, would you please talk a little bit about how we can get more girls, young women and minorities involved?

Dr. BURLEY. A couple of things. I mean, first we have to begin to really push forward role models so that people understand that there are people in the workforce that look like them and that are doing these jobs. That's very important, and evidence has shown that across all of the STEM disciplines, that that's an important consideration.

Ms. BONAMICI. And I'll put in a little plug for Hidden Figures if nobody else has done that.

Dr. BURLEY. Absolutely. We also need to unbundle what it means to be a cybersecurity professional. It really is a very broad field with many, many different occupations and different roles that people can play, and while you may not see yourself in one type of role, there are a thousand other roles that you could see yourself in and so we really have to do a better job at explaining what it means to be a part of the cybersecurity workforce.

Ms. BONAMICI. And you say "we." Who would that be? Teachers——

Dr. BURLEY. All of us, the government, academia, anybody who is developing or working on developing the cybersecurity workforce. This is part of what awareness programs ought to do but it's all of those who are involved in the development, the education of future professionals.

Ms. BONAMICI. Terrific. I have a little bit more time left if somebody wants to jump in. Dr. Romine?

Dr. ROMINE. I'd like to just make two very quick points. NIST, specifically my laboratory's, privileged to house the Program Office for the National Initiative for Cybersecurity Education, which is an interagency program with a lot of agencies committed to working together to help solve this problem, workforce problem and awareness problem, and certainly community colleges are one area where we have touch points and are engaged.

With regard to your public-private partnership, we're also privileged in my laboratory to house the National Cybersecurity Center of Excellence, the NCCOE. I'm delighted to learn that your State of Oregon is doing an analogous thing. I'd love to learn more about it.

Ms. BONAMICI. Terrific. Thank you very much.

Mr. WILSHUSEN. And if I may just add one comment real quick from a personal note? I took a community college course at PG Community—Prince Georges County Community College on network defense about a year and a half ago. It was very rigorous and it was very informative for me, and I used that as part of my continuing professional education. So there's definitely a very useful place for community college to provide technical skill sets to the federal workforce.

Ms. BONAMICI. Thank you very much. I see my time is expired. I yield back. Thank you, Madam Chair.

Chairwoman COMSTOCK. Thank you, Ms. Bonamici, and I believe we will continue on that education front and have future hearings, and I agree very much with you on the role of community colleges, you know, online classes, and a lot of these approaches, and we are very pleased that the Hidden Figures are not as hidden anymore, and it's a fabulous movie, and I'll just take the—since I have a young women's leadership program, I hope Dr. Burley can come and join us in highlighting the importance of this because STEM education and STEM careers are something that we very much try and promote with young people, and since I have a daughter in that field, I always appreciate getting mentors out there in front of young women, and it's exactly what you say. They need to see other people in that role so that they can relate and understand the job, so it is very apropos.

So I thank all of the members of the panel this morning for their testimony and their insight and their passion on this very important issue, and I know we will continue to have a number of hearings on this front.

The record will remain open for two weeks for additional written comments and written questions from members.

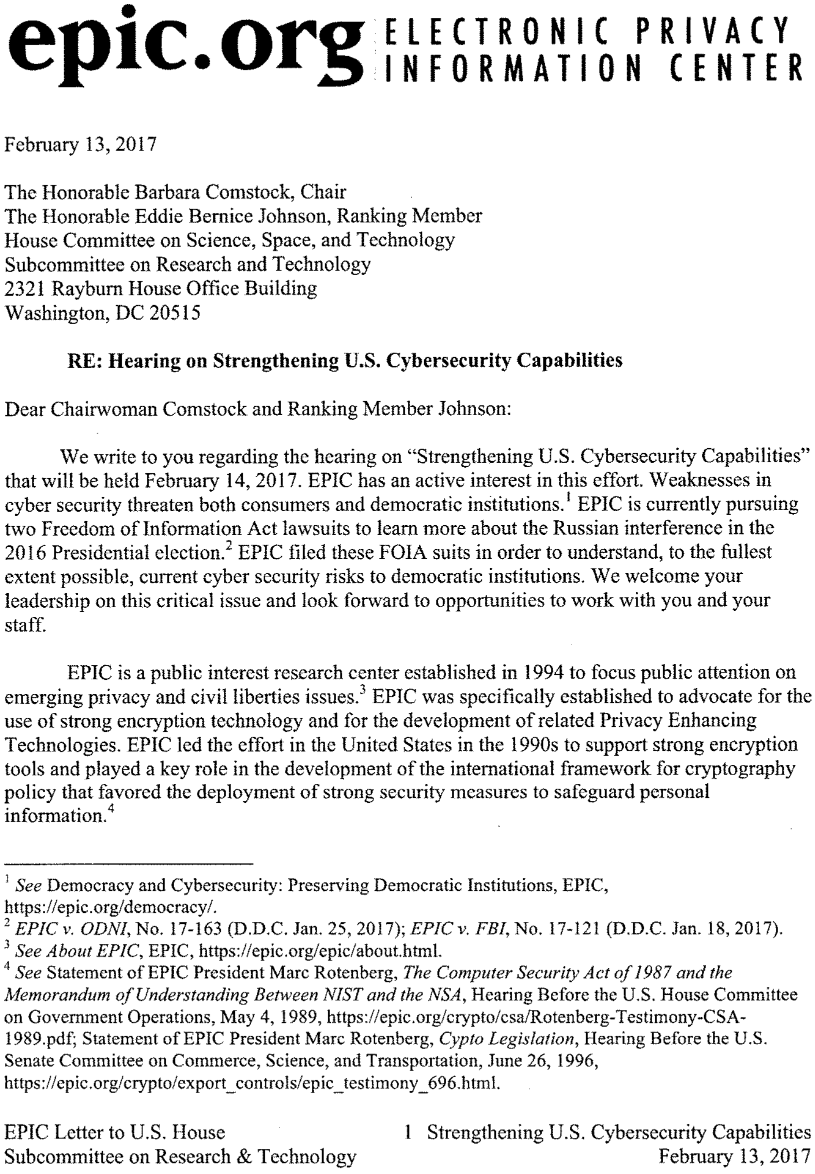
And this hearing is now adjourned.

[Whereupon, at 11:40 a.m., the Subcommittee was adjourned.]

Appendix I

Additional Material for the Record

Documents submitted by Subcommittee Chairwoman Barbara Comstock



epic.org ELECTRONIC PRIVACY INFORMATION CENTER

February 13, 2017

The Honorable Barbara Comstock, Chair
The Honorable Eddie Bernice Johnson, Ranking Member
House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
2321 Rayburn House Office Building
Washington, DC 20515

RE: Hearing on Strengthening U.S. Cybersecurity Capabilities

Dear Chairwoman Comstock and Ranking Member Johnson:

We write to you regarding the hearing on "Strengthening U.S. Cybersecurity Capabilities" that will be held February 14, 2017. EPIC has an active interest in this effort. Weaknesses in cyber security threaten both consumers and democratic institutions.[1] EPIC is currently pursuing two Freedom of Information Act lawsuits to learn more about the Russian interference in the 2016 Presidential election.[2] EPIC filed these FOIA suits in order to understand, to the fullest extent possible, current cyber security risks to democratic institutions. We welcome your leadership on this critical issue and look forward to opportunities to work with you and your staff.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC was specifically established to advocate for the use of strong encryption technology and for the development of related Privacy Enhancing Technologies. EPIC led the effort in the United States in the 1990s to support strong encryption tools and played a key role in the development of the international framework for cryptography policy that favored the deployment of strong security measures to safeguard personal information.[4]

[1] *See* Democracy and Cybersecurity: Preserving Democratic Institutions, EPIC, https://epic.org/democracy/.

[2] *EPIC v. ODNI*, No. 17-163 (D.D.C. Jan. 25, 2017); *EPIC v. FBI*, No. 17-121 (D.D.C. Jan. 18, 2017).

[3] *See About EPIC*, EPIC, https://epic.org/epic/about.html.

[4] *See* Statement of EPIC President Marc Rotenberg, *The Computer Security Act of 1987 and the Memorandum of Understanding Between NIST and the NSA*, Hearing Before the U.S. House Committee on Government Operations, May 4, 1989, https://epic.org/crypto/csa/Rotenberg-Testimony-CSA-1989.pdf; Statement of EPIC President Marc Rotenberg, *Cypto Legislation*, Hearing Before the U.S. Senate Committee on Commerce, Science, and Transportation, June 26, 1996, https://epic.org/crypto/export_controls/epic_testimony_696.html.

Data protection and privacy should remain a central focus of the cyber security policy of the United States. It is precisely the extensive collection of personal information without adequate safeguards that places the United States at risk from cyber criminals and foreign adversaries. In 2015, more than 22 million records of federal employees, including 5 million digitized fingerprints and the sensitive form SF-86, were compromised. So-called "credit monitoring services" are an insufficient response to the ongoing risk to the financial records, medical records, and private communications of Americans.

Strong encryption policy and robust technical measures must be enacted in order to safeguard personal data. Weaknesses in security standards create vulnerabilities for American businesses and consumers that will be exploited by foreign adversaries. Where it is possible to minimize or eliminate the collection of personally identifiable information, the risk to the American public will be reduced.

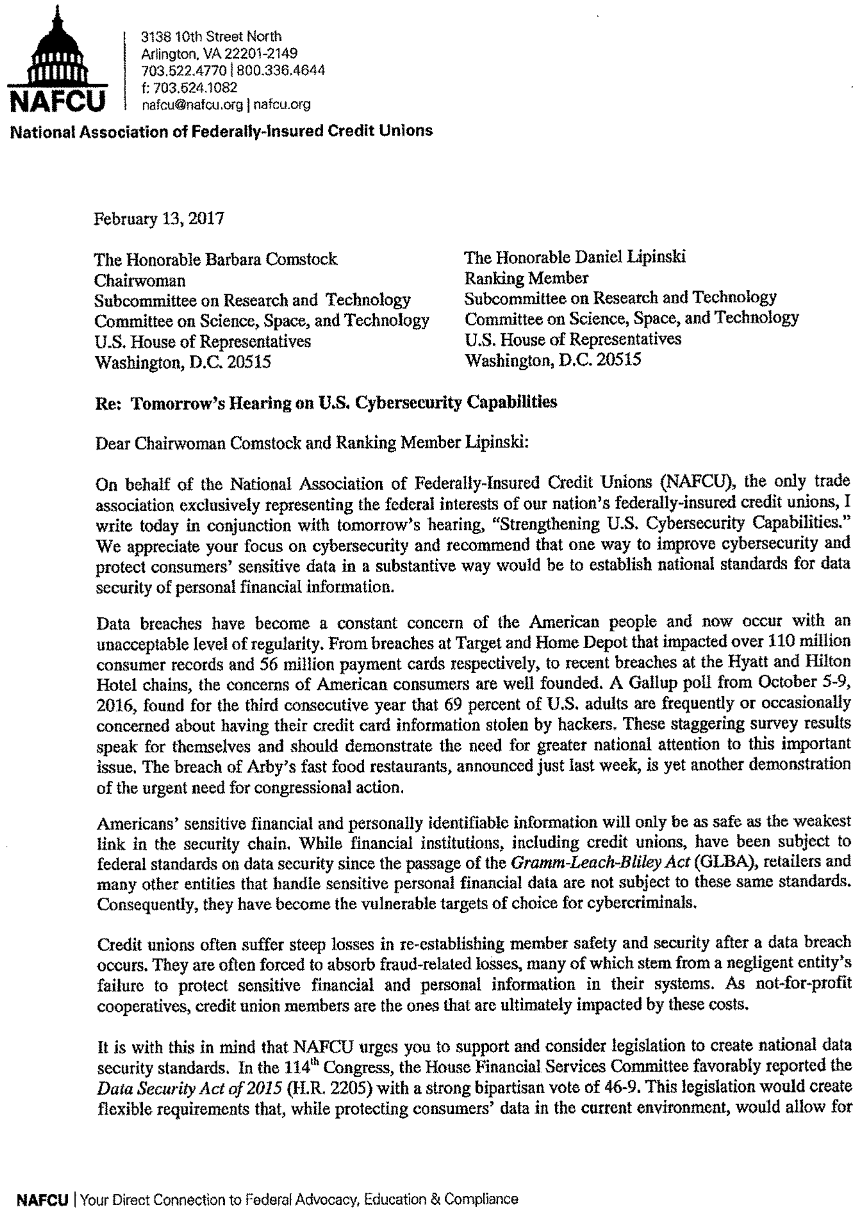
The Cyber Security Information "Sharing" Act is now in force. That law facilitates the transfer of customer and client data from the private sector to the government, raising widespread concerns among technical experts and privacy organizations about the protection of personal information. While we favor a cooperative relationship between companies and the federal government concerning cyber security, the federal government must respect the privacy obligations of private companies and ensure the transparency of its own conduct. In the cyber security domain, as with other programs supported by taxpayer dollars, the government must uphold the law and remain open and accountable.

Finally, Congress should strengthen the federal Privacy Act. Personal data stored in federal agencies remains one of the key targets of criminal hackers and foreign adversaries. Significant steps were taken by the last administration to establish a Federal Privacy Council and to coordinate privacy protection across the federal agencies. Still, more should be done, including updates to the federal privacy law and the establishment of a data protection agency in the United States.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on Research and Technology on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg	/s/ Caitriona Fitzgerald
Marc Rotenberg	Caitriona Fitzgerald
EPIC President	EPIC Policy Director



NAFCU

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

February 13, 2017

The Honorable Barbara Comstock
Chairwoman
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Daniel Lipinski
Ranking Member
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, D.C. 20515

Re: Tomorrow's Hearing on U.S. Cybersecurity Capabilities

Dear Chairwoman Comstock and Ranking Member Lipinski:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write today in conjunction with tomorrow's hearing, "Strengthening U.S. Cybersecurity Capabilities." We appreciate your focus on cybersecurity and recommend that one way to improve cybersecurity and protect consumers' sensitive data in a substantive way would be to establish national standards for data security of personal financial information.

Data breaches have become a constant concern of the American people and now occur with an unacceptable level of regularity. From breaches at Target and Home Depot that impacted over 110 million consumer records and 56 million payment cards respectively, to recent breaches at the Hyatt and Hilton Hotel chains, the concerns of American consumers are well founded. A Gallup poll from October 5-9, 2016, found for the third consecutive year that 69 percent of U.S. adults are frequently or occasionally concerned about having their credit card information stolen by hackers. These staggering survey results speak for themselves and should demonstrate the need for greater national attention to this important issue. The breach of Arby's fast food restaurants, announced just last week, is yet another demonstration of the urgent need for congressional action.

Americans' sensitive financial and personally identifiable information will only be as safe as the weakest link in the security chain. While financial institutions, including credit unions, have been subject to federal standards on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA), retailers and many other entities that handle sensitive personal financial data are not subject to these same standards. Consequently, they have become the vulnerable targets of choice for cybercriminals.

Credit unions often suffer steep losses in re-establishing member safety and security after a data breach occurs. They are often forced to absorb fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information in their systems. As not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs.

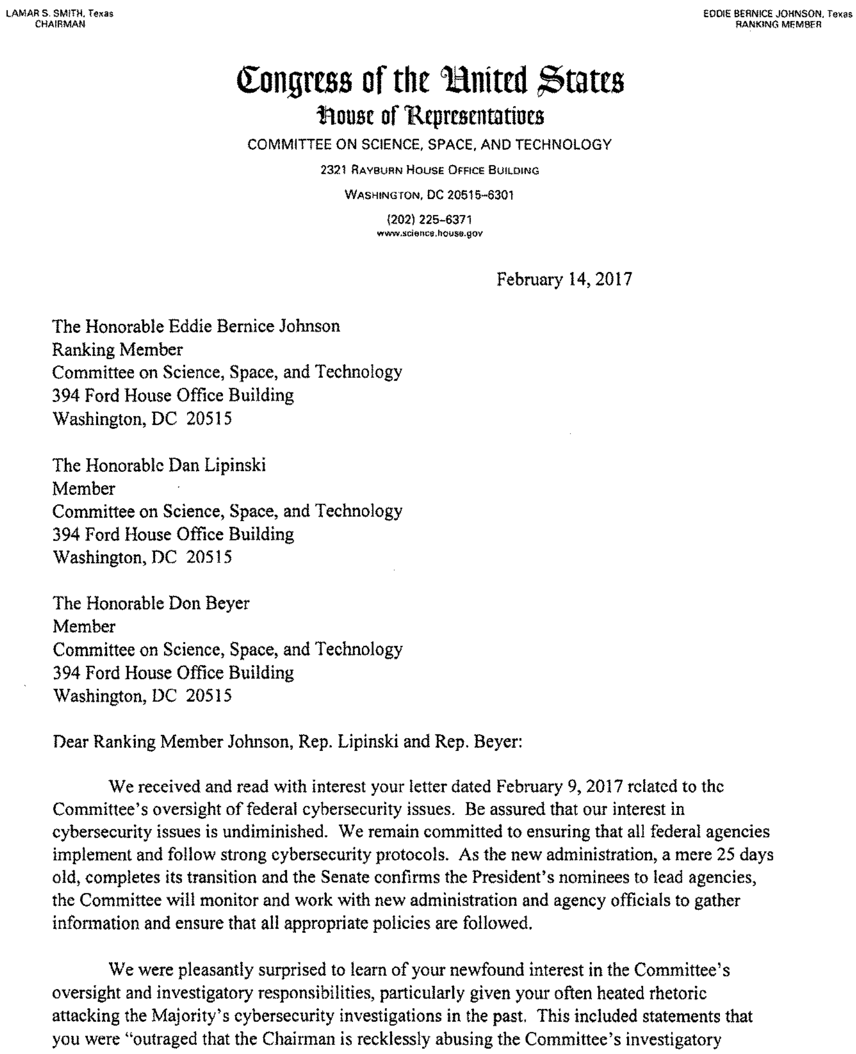
It is with this in mind that NAFCU urges you to support and consider legislation to create national data security standards. In the 114th Congress, the House Financial Services Committee favorably reported the *Data Security Act of 2015* (H.R. 2205) with a strong bipartisan vote of 46-9. This legislation would create flexible requirements that, while protecting consumers' data in the current environment, would allow for and encourage innovation to protect consumers from future threats we have not yet anticipated. Additionally, the national standards created in this bill would be scalable to allow for compliance by entities of all sizes. Just as the GLBA institutes requirements that are appropriate for both the smallest credit unions and the biggest banks, this legislation would allow for appropriate standards for the smallest corner store to the largest retailers. As you tackle the issue of cybersecurity in the 115th Congress, we urge you to consider including solutions such as the approach from the *Data Security Act of 2015* in any legislative effort.

Thank you for your attention and for your leadership on this issue of great importance to credit unions. Should you have any questions or require any additional information, please contact me or Chad Adams, NAFCU's Senior Associate Director of Legislative Affairs, at 703-842-2265 or cadams@nafcu.org.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Research and Technology



LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 Rayburn House Office Building
Washington, DC 20515–6301
(202) 225–6371
www.science.house.gov

February 14, 2017

The Honorable Eddie Bernice Johnson
Ranking Member
Committee on Science, Space, and Technology
394 Ford House Office Building
Washington, DC 20515

The Honorablc Dan Lipinski
Member
Committee on Science, Space, and Technology
394 Ford House Office Building
Washington, DC 20515

The Honorable Don Beyer
Member
Committee on Science, Space, and Technology
394 Ford House Office Building
Washington, DC 20515

Dear Ranking Member Johnson, Rep. Lipinski and Rep. Beyer:

We received and read with interest your letter dated February 9, 2017 rclated to thc Committee's oversight of federal cybersecurity issues. Be assured that our interest in cybersecurity issues is undiminished. We remain committed to ensuring that all federal agencies implement and follow strong cybersecurity protocols. As the new administration, a mere 25 days old, completes its transition and the Senate confirms the President's nominees to lead agencies, the Committee will monitor and work with new administration and agency officials to gather information and ensure that all appropriate policies are followed.

We were pleasantly surprised to learn of your newfound interest in the Committee's oversight and investigatory responsibilities, particularly given your often heated rhetoric attacking the Majority's cybersecurity investigations in the past. This included statements that you were "outraged that the Chairman is recklessly abusing the Committee's investigatory powers"[1] and that "[t]his is a wasteful use of taxpayer dollars by Chairman Smith and the Science Committee Republicans."[2] We trust that your calls last week for oversight of cybersecurity issues are sincere and not, as you state in your letter, the result of "the change of party in the Executive Branch."[3] Your participation in, and assistance with, the next steps in the following ongoing Committee efforts would be welcome:

- The Committee commenced an investigation into the FDIC's cybersecurity posture upon the receipt of several notifications of major breaches at the FDIC.[4] The Committee's investigation identified cybersecurity weaknesses widespread within the FDIC's information technology infrastructure, culminating in at least 14 major incidents that have been reported to the Committee since February 2016. The Committee also uncovered the existence of a significant attack on the FDIC's systems sponsored by the Chinese military, dating back to 2010. The Committee also brought to light FDIC leadership's reticence to reporting breaches to Congress and its willingness to insert countless delays into the agency's data breach management processes to avoid reporting breaches to Congress in a timely manner. To ensure they do not occur again, these systemic problems with FDIC IT management may require changes in management and policy at FDIC as well as continued Committee oversight; we welcome your assistance in promoting all necessary changes.

- Pursuant to the Committee's jurisdiction over the National Institute of Standards and Technology (NIST), which is responsible for updating and promulgating standards used to safeguard federal information systems, the Committee is conducting an investigation into the security of former Secretary Clinton's private email and server arrangement. The Committee found that, indeed, former Secretary Clinton's private server was subject to attempted attacks by multiple foreign entities, including hackers associated with China, Germany, and Korea.[5] Despite the issuance of a subpoena, one of former Secretary Clinton's IT contractors has refused to provide documents and communications crucial to the

[1] Press Release, Hon. Eddie Bernice Johnson, Ranking Member Johnson's Response to Issuance of Subpoenas in Investigation into Clinton Email Server (Aug. 22, 2016), http://democrats.science.house.gov/press-release/ranking-member-johnson-response-issuance-subpoenas-investigation-clinton-email-server.

[2] Press Release, Hon. Don Beyer, Beyer Denounces Science Committee Republicans' Clinton Subpoenas (Aug. 22, 2016), https://beyer.house.gov/news/documentsingle.aspx?DocumentID=407.

[3] Letter from Hon. Eddie Bernice Johnson, Ranking Member, H. Sci., Space, & Tech. Comm., Hon. Don Beyer, and Hon. Dan Lipinski, to Hon. Lamar Smith, Chair, H. Sci., Space, & Tech. Comm. 4 (Feb. 9, 2017).

[4] *See Interim Staff Report: The Science, Space, and Technology Committee's Investigation of FDIC's Cybersecurity* (July 12, 2016), *available at* https://science.house.gov/sites/republicans.science.house.gov/files/documents/Final%20GOP%20Interim%20Staff%20Report%207-12-16.pdf.

[5] *See Clinton Server Hack Attempts Came from China, Korea, Germany*, CHICAGO TRIBUNE (Oct. 8, 2016), http://www.chicagotribune.com/news/nationworld/politics/ct-clinton-emails-hack-20151007-story.html; Press Release, H. Sci., Space, & Tech. Comm., Smith Statement on FBI's Reopening of Clinton Email Investigation (Oct. 28, 2016), https://science.house.gov/news/press-releases/smith-statement-fbi-s-reopening-clinton-email-investigation.

Committee's investigation. We are sure that you agree that the refusal to comply with a lawfully issued subpoena demands the Committee's continued attention. We look forward to working with you to uphold Congress' oversight prerogatives.

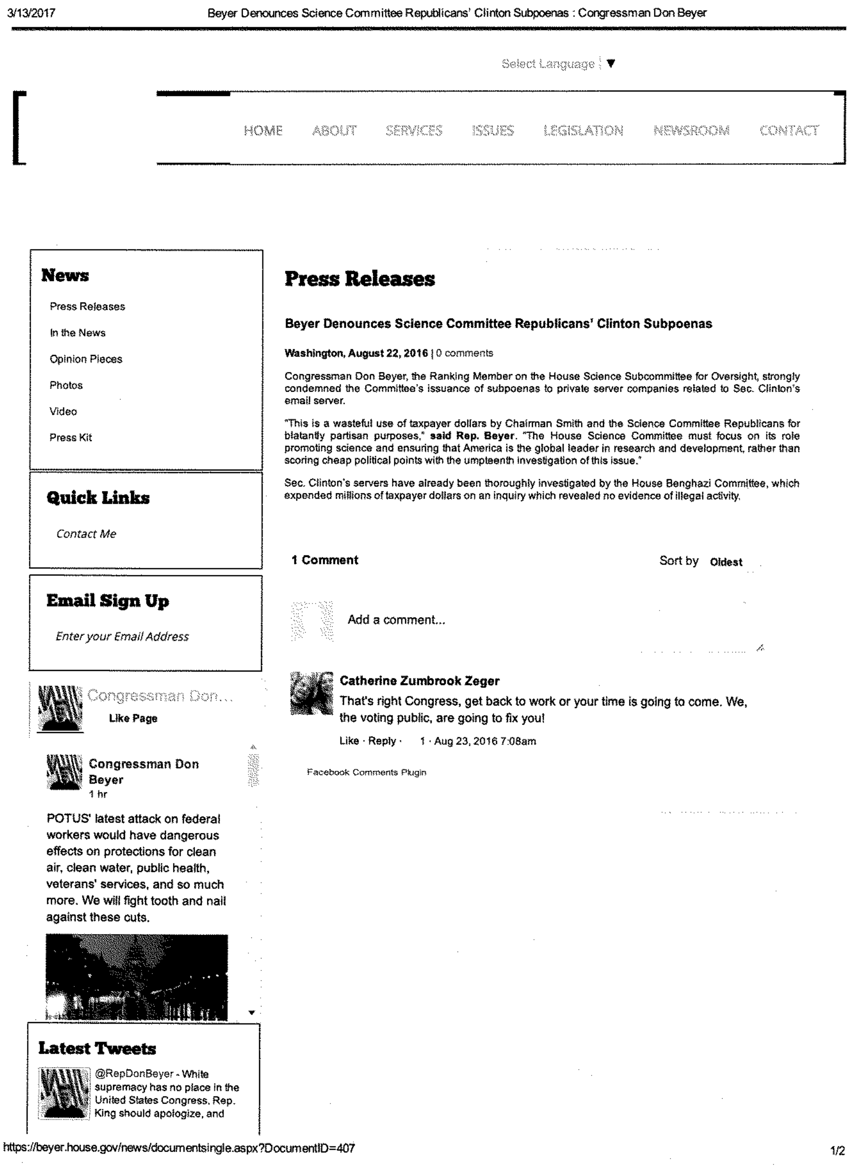
- The Committee commenced oversight of the Federal Reserve Board's cybersecurity posture after press reports indicated that the Federal Reserve had detected more than 50 cybersecurity breaches between 2011 and 2015, which included hacks, acts of espionage, and instances of unauthorized access. Pursuant to its jurisdiction under FISMA and attendant OMB guidelines, the Committee sought information about incident reports logged by the National Incident Response Team, or NIRT, and how the unit responded to and prevented threats from compromising the Federal Reserve's systems. Additionally, the Committee began oversight of a cyberattack at the Federal Reserve Bank of New York in which approximately $101 million was stolen from the Bank of Bangladesh through compromising the SWIFT Alliance Access server software with malware. Since the NY FED is a global monitor of the SWIFT system, the Committee requested information about the NY Fed's cybersecurity oversight of SWIFT as it related to the Bangladesh heist, and cybersecurity weaknesses in the system at large. While the Committee has received some of the material it has requested and reviewed more *in camera*, responsive items remain outstanding and we welcome your assistance in obtaining and reviewing this information.

Thank you again for your letter and for your offer to join the Majority in its oversight efforts. Please do not hesitate to contact us at any time to discuss these or other issues. In the meantime, Committee Majority staff will reach out to your offices to discuss next steps.

Sincerely,

Lamar Smith

Lamar Smith
Chair
Committee on Science, Space,
and Technology



3/13/2017 Beyer Denounces Science Committee Republicans' Clinton Subpoenas : Congressman Don Beyer

News

- Press Releases
- In the News
- Opinion Pieces
- Photos
- Video
- Press Kit

Quick Links

Contact Me

Email Sign Up

Enter your Email Address

Congressman Don...
Like Page

Congressman Don Beyer
1 hr

POTUS' latest attack on federal workers would have dangerous effects on protections for clean air, clean water, public health, veterans' services, and so much more. We will fight tooth and nail against these cuts.

Latest Tweets

@RepDonBeyer - White supremacy has no place in the United States Congress. Rep. King should apologize, and

Press Releases

Beyer Denounces Science Committee Republicans' Clinton Subpoenas

Washington, August 22, 2016 | 0 comments

Congressman Don Beyer, the Ranking Member on the House Science Subcommittee for Oversight, strongly condemned the Committee's issuance of subpoenas to private server companies related to Sec. Clinton's email server.

"This is a wasteful use of taxpayer dollars by Chairman Smith and the Science Committee Republicans for blatantly partisan purposes," **said Rep. Beyer**. "The House Science Committee must focus on its role promoting science and ensuring that America is the global leader in research and development, rather than scoring cheap political points with the umpteenth investigation of this issue."

Sec. Clinton's servers have already been thoroughly investigated by the House Benghazi Committee, which expended millions of taxpayer dollars on an inquiry which revealed no evidence of illegal activity.

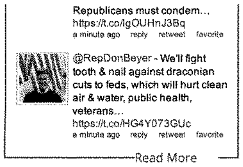
1 Comment Sort by **Oldest**

Add a comment...

Catherine Zumbrook Zeger
That's right Congress, get back to work or your time is going to come. We, the voting public, are going to fix you!
Like · Reply · 1 · Aug 23, 2016 7:08am

Facebook Comments Plugin

https://beyer.house.gov/news/documentsingle.aspx?DocumentID=407 1/2



Republicans must condem…
https://t.co/lgOUHnJ3Bq
a minute ago reply retweet favorite

@RepDonBeyer - We'll fight tooth & nail against draconian cuts to feds, which will hurt clean air & water, public health, veterans…
https://t.co/HG4Y073GUc
a minute ago reply retweet favorite

Read More

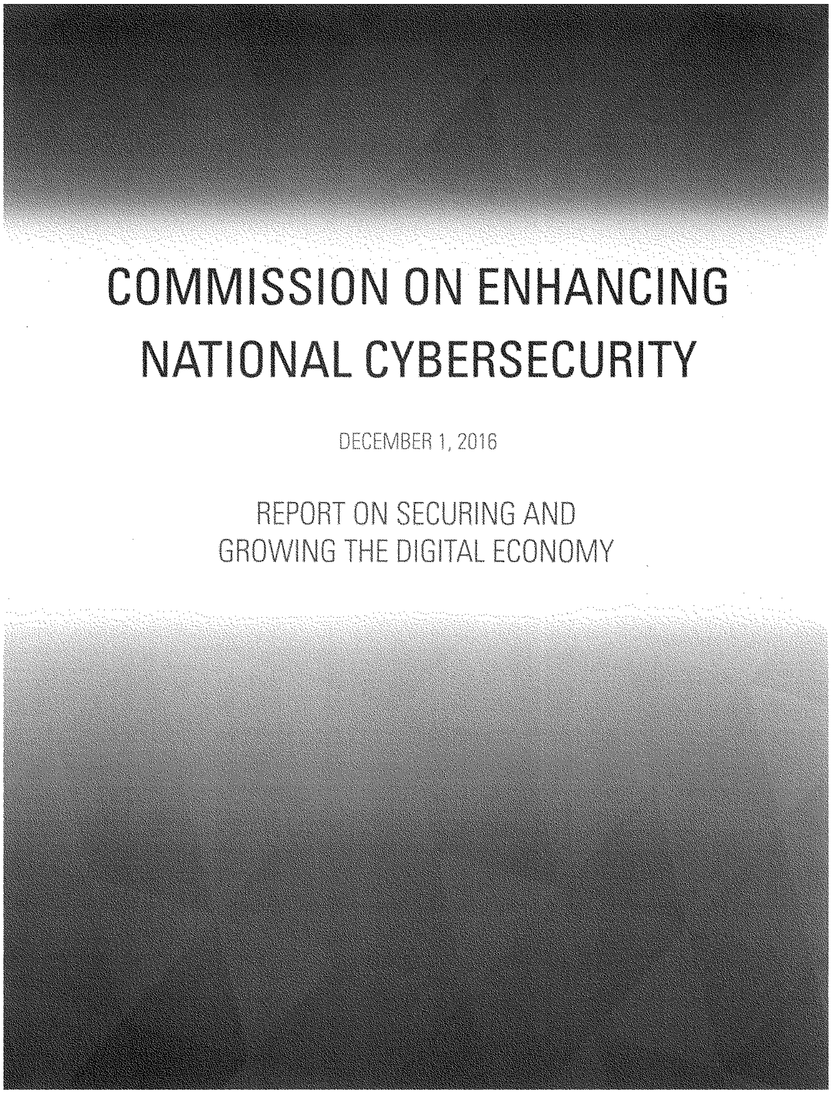
Chairwoman Barbara Comstock submitted a video by Domanique Jordan with WJLA, published on Monday, October 31, 2016.

Summary: 10/31/2016 — Rep. Don Beyer (D-Va.) and Michael Rubino, chairman of the Trump campaign in Virginia, looks at Hillary emails, 2016 campaign, lame duck session and possible House investigations.

"New Scrutiny of Clinton Emails" can be found here:

http://wjla.com/news/news-talk/new-scrutiny-of-clinton-emails

Reports provided to Members during hearing



COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY

Executive Summary

Recognizing the extraordinary benefit interconnected technologies bring to our digital economy—and equally mindful of the accompanying challenges posed by threats to the security of the cyber landscape—President Obama established this Commission on Enhancing National Cybersecurity. He directed the Commission to assess the state of our nation's cybersecurity, and he charged this group with developing actionable recommendations for securing the digital economy. The President asked that this enhanced cybersecurity be achieved while at the same time protecting privacy, ensuring public safety and economic and national security, and fostering the discovery and development of new technical solutions.

The interconnectedness and openness made possible by the Internet and broader digital ecosystem create unparalleled value for society. But these same qualities make securing today's cyber landscape difficult. As the world becomes more immersed in and dependent on the information revolution, the pace of intrusions, disruptions, manipulations, and thefts also quickens. Technological advancement is outpacing security and will continue to do so unless we change how we approach and implement cybersecurity strategies and practices. Recent attacks in which everyday consumer devices were compromised for malicious use have made it abundantly clear that we now live in a much more interdependent world. The once-bright line between what is critical infrastructure and everything else becomes more blurred by the day.

While the threats are real, we must keep a balanced perspective. We should be able to reconcile security with innovation and ease of use. The Internet is one of the most powerful engines for social change and economic prosperity. We need to preserve those qualities while hardening it and making it more resilient against attack and misuse. Changes in policies, technologies, and practices must build on the work begun by the private sector and government, especially over the past several years, to address these issues.

Our commitment to cybersecurity must match our commitment to innovation. If our digital economy is to thrive, it must be secure. That means that every enterprise in our society—large and small companies, government at all levels, educational institutions, and individuals—must be more purposefully and effectively engaged in addressing cyber risks. They must also have greater accountability and responsibility for their own security, which, as we now know all too well, directly impacts the cybersecurity of our country.

From its inception, this nonpartisan Commission developed a report directed both to President Obama and to the President-elect. The Commissioners, who possess a range of expertise relating to cybersecurity, reviewed past reports and consulted with technical and policy experts. The Commission held public hearings, issued an open solicitation for input, and also invited the public at large to share facts and views. It devoted attention to areas including critical infrastructure, the Internet of Things (IoT), research and development (R&D), public awareness and education, governance, workforce, state and local issues, identity management and authentication, insurance, international issues and the role of small and medium-sized businesses.

The Commission identified and considered broader trends affecting each of these topics, notably the convergence of information technologies and physical systems, risk management, privacy and trust, global versus national realms of influence and controls, the effectiveness of free markets versus regulatory regimes and solutions, legal and liability considerations, the importance and difficulty of developing meaningful metrics for cybersecurity, automated technology–based cybersecurity approaches, and consumer responsibilities. In these areas and others, the Commissioners examined what is working well, where the challenges exist, and what needs to be done to incentivize and cultivate a culture of cybersecurity in the public and private sectors.

There was much to readily agree on, including the growing convergence and interdependencies of our increasingly connected world; the need for greater awareness, education, and active stakeholder engagement in all aspects of cybersecurity, from developers and service providers to policy makers and consumers; the ways in which small- and medium-sized companies face additional pressures and limitations in addressing cybersecurity and the importance of remedying that situation, especially in light of their role in the supply chain; and the need, from both operational and mission perspectives, to clarify the federal government's roles and responsibilities.

It was also evident that most solutions require joint public–private action. Every enterprise in our society—large and small companies, government at all levels, educational institutions, and individuals—must be more purposefully and effectively engaged in addressing cyber risks. They must be equipped to understand the role they play in their own security and how their actions directly impact the cybersecurity of the nation more broadly.

Other areas required more consideration:

- how best to incentivize appropriate cybersecurity behaviors and actions and how to determine if or when requirements are called for;
- who should lead in developing some of the most urgently needed standards and how best to assess whether those standards are being met;
- what is the feasibility of better informing consumers, for example, through labeling and rating systems;
- which kinds of research and development efforts are most needed and at what cost;
- how to project the right number of new cybersecurity professionals our economy needs and how to choose among different approaches for attracting and training the workforce at all levels; and,
- what the roles and relationships of senior federal officials should be and how best to ensure that they not only have the right authorities but are empowered to take the appropriate actions.

From these discussions, some firm conclusions emerged. Partnerships—between countries, between the national government and the states, between governments at all levels and the private sector—are a powerful tool for encouraging the technology, policies, and practices we need to secure and grow the digital economy. The Commission asserts that the joint collaboration between the public and private sectors before, during, and after a cyber event must be strengthened. When it comes to cybersecurity, organizations cannot operate in isolation.

Resilience must be a core component of any cybersecurity strategy; today's dynamic cyber threat environment demands a risk management approach for responding to and recovering from an attack.

After building on those points of agreement and identifying foundational principles, the Commissioners organized their findings into six major imperatives, which together contain a total of 16 recommendations and 53 associated action items.

The imperatives are:

1. Protect, defend, and secure today's information infrastructure and digital networks.
2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3. Prepare consumers to thrive in a digital age.
4. Build cybersecurity workforce capabilities.
5. Better equip government to function effectively and securely in the digital age.
6. Ensure an open, fair, competitive, and secure global digital economy.

A table detailing these imperatives and their associated recommendations and action items is included in Appendix 1. The groupings should not be viewed as distinct and isolated categories; indeed, a number of recommendations apply to more than the imperative under which they first appear. The text notes when action items are particularly relevant to other imperatives. This structure reflects the interdependent nature of our digital economy, where steps taken to improve the cybersecurity of one enterprise can meaningfully improve the posture and preparedness of others.

Each recommendation is designed to have a major impact, and each action item is meant as a concrete step toward achieving that impact. Many require a commitment of financial resources far above the level we see today. Some are directed at government, some at the private sector, and many at both. Some call for entirely new initiatives, while others call for building on promising efforts currently under way.

Acknowledging the urgency of the challenges facing our nation, the Commission determined that most recommendations can and should begin in the near term, with many meriting action within the first 100 days of the new Administration. All of these recommendations and actions highlight the need for the private sector, government, and American public to recognize cybersecurity as an integral part of our welfare with serious implications for our country's national and economic security and our prospects to maintain a free and open society.

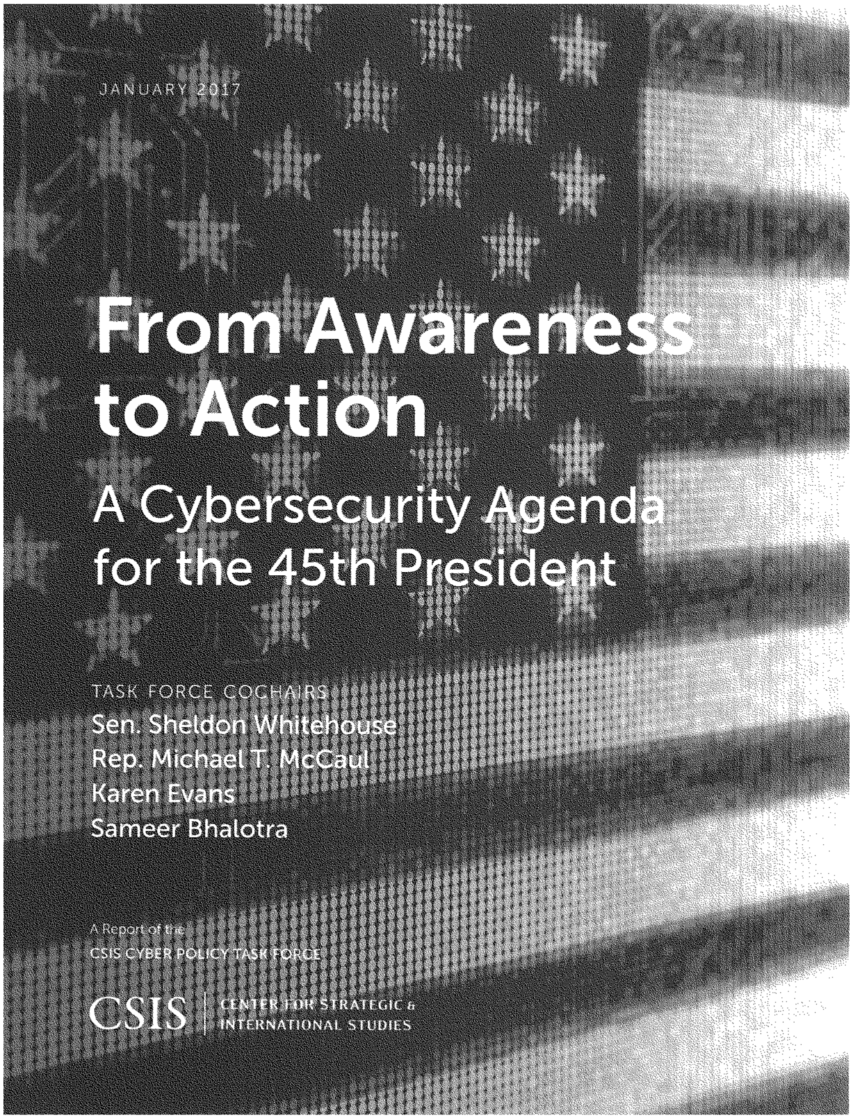
Report 1:

Title: *Report on Securing and Growing the Digital Economy*

Published By: Commission on Enhancing National Cybersecurity

Date: December 1, 2016

https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf



JANUARY 2017

From Awareness to Action

A Cybersecurity Agenda for the 45th President

TASK FORCE COCHAIRS
Sen. Sheldon Whitehouse
Rep. Michael T. McCaul
Karen Evans
Sameer Bhalotra

A Report of the
CSIS CYBER POLICY TASK FORCE

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JANUARY 2017

From Awareness to Action

A Cybersecurity Agenda for the 45th President

A Report of the CSIS Cyber Policy Task Force

TASK FORCE COCHAIRS
Sen. Sheldon Whitehouse
Rep. Michael T. McCaul
Karen Evans
Sameer Bhalotra

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by general support to CSIS. No direct sponsorship has contributed to its publication.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Contents

01

Introduction

This report lays out specific recommendations for the next administration's cybersecurity policy. It identifies the policies, organizational improvements, and resources needed for this. It builds on the 2009 Commission on Cybersecurity for the 44th Presidency, a foundational document for creating a strategic approach to cybersecurity. In the eight years since that report was published, there has been much activity, but despite an exponential increase in attention to cybersecurity, we are still at risk and there is much for the next administration to do.

We are still at risk because the intricate structure of networks we have built is based on technologies that are inherently vulnerable. In addition, the enforcement of laws in cyberspace is intrinsically difficult, and some countries refuse to cooperate in prosecuting cybercriminals. Nations are also unwilling to forsake the benefits of cyber espionage or military cyber operations. Domestically, the conflicting political imperatives that lead to stalemate for many initiatives also slow progress on cybersecurity.

The goals of cybersecurity strategy remain the same: to create a secure and stable digital environment that supports continued economic growth while protecting personal freedoms and national security. The requirements to implement that strategy also remain the same: central direction and leadership from the White House to create and implement a comprehensive and coordinated approach to policy, organization, and resourcing. These goals and requirements set the objectives, but cybersecurity is no longer a "greenfield" for policy development. The next administration will inherit a work in progress. Our starting point is that it should build on and improve what has already been done. In this, it faces five major issues:

1. It must decide on a new international strategy to account for a very different and dangerous global security environment.
2. It must make a greater effort to reduce and control cyber crime.
3. It must accelerate efforts to secure critical infrastructures and services and improve "cyber hygiene" across economic sectors. As part of this, it must develop a new approach to securing government agencies and services and improve authentication of identity.
4. It must identify where federal involvement in resource issues such as research or workforce development is necessary, and where such efforts are best left to the private sector.
5. Finally, it must consider how to organize the United States to defend cyberspace. Clarifying the role of the Department of Homeland Security (DHS) is crucial, and the new administration must either strengthen DHS or create a new cybersecurity agency.

Two principles should guide cybersecurity: creating consequences for foreign actors and incentivizing domestic actors to provide better cybersecurity. The creation of consequences for cyber crime, espionage, and cyber attack and making these consequences clear to malicious actors is the most effective ways to reduce cyber risk (especially if done in partnerships with like-minded nations). Since risk cannot be completely eliminated, better cybersecurity also requires holding key critical infrastructures to high standards while incentivizing basic improvements in the general population of online actors. These tasks will require some additional resources, but resources are not the major obstacle to better cybersecurity; the major obstacle has been and remains confusion over the role of government and a lack of will.

After eight years, there is far greater awareness of risk, the United States is better prepared, but from an attacker's perspective, cyberspace remains an area of almost boundless opportunity. Cyber crime and espionage remain omnipresent, but powerful opponents have used cyber attack as a coercive tool against the United States and its interests and there are new threats to the integrity of sensitive. While we lose billions of dollars to weak cybersecurity, we have gained trillions in income through the growth of Internet-enabled products and services, but there is a growing sense of danger and for the first time, people and companies are asking if the Internet is safe to use. The trend line is not going in the right direction.

Changing this will not be easy. The contours of a national policy are more complex than eight years ago and must take into account the uneven progress made by the current administration in the face of intractable foreign opponents and domestic political constraints. No network can be made entirely secure against advanced opponents and there is no technological "silver bullet." This means that if the pace of federal efforts slows, the United States will become more vulnerable—our attackers (an increasingly opportunistic collection of nation-states, criminals, and hacktivists) are not sitting still and have grown in skill and number since 2009. Even this president, who cared deeply about cybersecurity and pushed his administration to act, faced difficult problems in changing things. It will help set the stage by talking about why this was so.

Some Things to Avoid

The Obama administration made significant progress but suffered from two conceptual problems in its cybersecurity efforts. The first was a belief that the private sector would spontaneously generate the solutions needed for cybersecurity and minimize the need for government action. The obvious counter to this is that our problems haven't been solved. There is no technological solution to the problem of cybersecurity, at least any time soon, so turning to technologists was unproductive. The larger national debate over the role of government made it difficult to balance public and private-sector responsibility and created a sense of hesitancy, even timidity, in executive branch actions.

The second was a misunderstanding of how the federal government works. All White Houses tend to float above the bureaucracy, but this one compounded the problem with its desire to bring high-profile business executives into government. These efforts ran counter to what is needed to manage a complex bureaucracy where greatly differing rules, relationships, and procedures determine the success of any initiative. Unlike the private sector, government decisionmaking is more collective, shaped by external pressures both bureaucratic and political, and rife with assorted strictures on resources and personnel.

The point that many observers miss is that there is no such thing as the "government." It is not a single entity, but a conglomerate of Cabinet departments and agencies, with different missions, authorities, workforces, and leadership. Previous presidents have tried to cast themselves as CEOs. However, the government is not a corporation and creating a host of White House functionaries modeled on "C-suite" officers found in corporate organizations is ineffective because they lack resources and authority. These White House dignitaries are only ornamental. While the government can learn much from corporate experience, particularly in the delivery of services, the United States needs a different structure than a corporation if it is to effectively manage policy and programs. These White House CTOs CISOs, CIOs need to be pruned.

The next administration would also be well advised to move away from outdated ideas. Statements about strengthening public-private partnerships, information sharing, or innovation leads to policy dead ends. Many date back to the 1990s. Once-powerful ideas have been transformed into clichés. Others have become excuses for inaction. Too often, the cybersecurity debate has been shaped by a desire to prevent regulation. The next administration's task is to draft and implement policies that fit today's cyber environment and produce measurable improvements in the performance of companies and government agencies.

The temptation for grand national initiatives should be avoided, as these usually fall flat. The National Strategy for Trusted Identities in Cyberspace (NSTIC), for example, achieved little. The lesson is that initiatives must be carefully attuned to market forces (there are few takers for a product or service for which there is no demand or for which there are commercial alternatives), must have congressional endorsement, and are best if not run from the White House, which lacks the infrastructure needed for implementation.

The next administration has a sound foundation to build on if it so chooses. Cybersecurity has gone from a niche concern of a few specialists to being the focus of a well-intended if not always well- informed global discussion. The cybersecurity market has become a multibillion-dollar source for innovation and services to secure vulnerable networks, and the issue now gets far more senior attention in both companies and governments than it did eight years ago. There has been ongoing work to build both international cooperation and a sector-specific approach to critical infrastructure protection.

A Different and More Difficult Environment for Cybersecurity

The environment for cybersecurity has changed since 2009, and administration policies need to change with it, particularly for international engagement. There has been an erosion of American influence and the arrival of assertive challengers. Russia's use of cyber as an instrument of state power is impressive and worrying. Significant incidents—such as North Korea's and Iran's hacks against Sony and the Sands Casino, and the Chinese hack of the Office of Personnel Management (OPM)—reflect a growing willingness to use cyber tools against us.

A deteriorating situation for international security means that the next administration will face continued losses from cyber crime and espionage, threats to personal information and company data, the possibility of politically coercive cyber acts, and the risk of disruption or attack on critical infrastructure. We face dynamic state opponents who have developed the capabilities needed for cyber attack and who are testing the limits of action in cyberspace. They use the Internet to challenge the United States and create digital coercion. North Korea, Russia, Iran, and China have all tested American cyber defenses and found them wanting.

While the Obama administration tried with some success to reestablish redlines after the Sony hack, our cyber opponents have found ways around American deterrence as it is currently implemented. Few companies or agencies can prevent, or even detect, efforts by our most advanced opponents to gain access to their networks. At the same time, Russian active measures in cyberspace show that vulnerabilities can be exploited for more than the theft of data.

The contours of cyber espionage have changed. The 2015 Xi-Obama Summit agreement on commercial cyber espionage seems to have reduced Chinese commercial spying, but its political and military espionage is unabated, as a broader range of actors have acquired and use cyber espionage tools against the United States. Our experience with China shows that opponent behavior can be changed and the risk environment reshaped by U.S. actions.

The 2013 leaks by Edward Snowden also changed the cybersecurity landscape. The legitimacy of U.S. leadership in cyberspace was damaged by Snowden, and a lack of a dynamic American response accelerated demands for increased sovereignty and security at the expense of U.S. companies and the multi-stakeholder governance model. The leaks increased tensions over privacy and accelerated the trend for countries to assert sovereign control over national networks. This is not "Balkanization" of the Internet, but the gradual extension into cyberspace of national rules for privacy, security, and content. This extension of sovereign control, if done in an uncoordinated fashion, will harm the creation and use of online products and services in all countries.

Dealing with Foreign Opponents

The key to a cybersecurity strategy that moves beyond a defense of individual networks lies with changing the behavior of hostile states. This requires norms for responsible state and company behavior, building cybercrime cooperation, and shaping opponent behavior through interaction and consequences. Changing the behavior of our opponents, state and nonstate, will require a more serious and sustained effort at senior levels than anything we have seen to date.

Our most dangerous attackers must be dissuaded from going after American targets. However, this is not "classic" deterrence that relies on threats of military retaliation. A strategic approach to cybersecurity for the United States must rely on all tools of government to persuade and coerce. In this, the military may play only a supporting role as we employ the full range of private and public-sector power—including innovation, economic influence, sanctions, indictments, and other countermeasures against opponents who have spent years devising strategies to exploit our vulnerabilities and have been largely unimpeded in doing so.

In 2009, our assumption was that global agreement on norms for responsible state behavior in cyberspace (accompanied by confidence-building measures) would increase stability and reduce risk. The creation of norms for responsible state behavior is an essential part of the U.S. international cybersecurity strategy. That strategy needs to be reconsidered in light of the changed international security environment. Norms are not a panacea and by themselves, will not change opponent behavior sufficiently to reduce risk.

The open questions are to determine what norms of responsible state behavior can be effective and whether agreement on norms with opponents is possible. The utility of norms needs to be reassessed in light of increased hostility by our leading opponents. We also need to reconsider the usefulness of voluntary norms—the U.S. approach has been to secure voluntary adherence to general norms (using the UN Group of Government Experts as the primary vehicle for this) and embed cybersecurity in the larger framework of international law and state practice, but it is time to consider binding agreements just as we used binding agreements on arms in the Cold War.

There is little support now for such agreements. The usefulness of a formal agreement, as with the utility of voluntary norms, depends on the likelihood that others will comply with them. Verification of agreements for cybersecurity is more difficult than other areas, but it is not impossible. The truly difficult issue is not verification, but deciding what to do if we discover cheating. Developing a range of consequences for cheating or for cyber attack and making these consequences known to the world are as important as norms or agreements for reshaping opponent behavior.

What Does the Next Administration Need to Address?

We can bring clarity to the task of cybersecurity if we start by assessing what actions create risk. There are three categories of actions that create risk in cyberspace: attack, espionage, and crime. Espionage and crime are routine occurrences; true attacks are rare. The high frequency of espionage and cyber crime reflects the generally weak defenses of most networks and the ease with which they can be penetrated. Espionage is conducted largely by states or their proxies, although the lines between espionage and crime blur when a state actor steals data for commercial purposes.

The line between attack and espionage has also blurred, as America's principal cyber opponents—Russia, China, Iran, and North Korea—use cyber actions against domestic U.S. targets for coercive effect. These actions fall below the thresholds for the use of force derived from international law and practice but their intent is to damage the political independence of the United States. Incidents like Sony, Sands, GitHub, and the Democratic National Committee (DNC) hacks are a signal failure of what passes for deterrence or defense in cyberspace and an indicator of how weak network defense remains. These coercive actions have been carried out by state entities or their proxies, occasionally with the support of antiestablishment entities like WikiLeaks.

The prevalence of cyber crime reflects a larger rejection of international law and practice by our main opponents. Earlier work estimated that cyber crime and the theft of intellectual property cost the United States perhaps $100 billion annually, with global costs ranging between $450 billion and $600 billion. The unwillingness to accept the rule of law and to enforce both domestic and internal law against those who engage in cyber crime is one of the biggest challenges for strategy.

Nor should we tolerate the continued theft of military and advanced technology from the United States and its allies. For some areas, any improvement in cyber defense comes too late, as information related to stealth, nuclear weapons, fighter aircraft design, and other advance technologies were taken by hostile powers more than a decade ago. And while there have been good advances in the network protections of leading defense contractors, this has only encouraged opponents to become more inventive and more persistent. To argue that such spying is normal state practice and "we do it too" is inane. Even if China, Russia, and the United States were comparable in their adherence to human rights—and they are not—one great power does not let another "disrespect" it without penalty unless it is in decline. We cannot expect to stop espionage, but we can make it less effective by hardening defenses, and less frequent by increasing risk to opponents.

The Risk of Cyber Attack

Cyber crime and espionage cost the United States (and the global economy) billions of dollars every year, but the area of greatest risk involves attack—cyber actions whose effect is the equivalent of the use of force. There have been only a handful of such actions (accompanied by several incidents, such as the Iranian cyber attack on Aramco, that fall into a gray area between coercion and force). Currently, the only actors capable of the most damaging attack are nation states. The assessment of both American and foreign intelligence agencies is that nonstate actors do not possess such capabilities and are unlikely to acquire them in the next few years.

Cyber actions are already part of inter-state conflict and the risk of attack has increased, as flashpoints in our relations with leading opponents raise the possibility of armed clashes—over the South China Sea, the Baltics, or the Middle East. The potential for conflict, miscalculation, and escalation forms the backdrop to assessing the risk of cyber attack. The most likely targets for actual attack remain critical infrastructures—chief among them energy, telecommunications, finance, government services, and transportation.

Defending these sectors is a high priority for cybersecurity strategy and programs, and the United States has not done enough to ensure survivability, resilience, and restoration of services. What this means is that a more comprehensive approach to cybersecurity in critical infrastructures is essential. We need a "strategic" approach that prioritizes risk by estimating the value of a target to our opponents. Targets where a successful cyber attack could have mass effect, or a strategic effect on military and economic capabilities, need to be a priority for stronger defenses. While there are basic standards for cybersecurity that every company should meet, a more nuanced approach would set the goal of developing sector-specific standards and policies that ensure the continued delivery of critical services by these key sectors.

We can take steps to reduce risk by changing company and agency behavior through a mix of market and government incentives, but we need to take a pragmatic view of the timing and cost of various incentives. Market incentives, such as insurance, will improve cybersecurity, but more slowly than required for some high-value targets in a period of increasing risk. If we look at automobile or fire insurance, it took decades for price signals and incentives to play out and produce safety, and there was often an interplay with Congress and regulatory agencies that is inadequate when it comes to cybersecurity. While these kinds of incentives are valuable and will make a long-term contribution to cybersecurity, we cannot afford to wait decades for national defense. In all three instances of malicious cyber action—crime, espionage, attack—an effective prescription for policy must include the hardening of networks and establishing clearer understanding with opponents about redlines and consequences in cyberspace. This administration had made some progress, but the results vary among sectors and critical infrastructure remains a vulnerability the next president needs to address.

02

Recommendations for the Next Administration

The starting point for a discussion of cybersecurity policy is to ask, did this administration get it right? The answer depends on how we define "right." In terms of politics, it exceeded the art of the possible, largely through the use of executive authorities. In bureaucratic terms, it took an inchoate department structure and gave it a degree of order. In terms of capabilities, the record is mixed. Cyber Command has become a functional command, DHS is better, and the FBI is more than adequate. However, despite progress, advanced attackers can still penetrate most American networks.

The next administration is inheriting a going enterprise. This means that recommendations require a high degree of specificity and impenetrability. We do not need to start over, nor do we need broad, dramatic (and unworkable) initiatives, but much work remains to be done. What the next administration will inherit will be shaped by what this administration has done. In our discussion, we looked for what the priorities of the next administration should be and how it can best use the tools available to the executive branch to manage risk and improve cybersecurity.

This effort involved two groups—one on the West Coast and one on the East Coast that developed complementary recommendations on cybersecurity policy. This introduction does not discuss in detail every recommendation that the two groups developed. Some, for example, are aimed at best practices for business. These recommendations do not require presidential action but should form part of the principles that guide White House statements and decisions on cybersecurity. The task force's two groups generated over 80 pages of working papers and 220 specific recommendations. (The papers and recommendation are available online.) The most salient recommendations are summarized below, grouped into three categories: policy, organization, and resources.

1. Policy Recommendations

Revise the International Cybersecurity Strategy

The 2009 CSIS Report advocated a comprehensive approach to international cybersecurity using all the tools of national power. The central points included developing norms and confidence-building measures and finding ways to make deterrence effective. There has been progress in implementing these recommendations, but while the goals underpinning recommendations remain sound, the world is a very different place than it was in 2009, much more conflictual and much more dependent on cyberspace. There have been important political changes as well, with the 2013 recognition that international law, the UN charter, and national sovereignty all apply to cyberspace. The 2011 international strategy needs to be replaced to better fit a different world.

The next president needs to make key decisions on negotiations, the international framework for stability in cyberspace, deterrence and response, and law enforcement cooperation. These are the areas of greatest challenge, but the single greatest challenge may be in deciding how to engage with Russia and China, our most powerful and active opponents in cyberspace.

Take a New Approach to Building Agreement on International Stability

The next president needs to address two major questions on the direction of international cybersecurity: Is it time to consider a more formal approach to building security and stability in cyberspace? And to what extent should an expanded or even continued efforts to build focus on agreement among likeminded states.

There has been some progress on getting agreement on norms and confidence-building measures, but this approach may be of declining utility. The United States needs a new strategy for better coordination among likeminded nations, for engaging "swing states" like Brazil and India on cybersecurity issues, and a more persuasive narrative for a global audience.

The next president will need to decide when it is worth pursuing agreements that require global support and those where agreement is only possible among like-minded nations. Measures focused on reducing the risk of escalation or misunderstand will appeal to Russia and China, who fear America power in cyberspace and the domestic political threat the Internet creates for them. Measures that define responsible behavior to include support for human rights and constraints on cyber crime will not appeal to them. The United States will need a two-track strategy, agreeing on norms with likeminded nations while pursing risk-reduction measures with the authoritarians.

Expand Deterrence and Create Consequences

The 2009 Report called for the United States to develop new strategies to deter cyber attack. While there have been no cyber attacks against the United States that produced physical destruction or casualties, there have been immense numbers of incidents involving cyber espionage and cyber crime, and, in the last year, several troubling efforts at political coercion. While we have not succeeded in deterring these actions, they provide useful lessons on how deterrence might be strengthened.

The most important lesson is that deterrence cannot rely solely on the use or threat to use military force. The most effective deterrent actions were the threat of sanctions or indictments. The combination of indictments and the threat of sanctions led China to agree to end commercial espionage. In international law these would be called "countermeasures," retaliatory actions that do not involve the use of force. In arms control parlance, the United States would benefit from "populating all the rungs of the deterrence ladder" with the appropriate potential responses and then communicating them to opponents.

Doing this requires defining a proportional response. For cyber crime (see below) this will mean improved prosecution and conviction rates. For espionage and coercive actions (like Sony), the

United States will need to make greater use of threats to impose sanctions or indict. Our one caveat here is that even with an improved deterrent policy, including a clearer declaratory policy and a more complete range of response options, some opponents will not be deterred from some actions. This argues for improved cyber defenses, but it also raises the larger problem of relations with Russia and China. Reducing the risk of cyber crime, cyber espionage, or coercive acts by these nations will need to be part of a larger bilateral strategy.

An obvious candidate for replacement is the verbose and vague declaratory policy in the 2011 strategy. Declaratory policy is a crucial part of a deterrent strategy and a lack of clarity diminishes its effectiveness.

Take a More Assertive Approach to Combat Cyber Crime

Cyber crime is transborder and transnational, making international cooperation essential for effective prosecution. Existing mechanisms for this cooperation are, however, outdated. One dilemma is that many countries still do not have adequate cyber crime laws. The U.S. position is that the Budapest Convention on Cybercrime provides a sufficient legal framework for prosecuting cyber crime, and if nations would adopt the treaty, we would all be better off. In the 15 years since the convention was opened for signature, 50 countries have joined. More rapid progress is needed in winning global support. The fundamental problem is that key nations refuse to sign. Russia refuses to sign because Moscow benefits from cyber crime, and China, India, and Brazil refuse to sign because they were not involved in the original negotiations and see the convention as a fait accompli being forced upon them.

We need to break the stalemate on the Budapest Convention. We recommend two steps to do so: First, penalize in some way those countries that refuse to cooperate with law enforcement. Second, find a new negotiating vehicle that preserves the benefits of the convention but gives Brazil, India, and perhaps China a new negotiation that provides them with the opportunity to take their concerns into account. There will be objections that any reopening will undercut the convention, but the alternative is continued slow progress.

Penalties for the noncooperative could mirror the Financial Action Task Force (FATF) "blacklist" of noncooperative countries. Some will argue that such constraints run counter to the ideology of the Internet to be free and open, but one of the lessons of the last few years is that consequences have a powerful effect in changing behavior in cyberspace and in junction with a revitalized effort at deterrence, the next administration should create and publicize a portfolio of punitive responses for malicious cyber action.

Preserve Global Data Flows

One way to think about cybersecurity policy is that we are building the structure for a digital economy. The continuing growth in global data flows in both developed and emerging markets highlights the international nature of cybersecurity. This is another crucial change from 2009. Cybersecurity affects international data flows in two ways. The first, unsurprisingly, is to ensure that data and the networks that deliver them are secure. This will mean finding ways to ensure the integrity of the data, as malicious actors attempt to manipulate it for criminal or political purposes. The need for cybersecurity has become the rationale for imposing new and damaging restrictions on data flows. These are misguided efforts to improve security and privacy. They typically impose costs on the use of data and systems without reducing risk. As a consequence, the next administration will need to find cooperative approaches that ensure the free, secure flow of data and, as part of rethinking international strategy, this may require a discussion of rules (and perhaps institutions) for international cybersecurity, privacy, and digital trade.

Any effort should include agreement with likeminded countries on standards of privacy and civil liberties; choice-of-law rules that would apply in the absence of agreement on baseline standards; and a commitment by the United States to forgo unilateral extraterritorial data demands (conditioned on reciprocal forbearance by other nations). Efforts to improve the Mutual Legal Assistance Treaty (MLAT) process are an important part of building a more stable international environment for data flows. They should be accelerated and include an expansion of the existing negotiations and mutual recognition of legal process to other nations; and internal MLAT reform, speeding cooperative data flows that are not subject to the mutual recognition process. This must include a commitment of the requisite resources to be responsive to MLAT requests.

Data Protection, Privacy and Cybersecurity

Protecting the nation's cyber assets includes safeguarding sensitive personal information. Individuals frequently share facts about themselves online that they would not want made public, much less stolen by malicious actors. Organizations often do not understand the value of the data they hold and fail to protect it. Given the vulnerabilities and threats that exist in cyberspace, those who collect and hold data have greater responsibilities for cybersecurity. Additionally, with the increased global focus on data protection, more work is needed in the United States to clarify the value of personal data and measures that can be taken to protect it.

The next administration should include data protection as part of cybersecurity, starting with the principle for federal programs that "data belongs to the user." It can build on existing efforts, including the proposal for a Consumer Data Privacy Framework and Federal Trade Commission (FTC) efforts to enforce existing privacy policies. One improvement would be for the president to request the FTC to consolidate and strengthen its activities by establishing a Division of Data Protection, to provide expert advice on data protection and security. Another would be passage of national data breach legislation. A single standard would focus corporate data protection efforts on a single, well-understood regime and provide a long-awaited legislative vehicle for other major reforms.

The cybersecurity industry is developing sophisticated tools and services to protect networks. Traditional monitoring and perimeter defenses are being supplemented by advanced signature analysis, analytics that can detect anomalies associated with malware, and new approaches to multifactor authentication. These efforts may not involve personally identifiable information (PII) in the traditional sense but raise issues for protecting personal information while taking advantage of new cybersecurity technology. We recommend that the next president:

- Protect privacy in cybersecurity activities by developing with the private sector a set of principles and best practices that address commercial data collection and the expectation of privacy when physical and digital information is digitally mingled.

- Direct the National Institutes of Standards and Technology (NIST), working with the private sector, to update the definition of PII and develop a taxonomy of privacy-relevant data types to facilitate stronger data protection efforts.
- Direct NIST to develop a set of recommended data security standards and practices. This should include guidance on what data types to consider sensitive, as part of the effort to broaden the definition of personal data beyond the current legal definition of PII, and establish generally acceptable standards of care for that data.
- Direct agency chief information officers, chief privacy officers, and chief data officers to ensure "data" is addressed in their cybersecurity program.
- Instruct DHS to work with Congress and the National Governors Association to harmonize breach responses across states, leading to a national data breach law premised on best commercial practice and a regulatory framework under FTC authorities.
- Request that Congress amend the FTC Act to establish a Division of Data Protection.

Increased Transparency for Cyber Incidents

Much of the cybersecurity debate after 2012 was preoccupied with information sharing. The passage of the 2015 Cybersecurity Act ended this debate, but there was a clear sense that more needs to be done in two areas. The first is to break the gridlock over the release of classified information on cyber threats and attacks. Much of this information does not pose a risk to sources and methods if released, and a senior cybersecurity official must be empowered to order the release.

The second is to find ways to allow those who have experienced cyber attack to share, anonymously and without liability, the details of the incident. One common theme in our discussion was the difficulty of improving cybersecurity when those who have been hacked are unwilling to share information about the incident. The reasons for this are understandable—publicity about being hacked can damage revenue, stock price, reputation and brands. Incident reporting requires guarantees of anonymity and liability protection.

This could be modeled on the National Transportation Safety Board (NTSB), which investigates air crashes, or the Federal Aviation Authority's Aviation Safety Reporting System (ASRS), where there is a blanket prohibition against using submitted information for enforcement purposes. NASA (which administers the program for the Federal Aviation Administration) "deidentifies" the information (unless it involves criminal activity by the operator) before sharing it with other agencies. DHS or the Cyber Threat Information Integration Center (CTIIC) could manage a program, to create a clearinghouse that would make anonymized assessments and best practices available to information sharing organizations.

The Internet of Things

The Internet of Things (IOT) creates new problems for cybersecurity by introducing an immense number of connected, simple computing devices. The growth of the IOT means there will be unavoidable failures of hardware and software, and an unavoidable increase in opportunities for hackers. A move toward increased liability for IOT products is inevitable. Some IOT devices could inadequately protect sensitive data. Others could provide an opportunity to disrupt sensitive services or, in some instances, create the capability for mass disruption. Sensitivity of data and function should guide federal efforts, but absent federal intervention, standards will develop in divergent and potentially disruptive ways.

We recommend that the next administration (1) task NIST to collaborate with consumer and business groups to develop standards and principles for IOT security, (2) take a "sector-specific" approach to IOT security and the development of IOT resilience frameworks, and (3) use federal procurement standards to drive improvement and safeguard government functions. NIST should convene technical, operational, financial, legal, and public policy experts to define IOT security standards across a broad range of IOT architectures. The next administration should synthesize existing efforts and combine them to enhance the resilience of IOT. A publicly available IOT security-rating scheme could be modeled on National Highway Traffic Safety Administration crash tests.

Encryption Policy

Greater use of encryption improves cybersecurity across the board, but the kind of encryption and how it is implemented can have serious implications for national security. Any U.S policy and legal framework for encryption must take into account the global environment and the U.S. strategy for international cybersecurity. The change in administrations will allow a fresh start. The goal should be a policy that aligns individual and collective security and economic interests.

The president should develop a policy that supports the use of strong encryption for privacy and security while specifying the conditions and processes under which assistance from the private sector for lawful access to data can be required. While it is tempting to delegate this to market forces or action by other nations, the issue's complexity and the disparate factions make this an unlikely source of enduring alignment. The president should include in future budget submissions to the Congress sufficient resources for the FBI and the foreign intelligence agencies to develop new capabilities for execution of their missions.

In keeping with the trend to cloud-based applications and data storage accesses from mobile devices, the president should task NIST to work with encryption experts, technology providers, and Internet service providers to develop standards and methods for protecting applications and data in the cloud, and provide secure methods for data resiliency and recovery.

Ultimately, encryption policy requires a political decision on risk. Untrammeled use of encryption increases the risk from crime and terrorism, but societies may find this risk acceptable given the difficulty of imposing restrictions. No one in our groups believed that risk currently justifies restrictions. These recommendations are initial steps to help frame a larger debate and manage risk while the larger issues of privacy, security and innovation are weighed and debated.

Active Defense

Discussion of a stronger approach to dealing with cyber crime will need to consider "active defense." This is a contentious topic. The term itself has become associated with vigilantism, hack-back, and cyber privateers, things that threaten to create a destabilizing global free-for-all in cyberspace. Even if the United States authorized companies to take limited measures against cyber adversaries, these actions would remain illegal under foreign law, exposing U.S. companies to legal action. Another dilemma with much of the discussion of active defense is that it does not take opponent reaction and countermeasures into account, and active defense measures against advanced opponents is likely to result in retaliation.

This makes active defense at best a stopgap measure, intended to address companies' frustration over the seeming impunity of transborder criminals. Ultimately, progress requires stronger procedures for law enforcement cooperation, greater acceptance by all nations of their responsibilities, and, since that recognition may not be forthcoming anytime soon, penalties and incentivize to encourage better law enforcement cooperation among countries.

In the interim, the next administration should look for ways to assist companies to move beyond their traditional perimeter defenses. This would focus on identifying federal actions that could disrupt cyber criminals' business model or expanding the work of the Department of Justice (DOJ), Federal Communications Commission (FCC), and service providers against "botnets." Additionally, the administration could consider measures, carried out with the prior approval of federal law enforcement agencies (most likely requiring a warrant to enter a third-party network) to recover or delete stolen data stored on servers or networks under U.S. jurisdiction.

"Baseline" Cybersecurity, Critical Infrastructure, and the NIST Framework

Organizations, no matter their size, have an obligation to strengthen cybersecurity, not only to secure their businesses and data of their customers, but also for the sake of our interconnected digital society itself and the security of the broader digital ecosystem. Progress on cybersecurity requires organizations to improve baseline cybersecurity, the standard security measures and best practices needed to reduce cyber risk. Since 2008, significant progress has been made toward raising the bar for security of private entities. To improve baseline security, we recommend (1) improving organizational governance for cybersecurity, (2) improving cyber "hygiene," and (3) adopting measures that take the technology "lifecycle" into account (including improved measures for authentication of identity).

Critical infrastructure is the area of greatest risk from cyber attack. The most likely targets for attack include energy, telecommunications, government services, finance, and transportation. Defending these sectors is a high priority for cybersecurity strategy and programs. The February 2013 Executive Order for critical infrastructure protection adopted a voluntary, sector-specific approach, with individual regulatory agencies responsible for their sector rather than making DHS an "uber-regulator." These agencies, using their existing authorities, work to ensure that cybersecurity is a priority for the sectors they oversee. The executive order encourages independent agencies to adopt a similar approach. The centerpiece of the executive order is the NIST framework, which established general guidance on actions that companies can take to improve security. The president should continue to promote and, where appropriate, compel implementation of the cybersecurity framework.

Organizations should assess their own risk and compare it against their peers and determine whether they are investing appropriately given their risk tolerance and threat environments. The NIST Cybersecurity Framework is the starting point for these efforts. We should expect to amend the NIST framework in light of experience, but the priority is to implement the framework as it now exists. Existing regulations should be streamlined in accordance with the cybersecurity framework's risk-based approach. Agencies, industry groups and individual organizations should adopt the framework to their sector's needs.

Metrics provide essential information for guiding policy. The lack of measurements on adoption and effectiveness remains a problem for assessing the framework. NIST should be tasked to develop these metrics, working with the private sector. In doing this, NIST should publicize specific implementation examples and measurement tools that organizations can use to implement the framework. NIST should publicly report on the effectiveness and adoption rate of the framework every year.

Raise the Cost to Attackers

While cyber defense measures are important, it is time to raise the cost to the attacker through proportionate responses. Threats are real and growing beyond our ability to passively defend business and government networks. Traditional cybersecurity functions include the ability to protect, prevent, mitigate, respond, and recover, but other responses have been neglected. These include:

- Actions to impede the monetization of stolen data and credentials. This could include measures to increase uncertainty about the value of stolen credentials.
- Techniques to divert adversary resources toward defense and to paralyze their network infrastructure used for attacks.
- Accelerate the move to multifactor authentication, using existing authorities to reduce anonymity and improve attribution.
- Find better ways to counter and disrupt botnets, a growing risk as more IOT devices are connected to the Internet. This could be done by expanding the ability to seek civil injunctions for use against botnets and raising the penalties for using botnets against critical infrastructure, taking into account privacy concerns.
- Improve cyber hygiene by creating standards much like generally accepted accounting principles (GAAP) that would let companies and agencies measure performance.

The Military's Role in Cybersecurity

The next president will be the first to inherit a military force structure for cyberspace operations. It is currently charged with three missions: defend the military's networks and systems; provide offensive cyber support to regional military commands; and defend the nation from a cyber attack of significant consequences. One of the challenges the next president will have to consider is how military cyber forces can be used to defend U.S. critical infrastructure from a significant cyber attack. This will require decisions on thresholds for "significant attack," deconfliction of any Department of Defense (DOD) role with DHS and the FBI, and establishing priorities for cyber defense.

A series of proposed organizational changes in DOD give the next president the opportunity to strengthen the oversight of military planning in cyberspace and offensive cyber operations. Despite the common refrain that offense and defense are merely two sides of the same coin in cyberspace, the civilian oversight and coordination functions are sufficiently distinct to warrant a division of labor.

Regardless of whether the current administration separates Cyber Command from Strategic Command, the next administration should evaluate Cyber Command's authorities and ensure it can set its own requirements for acquisitions. It should also be authorized and resourced to acquire needed capabilities as rapidly as possible. The next president should assess how these forces are assigned and consider alternate constructs that may reflect the experience that comes with four years of building the cyber mission force.

The need for close partnerships between U.S. military cyber forces and the intelligence community cannot be overstated. For U.S. military forces to be able to prevent or preempt an adversary's offensive cyber operations against the United States, intelligence—no matter the type or source—is critical. Previous administrations have provided the resources and organizational flexibility to foster close collaboration between the intelligence and military cyber communities. For the next administration, the opportunity will be to streamline the speed at which information can be shared between intelligence and military communities, as well as from those communities to law enforcement and other agencies.

The role of DOD in cybersecurity was one of the most contentious issues the group considered. A small number of members felt that DOD should play an expanded and perhaps leading role in critical infrastructure protection. A large majority of members believed that this mission must be assigned to a civilian agency, not to DOD, nor given to a law enforcement agency such as the FBI. While recognizing that the National Security Agency (NSA), an element of DOD, has unrivaled skills, we believe that the best approach is to strengthen DHS, not to make it a "mini-NSA," and to focus its mission on mitigation of threats and attacks, not on retaliation, intelligence collection, or law enforcement.

NETGuard, the National Guard, and the Reserves

The National Guard and the Reserves can be useful supplements to our cybersecurity posture. The traditional inclination is to consider employing these forces in the aftermath of a cyber attack. However, the next administration should consider how the Guard and Reserves can be used in advance of a cyber attack to better protect critical assets before an incident occurs. The capability of National Guard units to operate across the range of state (Title 32) and federal (Title 10 and 50) authorities and the ability of the private sector to generate talent in citizen-soldiers makes the guard and reserves a cost-effective, high-value force.

DOD and state governors share control of the National Guard, and many governors are moving to use the National Guard to assist with cybersecurity incidents. DHS has been authorized to create Net Guard, which was envisioned to be a means to surge additional information technology (IT) and communications personnel to provide emergency support to government and private-sector entities providing essential services. Congress should amend how Net Guard efforts can be integrated with the National Guard and Reserve capabilities to prepare for and support responses to a large-scale cyber attack.

2. Organization

Streamline the White House

The next president should move quickly to appoint a new cybersecurity coordinator, and elevate the position to assistant to the president. The president should not undertake another lengthy policy review, as was done in 2009. The next president should also strengthen the apparatus within the White House for managing cybersecurity policy and operations. To this end, the special assistant to the president should be elevated to an assistant to the president; the Office of Management and Budget (OMB) should reinforce DHS efforts for federal agency cybersecurity; and CTIIC should be tasked to support the White House on strategic operational planning for cybersecurity.

Strengthen DHS

The United States is no longer the cutting edge when it comes to organizing for cybersecurity. Other nations are experimenting with more models that make cybersecurity the responsibility of a specialized agency reporting to the chief executive. While the creation of a cyber coordinator in the National Security Council (NSC) did much to reduce federal disorganization, there are still problems. To be fair, the United States is larger than most countries, with thousands of critical infrastructure companies and gigantic agencies, but no one would argue that there is no room for improvement.

There was some discussion in the group of transferring DHS cybersecurity responsibilities, particularly for critical infrastructure, to other agencies such as DOD or the FBI. The group felt this would be unwise. A cyber agency should be civilian to maximize cooperation with the private sector, which greatly prefers a civilian agency. The next president can build upon the 2010 memorandum of understanding between DHS and DOD, which clarified how the NSA can support DHS in its cybersecurity efforts and allows NSA's technical and intelligence capabilities to be used for homeland defense.

CSIS's 2009 report recommended the creation of a standalone cybersecurity agency (the model many other nations are adopting), but the Obama administration chose at the start to make DHS the focal point for the national cybersecurity effort. There were two problems with this. The administration did not clearly define DHS's cybersecurity mission and DHS did not have the capabilities it needed. The current leaders of DHS have done good work in transforming the agency, but crucial problems remain. The last few years have seen significant improvement, but to turn DHS into the real center of cybersecurity, the next president must take three steps.

1. Define and Focus the DHS Cyber Mission. A focused mission statement would read:

> The Department of Homeland Security's National Cybersecurity Agency will lead the national cyber defense to protect critical infrastructure and federal agencies, to mitigate the effect of cyber attacks, and to ensure public awareness of serious cyber threats.

This mission has three parts. First, building on Presidential Policy Directive (PPD)-41, which makes DHS the lead agency for "asset response activities," DHS must be able to mitigate major attacks, particularly on critical infrastructure. This means having personnel who can respond, repair and restore the victims of cyber attack. DHS cannot be a national fire department, respond to every incident (there are too many) but it needs deployable teams that can help restore critical services and prevent systemic collapse in critical sectors. Second, DHS, working with the NSC, OMB, and General Services Administration (GSA), must master its role of defending civilian agency networks, extending its success with continuous diagnostics and monitoring (CDM). Finally, DHS must build on its recent successes and become the hub of information sharing, not controlling but ensuring coordination and equity among firms and sectors. Information sharing is of limited value and it is something the private sector can do without much government help.

2. Make Cybersecurity an Independent, Operational Component at DHS. Cybersecurity at DHS needs to be an operational component agency like the Coast Guard or Customs and Border Patrol. We suggest the name "National Cybersecurity Agency." Focusing on cybersecurity means shedding some peripheral functions. The National Protection and Programs Directorate (NPPD) is responsible for cybersecurity but also currently manages the Federal Protective Service (FPS), the agency that provides guards for federal buildings. DHS has argued that FPS can play an important role in cybersecurity. FPS should be moved to another part of the agency.

NPPD is also responsible for the physical security of critical infrastructures. This is an important mission, but much less crucial than cybersecurity. Some argue that the growth of IOT means that the DHS cyber agency should focus on the "cyber-physical interface." Our discussion concluded that cybersecurity is a full-time job and the most important function DHS may have if it is to be more than a border security agency. If DHS is serious about cybersecurity, it should make it a core mission and remove peripheral activities.

3. Strengthen Other Key Agencies. DHS and DOD play key roles in cybersecurity, but so do the State Department, FBI, Commerce Department, and Intelligence Community. Changes at other organizations will let the United States exercise all instruments of national power against cyber threats. These include making the cyber coordinator at the State Department an ambassador-at-large and creating a new bureau for cyber and information issues. The secretary should not consolidate related activities on telecommunications, Internet freedom, and intelligence under the new bureau; these efforts are best carried out from their current locations.

The FBI is already reorganizing its cyber capabilities; these efforts should be accelerated by the next administration. The outstanding problem is that individuals, companies, and agencies often do not know who to engage when they are a victim of a cyber crime, and crimes involving some "cyber" aspect are increasing at an alarming rate. The FBI and Secret Service are very effective in dealing with significant events, but a host of smaller cyber crimes fall on local law enforcement agencies that are usually underfunded and understaffed. Existing efforts where the FBI works with local law enforcement to respond to cyber crime should receive increased resources and attention.

The Cyber Threat Information Integration Center, established under the Director of National Intelligence (DNI), needs an expanded role. The CTIIC should be developed to take on the same set of roles for cyber that the National Counterterrorism Center (NCTC) plays for counterterrorism and support the White House on strategic operational planning. Beyond its responsibilities for enabling intelligence sharing, the CTIIC should be responsible for developing and maintaining, under the direction of the National Security Council, plans for countering cyber threats, including developing red team scenarios and plans to address their findings.

Early in its tenure, the administration should issue a clear statement of roles and responsibilities for the DHS, FBI, DOD, and CTIIC to minimize the internecine struggles that occur at the beginning of a new administration. This statement should define how DOD will support DHS in its efforts to mitigate incidents, how DHS should support the FBI in investigation, and when the "handoff" from DHS to DOD should take place in response to foreign actors. PPD-41, which identifies the lead agencies for the different takes in responding to a cyber incident, is a useful precedent for this, but it does not go far enough. A comprehensive statement, perhaps in the form of an executive order, could get a new administration off to a fast start.

Use GAO to Provide Independent Congressional Review of Federal Agency Cybersecurity

The current system of oversight is not achieving the results needed in order to improve cybersecurity and reduce the number of breaches occurring within the federal government. The current arrangement continues to perpetuate security by checklist. Establishing a new review capability within the GAO would allow for an independent congressional review for federal agency cybersecurity. With new authorities and resources, GAO would be able to provide robust, continuous evaluation of agency cybersecurity, using penetration testing and similar measures.

Streamline Congressional Oversight

A discussion of federal organization would be incomplete without a discussion of congressional committee jurisdiction. DHS has far too many committees—more than 80—exercising jurisdiction. Other committees have taken up specific aspects of cybersecurity, such as law enforcement and defense. Although it is important to streamline congressional jurisdiction over cybersecurity and homeland security, this responsibility does not lie with the president, but with the speaker of the House, the majority leader of the Senate, and the Rules Committees. The absence of specific jurisdictional tasking from congressional leadership limits congressional oversight, but assigning jurisdiction is a politically thorny issue whose pursuit should not detract from the creation and implementation of measures that provide immediate effect. This should be a long-term objective for improvement.

3. Resources

Expand Zero Vulnerabilities Programs and Clarify Their Legality

The risk that software vulnerabilities pose to critical information systems has grown dramatically. Software vulnerabilities have become commodities; they are traded on the market, offering opportunities for the highest bidder to gain unauthorized access to critical systems. Exacerbating the issue, many of these critical systems use components that are composed of open-source software—code that is not owned by any one responsible vendor or party—and thus often go unmaintained where vulnerabilities may go unnoticed and unpatched for years.

The exchange of information about vulnerabilities has grown into a complex and sometimes illicit marketplace. Today, one of our most promising efforts to patch vulnerabilities in critical software has been incentive programs for security researchers to find and fix bugs. These so-called "bug bounty" programs, in which companies pay researchers in exchange for information about vulnerabilities, have become a key tool to secure the infrastructure we all use.

However, there remains great legal uncertainty about whether or not security research is lawful. Researchers fear that they could be prosecuted. Current efforts are either too limited (as in the Industry Control Systems Computer Emergency Response Team guidance) or too ambiguous (such as the vaguely defined vulnerability equities process, or VEP, that governs vulnerabilities discovered by federal agencies).

The lack of a consistent regime for conducting vulnerability research and disclosure hinders efforts to find and fix critical vulnerabilities. In light of this uncertainty, market incentives are insufficient. Working with the private sector, the next administration needs to establish responsible vulnerability research and disclosure processes, eliminate legal risk, and devote additional funding to efforts to reduce the number of software vulnerabilities.

The president should ask the attorney general to clarify the legal status of vulnerability research. He should also direct NIST to lead a public-private effort to gather best practices on vulnerability reporting from security research and software companies. Given the usefulness of these programs, the administration should focus on clarity and incentives to accelerate vulnerability discovery.

The usefulness of these bug bounty programs has been proven again and again. Instead of sporadic, poorly funded efforts, we believe that the next administration should devote substantial funding (perhaps as much as $50 million). The administration should explore ways to allow for matching funding from private industry for bug bounty programs. As part of this, the administration should develop ways to support open-source software vulnerability research programs, through DHS or perhaps the National Science Foundation (NSF).

Increase the Use of Shared and Cloud Services

The use of third-party services can rapidly improve an organization's cybersecurity. In many cases, cybersecurity isn't an organization's core business or competency. The requirements for adequate cybersecurity can distract from the core business and can lead to data breach due to underinvestment. This problem is exacerbated as a result of too few qualified security personnel. Third-party security services can play a larger role in filling the gaps of many enterprises.

Most federal agencies are not in the cybersecurity business. As incidents like the massive data breach at the Office of Personnel Management remind us, protecting cyber assets is not a core competency for most agencies. While much is being done to increase the number and skill level of cybersecurity staff, expecting every organization to be competent in defending against massive, well-resourced state opponents is unrealistic. Outsourcing basic security functions enables better threat sharing and allows organizations to focus their resources on other critical or uncommon cyber risks that are the most consequential to their organization.

Better cybersecurity requires rethinking how the federal government acquires and manages information technology. It should move to a managed services model, with smaller agencies contracting for email, data storage, and cybersecurity. Services fall into four categories: email, data storage, networks, and business applications (the programs agencies use to conduct their missions). The first three categories are better provided from external sources as a managed service. Agencies should procure these services from third-party providers rather than attempting to build and manage their own. While the current administration has made the move to shared and cloud service a priority, these efforts need to be accelerated.

This should be part of a larger effort by OMB and GSA to build cybersecurity into IT acquisitions and programs. Both the administration and Congress need to recognize that federal agencies do not have a "refresh cycle" that improves cybersecurity. Old software is vulnerable. Moving to greater federal use of cloud and managed services reduces the problem of old software.

Cybersecurity Workforce Acceleration

Hiring of well-trained cybersecurity candidates is growing increasingly difficult due to skyrocketing demand. Anecdotally, many task force members shared the experience that they are forced to hire inexperienced candidates and then risk losing them to higher-paying positions at other companies after they were trained. To remedy this, the next administration should develop and implement an ambitious education and workforce model for cybersecurity, with a system for accrediting training and educational institutions; a taxonomy of cybersecurity roles and the skills that practitioners must demonstrate to claim competence in each specialty; and a robust network of professional credentialing entities.

One of the issues we discussed was whether, as an interim measure, to increase the number of H-1B visas for specialty workers. One idea was to establish a new visa category providing an allocation of 25,000 visas for foreign cybersecurity professionals or computer scientists to be employed at companies building cybersecurity products. This would be an interim step because the long-term solution must be to create an adequate U.S. cybersecurity workforce.

We recommend that the president direct key departments to allocate additional funding to cybersecurity education, training, and public awareness programs. The president should task DHS and the Department of Education to develop these programs, including white-hat hacking programs and ethical hacking, and with the Department of Veterans Affairs for programs aimed at veterans. The president should convene private-sector leaders, gather funding commitments, and launch a new program as a landmark initiative by the end of 2017.

We also recommend that the next administration move the workforce operation currently within DHS (which resides in NPPD's Office of Cybersecurity and Communications) to the National Institute of Standards and Technology (NIST) where the National Initiative for Cyber Education (NICE) is housed. There is no statutory authority for NPPD, and this causes confusion within and outside of the federal government since the statutory lies with NIST.

The United States has made progress in funding cybersecurity education, training, and awareness, but funding remains inadequate for the larger cyber workforce we need. Cybersecurity education and training is at the heart of this task force's recommendations. Education across age and other demographics is crucial to upgrading our human capital for cyber professions. This should include engagement early at the elementary school level. It should also include a special emphasis on veterans, who often bring invaluable skills and discipline to the tasks of cybersecurity. We recommend a range of education and training programs be implemented at the federal, state, and local levels. Growing the pipeline of qualified students in cyber is the only sustainable method to ensure our nation's continued cybersecurity.

03

Moving Ahead in the Next Four Years

Our one central conclusion is that the United States needs a coordinated approach to cybersecurity led by the White House and using all tools available to the president. Strategy is an overused term but the alternative is an ad hoc, piecemeal approach. Many individual efforts do not automatically aggregate into a strategy or effective defense. Strategy implies taking a step back and looking at the bigger picture to see the whole of the problem, the opportunities to address it, and how to connect these opportunities with available resources. Many countries now realize the benefits of having a national cybersecurity strategy to provide coherence and focus in their cybersecurity efforts.

Strategists need to consider how they are affected by resource and political constraints. Resources are not an insurmountable problem for the United States and other large countries (except for the workforce shortage), but are a significant impediment for many nations. The political obstacles are more intractable, since they reflect a lack of international consensus on state responsibilities and domestically (in the United States) on the role of government. Nor are many countries, including the United States, sufficiently organized to meet all the challenges of cybersecurity. In contrast to the resources, where small countries face the greater challenge, large countries may be at a disadvantage in organizing themselves given their size and complexity.

The strategic problem for cybersecurity is that societies depend on networks that are inherently not secure and that hostile actors have been quick to exploit, seemingly without hindrance. What we have learned in 20 years is that a focus solely on hardening networks is inadequate. It must be complemented by the development of understandings and rules for businesses and states on how they will behave in cyberspace.

The last formal cybersecurity strategy was issued in February 2003. The Obama administration's Sixty Day Review was effectively a strategy, albeit overly prescriptive. Developing a new strategy can provide a useful process for identifying goals and aligning problems with resources, but one lesson from both of these efforts is that strategies can become rapidly outdated as the business of the Internet changes—neither of the preceding documents considered how social media would grow in importance, the role of cloud computing and mobile devices, or the spread of IOT. The lesson is that a strategy, if considered necessary, must be developed quickly and be replaced just as quickly when circumstances warrant.

The new president has relatively few tools to manage cyber risk. Implementation of any new directives can be slow and uneven, and impose unexpected and unnecessary burdens on private actors. Despite this, none of the problems we face are insurmountable, but all require continuous, senior-level attention and steady effort if we are to make progress. Cyberspace has become the central global infrastructure. It will only grow in importance as more things and people depend upon it. But it is not secure, and the risks we face are unnecessarily great. Our opponents still have the advantage. We can change this if we want—not quickly and not easily—but of necessity if we are to build security for this century and the new world it has brought us.

About the Task Force Cochairs and Project Director

Cochairs

Sen. Sheldon Whitehouse is currently serving his second term representing Rhode Island. Since his election to the Senate in 2006, Senator Whitehouse has made cybersecurity one of his top legislative priorities. Among other work, he has authored comprehensive cybersecurity legislation, prepared the Senate Intelligence Committee's first cyber report, and worked with members of both parties to call attention to the growing cyber threat. In 2010, Senator Whitehouse chaired the Intelligence Committee's Cyber Task Force. As chairman of the Judiciary Subcommittee on Crime and Terrorism from 2011 to 2014, he held regular hearings on the cyber threat, including hearings on the role of law enforcement in responding to cyber attacks and on the dangers that cyber-enabled intellectual property theft pose to American businesses. In 2013, he introduced the bipartisan Cybersecurity Public Awareness Act to improve public access to information on cyber attacks. A graduate of Yale University and the University of Virginia Law School, Senator Whitehouse served as Rhode Island's U.S. attorney and as attorney general of Rhode Island before his election to the Senate. In addition to the Judiciary Committee, he is a member of the Budget Committee; the Environment and Public Works Committee; the Health, Education, Labor and Pensions Committee; and the Special Committee on Aging.

Rep. Michael T. McCaul is currently serving his sixth term representing Texas's 10th District in the U.S. House of Representatives and as the chairman of the House Committee on Homeland Security. Prior to Congress, Representative McCaul served as chief of counterterrorism and national security in the U.S. attorney's office, Western District of Texas, and led the Joint Terrorism Task Force charged with detecting, deterring, and preventing terrorist activity. McCaul also served as Texas deputy attorney general under current Sen. John Cornyn and served as a federal prosecutor in the Department of Justice's Public Integrity Section in Washington, D.C.

Karen S. Evans serves as the national director of U.S. Cyber Challenge, a nationwide talent search and skills development program focused on the cyber workforce, as well as an independent consultant, providing guidance in the areas of leadership, management, and the strategic use of information technology. Ms. Evans previously served as the administrator for e-government and information technology (IT) at the Office of Management and Budget (OMB) within the Executive Office of the President. She oversaw the federal IT budget of nearly $71 billion, which included implementation of IT throughout the federal government. This included advising the director of OMB on the performance of IT investments, overseeing the development of enterprise architectures within and across the agencies, directing the activities of the Chief Information Officers (CIO) Council, and overseeing the usage of the E-Government Fund to support interagency partnerships and innovation. Prior to becoming the administrator, Ms. Evans was the CIO for the Department of Energy.

Sameer Bhalotra is cofounder and CEO at StackRox, a senior associate at the Center for Strategic and International Studies (CSIS), and a Stanford CISAC affiliate. In addition to these roles, Dr. Bhalotra sits on the boards of many security startups. He previously worked in cybersecurity at Google and as COO at Impermium (acquired by Google). In government, he served as senior director for cybersecurity at the White House and as technology and cybersecurity lead for the Senate Select Committee on Intelligence (SSCI). Dr. Bhalotra graduated from Harvard University with a B.A. in physics and chemistry and from Stanford University with a Ph.D. in applied physics.

Project Director

James Andrew Lewis is a senior vice president and program director at CSIS, where he writes on technology, security, and innovation.

COVER PHOTO ISTOCKPHOTO ALENGO

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.**csis**.org

Report 2:

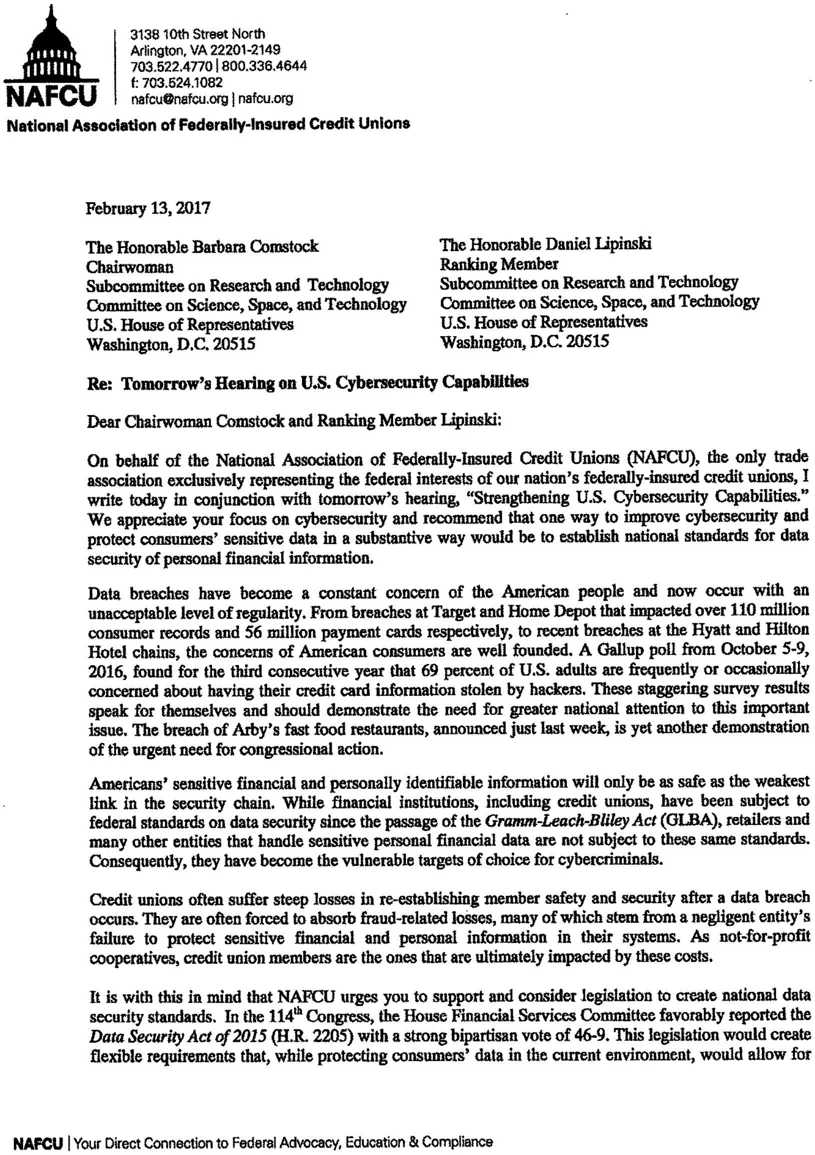
Title: *From Awareness to Action – A Cybersecurity Agenda for the 45th President*

Published By: Center for Strategic and International Studies (CSIS)

Date: January 4, 2017

https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf

Documents submitted by Subcommittee Ranking Member Daniel Lipinski



NAFCU

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

February 13, 2017

The Honorable Barbara Comstock
Chairwoman
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Daniel Lipinski
Ranking Member
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
U.S. House of Representatives
Washington, D.C. 20515

Re: Tomorrow's Hearing on U.S. Cybersecurity Capabilities

Dear Chairwoman Comstock and Ranking Member Lipinski:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), the only trade association exclusively representing the federal interests of our nation's federally-insured credit unions, I write today in conjunction with tomorrow's hearing, "Strengthening U.S. Cybersecurity Capabilities." We appreciate your focus on cybersecurity and recommend that one way to improve cybersecurity and protect consumers' sensitive data in a substantive way would be to establish national standards for data security of personal financial information.

Data breaches have become a constant concern of the American people and now occur with an unacceptable level of regularity. From breaches at Target and Home Depot that impacted over 110 million consumer records and 56 million payment cards respectively, to recent breaches at the Hyatt and Hilton Hotel chains, the concerns of American consumers are well founded. A Gallup poll from October 5-9, 2016, found for the third consecutive year that 69 percent of U.S. adults are frequently or occasionally concerned about having their credit card information stolen by hackers. These staggering survey results speak for themselves and should demonstrate the need for greater national attention to this important issue. The breach of Arby's fast food restaurants, announced just last week, is yet another demonstration of the urgent need for congressional action.

Americans' sensitive financial and personally identifiable information will only be as safe as the weakest link in the security chain. While financial institutions, including credit unions, have been subject to federal standards on data security since the passage of the *Gramm-Leach-Bliley Act* (GLBA), retailers and many other entities that handle sensitive personal financial data are not subject to these same standards. Consequently, they have become the vulnerable targets of choice for cybercriminals.

Credit unions often suffer steep losses in re-establishing member safety and security after a data breach occurs. They are often forced to absorb fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information in their systems. As not-for-profit cooperatives, credit union members are the ones that are ultimately impacted by these costs.

It is with this in mind that NAFCU urges you to support and consider legislation to create national data security standards. In the 114th Congress, the House Financial Services Committee favorably reported the *Data Security Act of 2015* (H.R. 2205) with a strong bipartisan vote of 46-9. This legislation would create flexible requirements that, while protecting consumers' data in the current environment, would allow for and encourage innovation to protect consumers from future threats we have not yet anticipated. Additionally, the national standards created in this bill would be scalable to allow for compliance by entities of all sizes. Just as the GLBA institutes requirements that are appropriate for both the smallest credit unions and the biggest banks, this legislation would allow for appropriate standards for the smallest corner store to the largest retailers. As you tackle the issue of cybersecurity in the 115th Congress, we urge you to consider including solutions such as the approach from the *Data Security Act of 2015* in any legislative effort.

Thank you for your attention and for your leadership on this issue of great importance to credit unions. Should you have any questions or require any additional information, please contact me or Chad Adams, NAFCU's Senior Associate Director of Legislative Affairs, at 703-842-2265 or cadams@nafcu.org.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

cc: Members of the Subcommittee on Research and Technology epic.org ELECTRONIC PRIVACY INFORMATION CENTER

February 13, 2017

The Honorable Barbara Comstock, Chair
The Honorable Eddie Bernice Johnson, Ranking Member
House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
2321 Rayburn House Office Building
Washington, DC 20515

RE: Hearing on Strengthening U.S. Cybersecurity Capabilities

Dear Chairwoman Comstock and Ranking Member Johnson:

We write to you regarding the hearing on "Strengthening U.S. Cybersecurity Capabilities" that will be held February 14, 2017. EPIC has an active interest in this effort. Weaknesses in cyber security threaten both consumers and democratic institutions.[1] EPIC is currently pursuing two Freedom of Information Act lawsuits to learn more about the Russian interference in the 2016 Presidential election.[2] EPIC filed these FOIA suits in order to understand, to the fullest extent possible, current cyber security risks to democratic institutions. We welcome your leadership on this critical issue and look forward to opportunities to work with you and your staff.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC was specifically established to advocate for the use of strong encryption technology and for the development of related Privacy Enhancing Technologies. EPIC led the effort in the United States in the 1990s to support strong encryption tools and played a key role in the development of the international framework for cryptography policy that favored the deployment of strong security measures to safeguard personal information.[4]

[1] *See* Democracy and Cybersecurity: Preserving Democratic Institutions, EPIC, https://epic.org/democracy/.

[2] *EPIC v. ODNI*, No. 17-163 (D.D.C. Jan. 25, 2017); *EPIC v. FBI*, No. 17-121 (D.D.C. Jan. 18, 2017).

[3] *See About EPIC*, EPIC, https://epic.org/epic/about.html.

[4] *See* Statement of EPIC President Marc Rotenberg, *The Computer Security Act of 1987 and the Memorandum of Understanding Between NIST and the NSA*, Hearing Before the U.S. House Committee on Government Operations, May 4, 1989, https://epic.org/crypto/csa/Rotenberg-Testimony-CSA-1989.pdf; Statement of EPIC President Marc Rotenberg, *Cypto Legislation*, Hearing Before the U.S. Senate Committee on Commerce, Science, and Transportation, June 26, 1996, https://epic.org/crypto/export_controls/epic_testimony_696.html.

Data protection and privacy should remain a central focus of the cyber security policy of the United States. It is precisely the extensive collection of personal information without adequate safeguards that places the United States at risk from cyber criminals and foreign adversaries. In 2015, more than 22 million records of federal employees, including 5 million digitized fingerprints and the sensitive form SF-86, were compromised. So-called "credit monitoring services" are an insufficient response to the ongoing risk to the financial records, medical records, and private communications of Americans.

Strong encryption policy and robust technical measures must be enacted in order to safeguard personal data. Weaknesses in security standards create vulnerabilities for American businesses and consumers that will be exploited by foreign adversaries. Where it is possible to minimize or eliminate the collection of personally identifiable information, the risk to the American public will be reduced.

The Cyber Security Information "Sharing" Act is now in force. That law facilitates the transfer of customer and client data from the private sector to the government, raising widespread concerns among technical experts and privacy organizations about the protection of personal information. While we favor a cooperative relationship between companies and the federal government concerning cyber security, the federal government must respect the privacy obligations of private companies and ensure the transparency of its own conduct. In the cyber security domain, as with other programs supported by taxpayer dollars, the government must uphold the law and remain open and accountable.

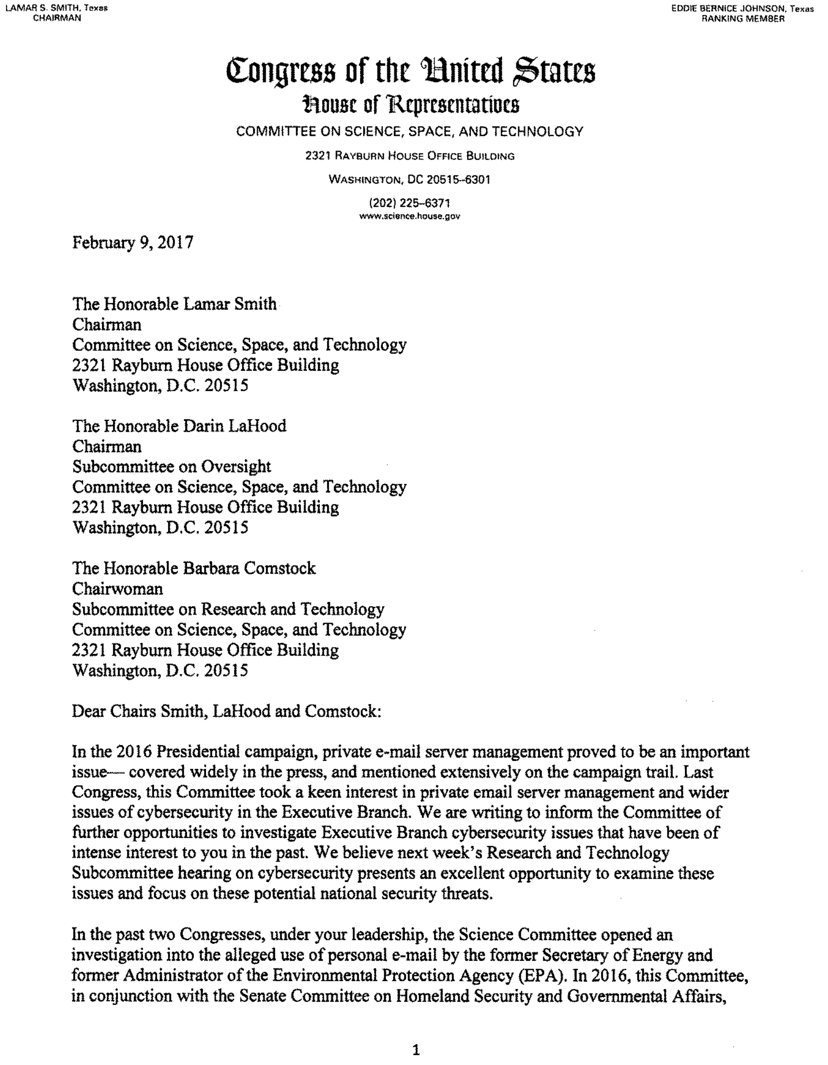
Finally, Congress should strengthen the federal Privacy Act. Personal data stored in federal agencies remains one of the key targets of criminal hackers and foreign adversaries. Significant steps were taken by the last administration to establish a Federal Privacy Council and to coordinate privacy protection across the federal agencies. Still, more should be done, including updates to the federal privacy law and the establishment of a data protection agency in the United States.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on Research and Technology on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg	/s/ Caitriona Fitzgerald
Marc Rotenberg	Caitriona Fitzgerald
EPIC President	EPIC Policy Director

Documents submitted by Full Committee Ranking Member Eddie Bernice Johnson



LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
2321 Rayburn House Office Building
Washington, DC 20515–6301
(202) 225–6371
www.science.house.gov

February 9, 2017

The Honorable Lamar Smith
Chairman
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Darin LaHood
Chairman
Subcommittee on Oversight
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Barbara Comstock
Chairwoman
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairs Smith, LaHood and Comstock:

In the 2016 Presidential campaign, private e-mail server management proved to be an important issue— covered widely in the press, and mentioned extensively on the campaign trail. Last Congress, this Committee took a keen interest in private email server management and wider issues of cybersecurity in the Executive Branch. We are writing to inform the Committee of further opportunities to investigate Executive Branch cybersecurity issues that have been of intense interest to you in the past. We believe next week's Research and Technology Subcommittee hearing on cybersecurity presents an excellent opportunity to examine these issues and focus on these potential national security threats.

In the past two Congresses, under your leadership, the Science Committee opened an investigation into the alleged use of personal e-mail by the former Secretary of Energy and former Administrator of the Environmental Protection Agency (EPA). In 2016, this Committee, in conjunction with the Senate Committee on Homeland Security and Governmental Affairs, opened a separate investigation of former Secretary of State Hillary Clinton's private e-mail server used during her time with the Department of State. Citing "numerous security concerns" and the possibility "that hostile actors gained access to Secretary Clinton's email account," this Committee subpoenaed the Federal Bureau of Investigation (FBI) and private companies for documents. Additionally, the Committee requested transcribed interviews with employees of one of the private companies[1].

Though Secretary Clinton left government service in 2013, the Science Committee stated that its oversight of the National Institute of Standards and Technology (NIST) still compelled an investigation of Secretary Clinton's email practices. The Committee sought to investigate the level of security that existed on her servers and possible records vulnerabilities that needed mitigation.[2] However, the Science Committee quickly dropped this investigation after the November 2016 Presidential election.

The current Administration, in its short time in office, has shown a shocking disregard for cybersecurity practices. Given your previous investigations of cybersecurity practices at multiple Federal agencies, including the Federal Deposit Insurance Corporation (FDIC) and Federal Reserve Board, and with respect to former Secretary Clinton's private email server, we trust you will be equally concerned with any and all careless cybersecurity practices of the Trump Administration. Although we are just weeks into the new Administration, already serious cybersecurity issues affecting the office of the President have arisen. Below are possible areas for review.

E-mail Server Management

According to various press reports, as of the end of last month, Senior Trump administrative staffers had active accounts on a Republican National Committee (RNC) email server.[3] During the Bush 43 administration, officials used this same RNC email server to circumvent the Presidential Records Act of 1978—resulting in the erasure of more than 22 million relevant emails.[4] Additionally, according to US Intelligence sources, Russian Intelligence Services hacked the Republican National Committee (RNC) email servers during the 2016 campaign—

[1] "Letters and Correspondence Regarding Clinton Server Subpoenas," maintained by Democratic staff of the House Committee on Science, Space & Technology, http://democrats.science.house.gov/letter/letters-and-correspondence-regarding-clinton-server-subpoenas

[2] *Id.*

[3] Nina Burleigh, "Trump White House Senior Staff Have Private RNC Email Accounts," Newsweek, January 25, 2017, accessed at: http://www.newsweek.com/trump-emails-rnc-reince-priebus-white-house-server-548191; Nicole Rojas, "White House senior staffers linked to private RNC email accounts," International Business Times, January 26, 2017, accessed at: http://www.ibtimes.co.uk/white-house-senior-staffers-linked-private-rnc-email-accounts-1603148.

[4] Many of the emails were later eventually recovered through the laborious efforts of the Obama administration. Dan Eggen, " Groups Announce Settlement in Missing Bush Emails Case," Washington Post, December 14, 2009, accessed at: http://voices.washingtonpost.com/44/2009/12/groups-announced-settlement-in.html; Nina Burleigh, "The George W. Bush White House 'Lost' 22 Million Emails," Newsweek, September 12, 2016, accessed at: http://www.newsweek.com/2016/09/23/george-w-bush-white-house-lost-22-million-emails-497373.html; *also see* Nicole Rojas, "White House senior staffers linked to private RNC email accounts," International Business Times, January 26, 2017, accessed at: http://www.ibtimes.co.uk/white-house-senior-staffers-linked-private-rnc-email-accounts-1603148.

retrieving older RNC emails from an older RNC server.[5] While there is no indication that any of the senior Trump staffers had their accounts hacked, their use of a private email server, so soon after the 2016 campaign and foreign intelligence service hacks, is quite dismaying.

Poor Security on Administration Twitter Accounts

An even bigger cybersecurity issue is the President's use of his Twitter account. A President's words have the power to move markets, imperil diplomatic relationships, or put militaries on high alert. President Trump has demonstrated this through his Twitter account, as his tweets have caused a drop in Toyota stock,[6] caused the Mexican peso to tumble[7], and caused the Mexican President to scuttle a planned diplomatic trip to the United States.[8]

Based on this power, the President's Twitter account should have strong cybersecurity safeguards. Unfortunately, this has not been the case. A well-known computer hacker, known by his Twitter handle @WauchulaGhost, revealed that the @POTUS twitter account was linked to an unsecured Gmail account.[9] This reportedly opened an easy route to hacking the President's Twitter account—1) request a password reset from Twitter for the @POTUS account, 2) hack into the linked unsecured Gmail account, and 3) simply wait for the new password for @POTUS to arrive in the Gmail inbox.[10] This vulnerability remained for days after @WauchulaGhost's tweet, not just on the @POTUS account, but the President's personal account @realDonaldTrump[11] and the @PressSec account of Press Secretary Sean Spicer,[12] which were both linked to unsecured Gmail accounts.[13]

[5] Nicole Gaouette, "FBI's Comey: Republicans also hacked by Russia," CNN.com, January 10, 2017, accessed at: http://www.cnn.com/2017/01/10/politics/comey-republicans-hacked-russia/index.html; *see* "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment, January 6, 2017, accessed at: http://www.foxnews.com/politics/2017/01/06/report-on-russian-activities-and-intentions-in-recent-us-elections.html.

[6] Toyota stock fell about 2%--more than $1 billion in market value—after then President-elect Trump threatened a "border tax" for Toyota because of the manufacturer's plan to build a factory in Mexico. Yuri Kageyama, "Toyota stock dips after Trump tweet on planned Mexico plant," Associated Press, January 5, 2017, accessed at: https://www.yahoo.com/news/toyota-stock-dip-trump-tweet-005441021.html.

[7] Ben Eisen, "Dollar Jumps Against Mexican Peso After Trump Tweet," The Wall Street Journal, January 26, 2017, accessed at: http://blogs.wsj.com/moneybeat/2017/01/26/dollar-jumps-against-mexican-peso-after-trump-tweet/; Dolia Estevez, "Analysts Say Donald Trump's Tweets Are Weakening the Mexican Peso," Forbes Magazine January 6, 2017, accessed at: http://www.forbes.com/sites/doliaestevez/2017/01/06/analysts-say-donald-trumps-tweets-are-weakening-the-mexican-peso/#9d0f5e6198b1.

[8] Jacob Pramuk, "Mexican president says he canceled meeting with Trump, who maintains the decision was mutual," CNBC.com, January 26, 2017, accessed at: http://www.cnbc.com/2017/01/26/mexican-president-pena-nieto-says-he-canceled-meeting-with-trump.html; "Mexican President Pena Nieto cancels trip to Washington," Chicago Tribune, January 26, 2017, accessed at: http://www.chicagotribune.com/news/nationworld/ct-trump-nieto-meeting-20170126-story.html.

[9] Laurie Segall, "Hacker to Trump: Fix your security settings on Twitter," CNN.com, January 24, 2017, accessed at: http://money.cnn.com/2017/01/24/technology/trump-white-house-twitter-security/index.html; Max Greenwood, "Trump's @POTUS Twitter account was tied to Gmail, The Hill, January 26, 2017, accessed at http://thehill.com/homenews/administration/316318-potus-twitter-account-is-tied-to-personal-email.

[10] Sam Biddle, "Donald Trump is Using a Private Gmail Account to Secure the Most Powerful Twitter Account in the World," The Intercept, January 26, 2017, accessed at: https://theintercept.com/2017/01/26/donald-trump-is-using-a-private-gmail-account-to-secure-the-most-powerful-twitter-account-in-the-world/.

[11] Mr. Trump's Twitter account has been hacked before, as his @realDonaldTrump account was hacked in 2013. Kevin Cirilli, "Trump: Twitter account was hacked," Politico, February 21, 2013, accessed at: http://www.politico.com/story/2013/02/donald-trump-twitter-account-was-hacked-087912.

Cellphone Vulnerabilities

A still bigger cybersecurity vulnerability is President Trump's outdated Android phone. According to press reports, Trump has either a Samsung Galaxy S3 or S4[14] and still uses it to access his @realDonaldTrump Twitter account.[15] This is despite the fact that he received a "secure, encrypted [phone] approved by the Secret Service."[16] Foreign intelligence services, or even an unsophisticated hacker, could easily exploit either of these phones. Foreign intelligence services could set up the President's phone to be a bug—recording everything around it and transmitting the recordings back to the hacker. Malware could also allow a foreign intelligence service to log keystrokes, take over the phone's camera, or track the phone's location.[17]

President Obama famously had a secure cellphone and complained about its lack of features.[18] Nevertheless, he understood that the phone's limitations arose from the extreme cybersecurity safeguards needed to protect national security. Thus far, President Trump has not shown an appreciation of the security needs inherent with the office of the Presidency.

The specific issues discussed above—1) private email server use by senior staff of the Trump Administration, 2) lack of safeguards on the social media accounts of the President and his senior staff, and 3) the President's continued use of an unsecured, imminently hackable cellphone, all speak to this Administration's disregard for cybersecurity and the dictates of protecting national security. As this Committee has previously taken an interest in Executive Branch cybersecurity issues, we hope that the change of party in the Executive Branch will not diminish your interest in this important area.

The Majority's Oversight Plan for the 115th Congress says the Committee intends to "continue to hold cybersecurity oversight hearings" in order to review "compliance with federal information security standards and guidelines…." and that the Committee will continue to investigate issues within this Committee's jurisdiction, "regardless of where they may be found." Ensuring that cybersecurity standards and proper cybersecurity practices are applied across the government,

[12] Additionally, Sean Spicer has already twice tweeted characters that look like a password from the @PressSec Twitter account. Bryan Menegus, "Sean Spicer Just Tweeted Something That Looks an Awful Lot Like a Password," Gizmodo, January 26, 2017, accessed at: http://gizmodo.com/sean-spicer-just-tweeted-something-that-looks-an-awful-1791649692.

[13] Sam Biddle, "Donald Trump is Using a Private Gmail Account to Secure the Most Powerful Twitter Account in the World," The Intercept, January 26, 2017, accessed at: https://theintercept.com/2017/01/26/donald-trump-is-using-a-private-gmail-account-to-secure-the-most-powerful-twitter-account-in-the-world/.

[14] Alex Dobie, "Which Android phone does Donald Trump use?" Android Central, January 25, 2017, accessed at: http://m.androidcentral.com/which-android-phone-does-donald-trump-use.

[15] Maggie Haberman, "A Homebody Finds the Ultimate Home Office, New York Times, January 25, 2017, accessed at: https://www.nytimes.com/2017/01/25/us/politics/president-trump-white-house.html.

[16] "[A]ccording to people close to the transition, he has traded in his Android phone for a secure, encrypted device approved by the Secret Service with a new number that few people possess." Maggie Haberman and Glenn Thrush, "A Trump Administration, With Obama Staff Members Filling the Gaps," New York Times, January 19, 2017, accessed at: https://www.nytimes.com/2017/01/19/us/trump-cabinet-picks-inauguration.html.

[17] Cecilia King, "That Old Phone Trump Uses for Twitter Could Be an Opening to Security Threats," New York Times, January 25, 2017, accessed at: https://www.nytimes.com/2017/01/25/technology/donald-trump-phone-social-media-security.html.

[18] Aaron Pressman, "President Obama's New Smartphone is More Like a Toddler Phone," Fortune Magazine, June 10, 2016, accessed at: http://fortune.com/2016/06/10/president-obamas-new-smartphone-is-more-like-a-toddler-phone/.

particularly in today's cybersecurity environment, is critically important. We hope that your commitment to ensuring federal cybersecurity standards are in place and that common sense cybersecurity practices are upheld does not stop at the White House lawn.

We stand ready to join the Majority in any robust investigation of these issues and wider federal cybersecurity issues in general.

Sincerely,

Eddie Bernice Johnson

Eddie Bernice Johnson
Ranking Member
Committee on Science, Space,
and Technology

Don Beyer
Member
Committee on Science, Space,
and Technology

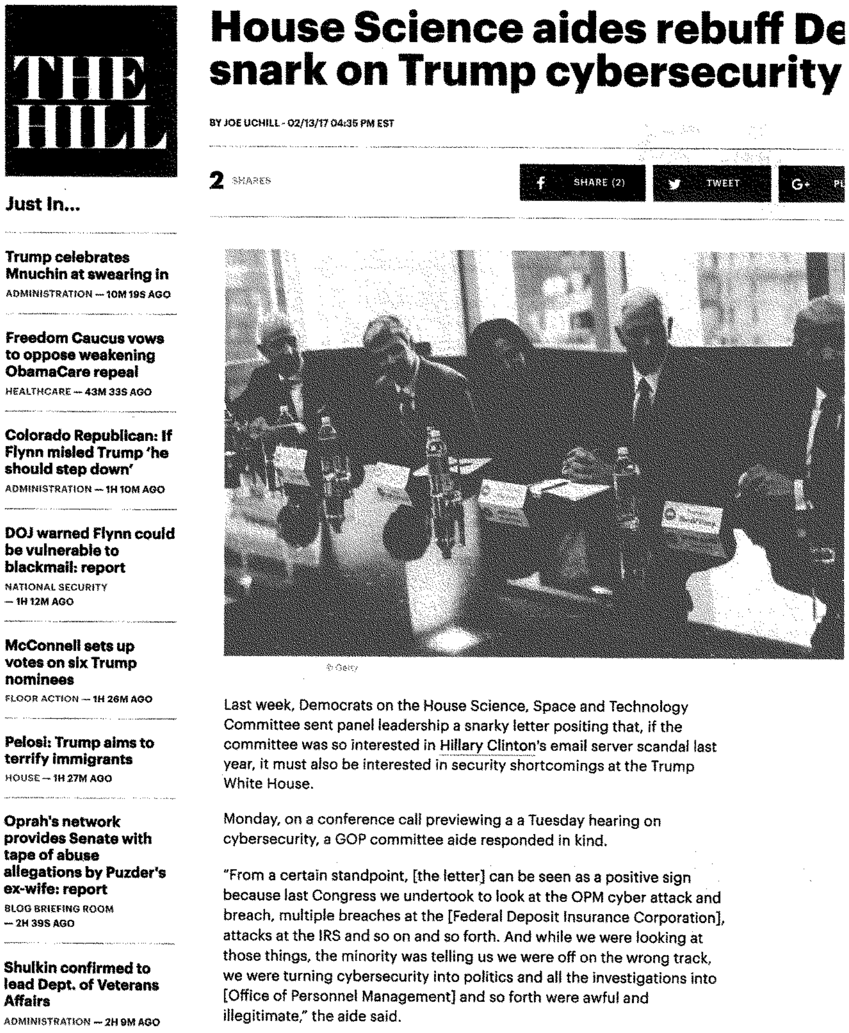
Dan Lipinski
Member
Committee on Science, Space and Technology

Ms. Johnson Statement on The Hill article and Documents-For-The-Record

Chairwoman Comstock, I have been in Congress and on this Committee a long time. There are many times I have disagreed with my Republican colleagues. Sometimes we have had harsh criticisms of each other's political positions. That comes with the job description of being a Member of Congress. I accept that.

What I will **not** accept is when Members or staff provide clearly misleading information about me or my colleagues to the press, the public or anyone else. Yesterday, a story in *The Hill* newspaper regarding a letter that I sent along with Mr. Lipinski and Mr. Beyer to you, Chairman Smith and Chairman LaHood about President Trump's cybersecurity practices, quoted an unnamed "GOP committee aide." That aide suggested that last Congress Committee Democrats opposed the cybersecurity hearings that were held on this Committee regarding the Office of Personnel Management (OPM), the Internal Revenue Service (IRS) and the Federal Deposit Insurance Corporation (FDIC) because we believed they were political and illegitimate. I won't speak for my colleagues, but I did believe many of the hearings that were held on this Committee were politically motivated. But none of them included any of the hearings mentioned by this Committee aide. If this aide had attended any of those hearings or read any of the statements by me or Ranking Members Beyer and Lipinski they would have understood that.

Since I believe in ensuring there is an honest record of events I would like unanimous consent to enter into the record all of the Ranking Member statements and press releases issued by the Democrats for each of the hearings referenced by this Republican staffer in order to set the record straight.



House Science aides rebuff De snark on Trump cybersecurity

BY JOE UCHILL - 02/13/17 04:35 PM EST

Last week, Democrats on the House Science, Space and Technology Committee sent panel leadership a snarky letter positing that, if the committee was so interested in Hillary Clinton's email server scandal last year, it must also be interested in security shortcomings at the Trump White House.

Monday, on a conference call previewing a a Tuesday hearing on cybersecurity, a GOP committee aide responded in kind.

"From a certain standpoint, [the letter] can be seen as a positive sign because last Congress we undertook to look at the OPM cyber attack and breach, multiple breaches at the [Federal Deposit Insurance Corporation], attacks at the IRS and so on and so forth. And while we were looking at those things, the minority was telling us we were off on the wrong track, we were turning cybersecurity into politics and all the investigations into [Office of Personnel Management] and so forth were awful and illegitimate," the aide said.

Just In...

Trump celebrates Mnuchin at swearing in
ADMINISTRATION — 10M 19S AGO

Freedom Caucus vows to oppose weakening ObamaCare repeal
HEALTHCARE — 43M 33S AGO

Colorado Republican: If Flynn misled Trump 'he should step down'
ADMINISTRATION — 1H 10M AGO

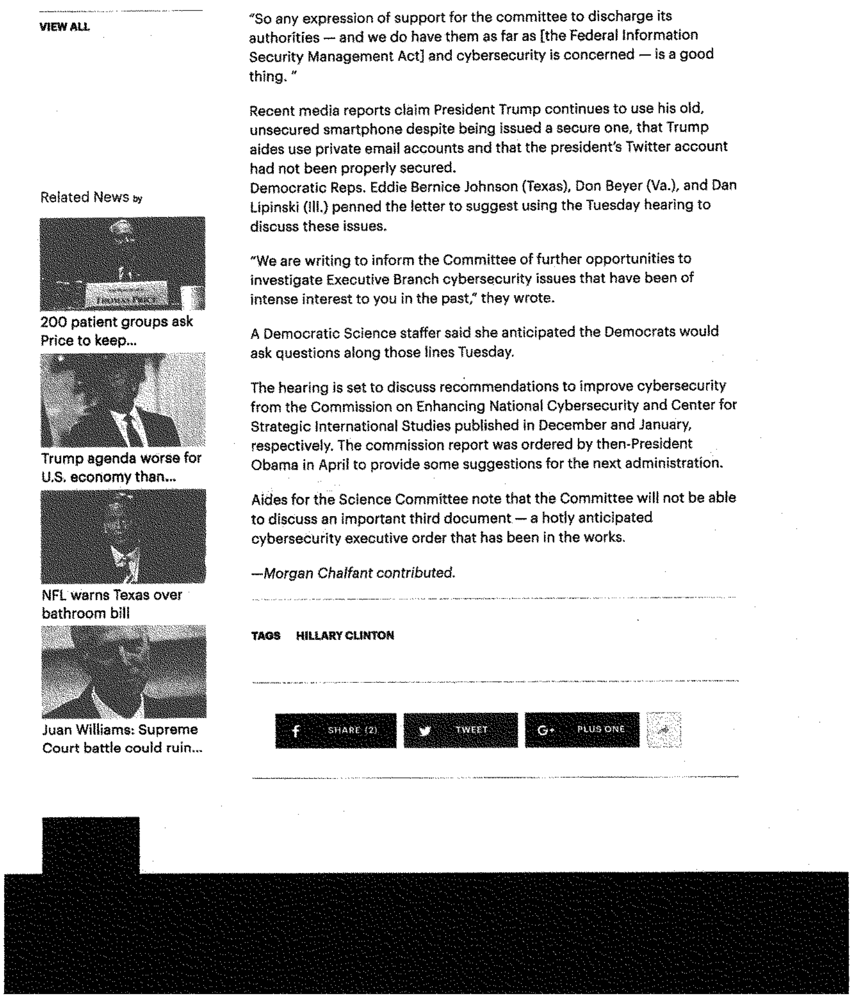
DOJ warned Flynn could be vulnerable to blackmail: report
NATIONAL SECURITY — 1H 12M AGO

McConnell sets up votes on six Trump nominees
FLOOR ACTION — 1H 26M AGO

Pelosi: Trump aims to terrify immigrants
HOUSE — 1H 27M AGO

Oprah's network provides Senate with tape of abuse allegations by Puzder's ex-wife: report
BLOG BRIEFING ROOM — 2H 39S AGO

Shulkin confirmed to lead Dept. of Veterans Affairs
ADMINISTRATION — 2H 9M AGO



VIEW ALL

Related News by

200 patient groups ask Price to keep...

Trump agenda worse for U.S. economy than...

NFL warns Texas over bathroom bill

Juan Williams: Supreme Court battle could ruin...

"So any expression of support for the committee to discharge its authorities — and we do have them as far as [the Federal Information Security Management Act] and cybersecurity is concerned — is a good thing. "

Recent media reports claim President Trump continues to use his old, unsecured smartphone despite being issued a secure one, that Trump aides use private email accounts and that the president's Twitter account had not been properly secured.
Democratic Reps. Eddie Bernice Johnson (Texas), Don Beyer (Va.), and Dan Lipinski (Ill.) penned the letter to suggest using the Tuesday hearing to discuss these issues.

"We are writing to inform the Committee of further opportunities to investigate Executive Branch cybersecurity issues that have been of intense interest to you in the past," they wrote.

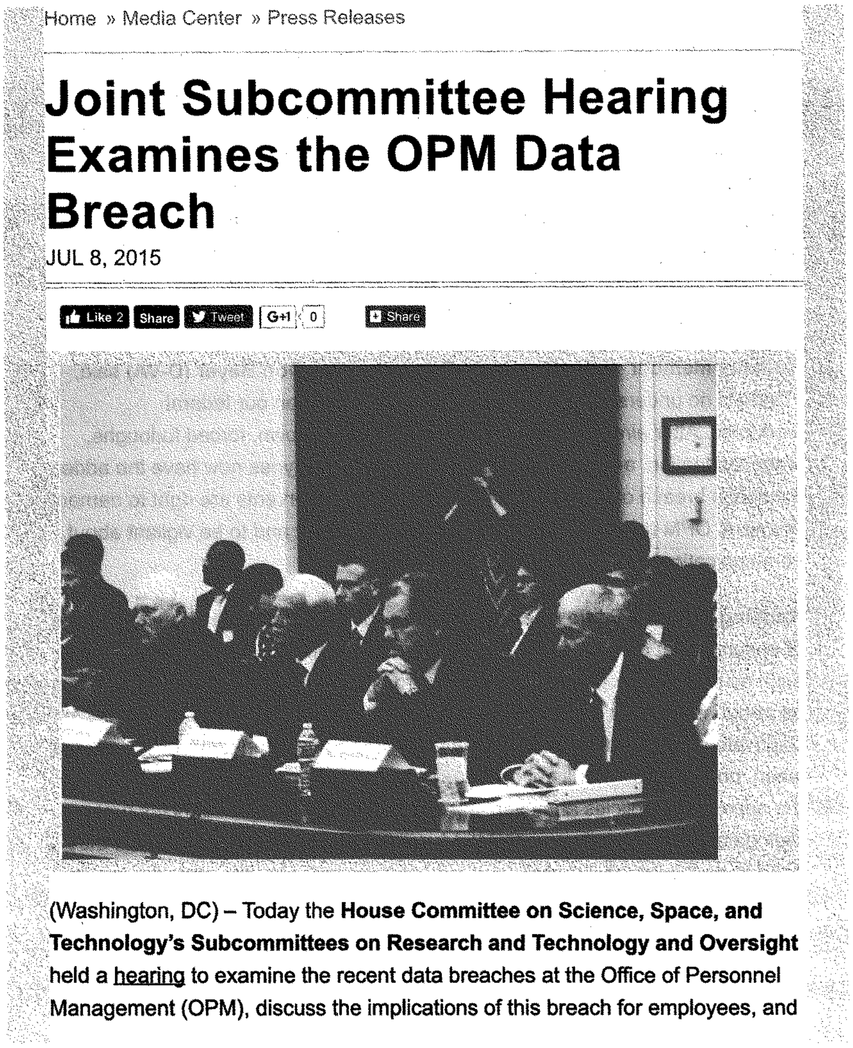
A Democratic Science staffer said she anticipated the Democrats would ask questions along those lines Tuesday.

The hearing is set to discuss recommendations to improve cybersecurity from the Commission on Enhancing National Cybersecurity and Center for Strategic International Studies published in December and January, respectively. The commission report was ordered by then-President Obama in April to provide some suggestions for the next administration.

Aides for the Science Committee note that the Committee will not be able to discuss an important third document — a hotly anticipated cybersecurity executive order that has been in the works.

—Morgan Chalfant contributed.

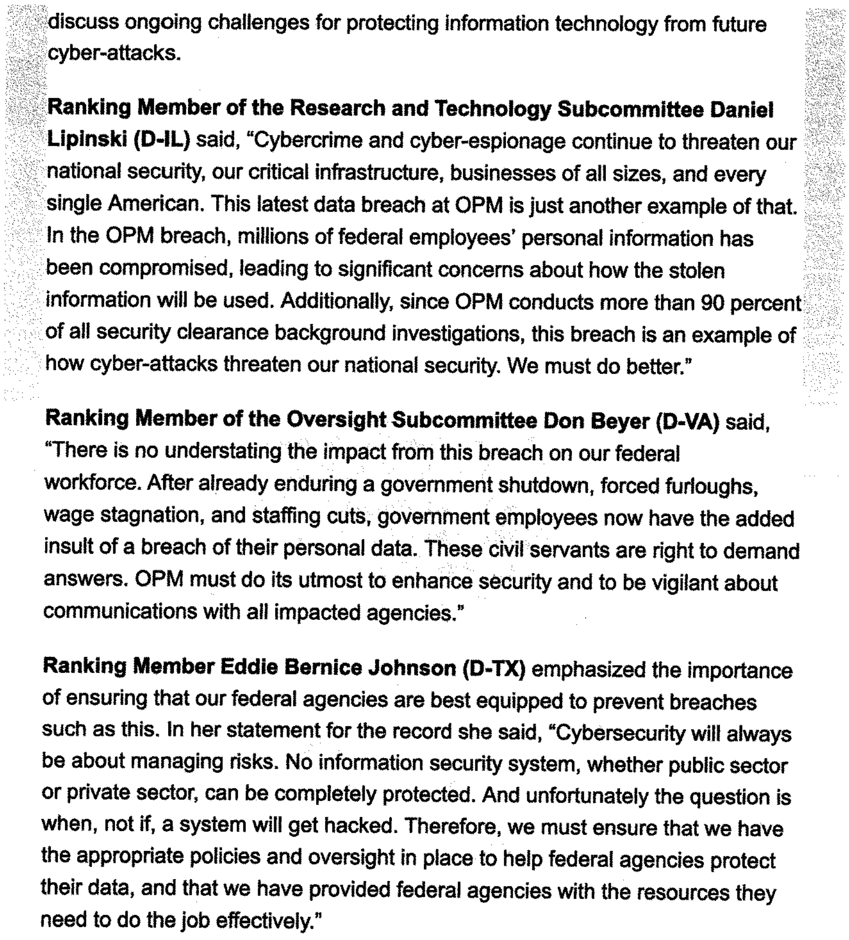
TAGS HILLARY CLINTON



Joint Subcommittee Hearing Examines the OPM Data Breach

JUL 8, 2015

(Washington, DC) – Today the **House Committee on Science, Space, and Technology's Subcommittees on Research and Technology and Oversight** held a hearing to examine the recent data breaches at the Office of Personnel Management (OPM), discuss the implications of this breach for employees, and



discuss ongoing challenges for protecting information technology from future cyber-attacks.

Ranking Member of the Research and Technology Subcommittee Daniel Lipinski (D-IL) said, "Cybercrime and cyber-espionage continue to threaten our national security, our critical infrastructure, businesses of all sizes, and every single American. This latest data breach at OPM is just another example of that. In the OPM breach, millions of federal employees' personal information has been compromised, leading to significant concerns about how the stolen information will be used. Additionally, since OPM conducts more than 90 percent of all security clearance background investigations, this breach is an example of how cyber-attacks threaten our national security. We must do better."

Ranking Member of the Oversight Subcommittee Don Beyer (D-VA) said, "There is no understating the impact from this breach on our federal workforce. After already enduring a government shutdown, forced furloughs, wage stagnation, and staffing cuts, government employees now have the added insult of a breach of their personal data. These civil servants are right to demand answers. OPM must do its utmost to enhance security and to be vigilant about communications with all impacted agencies."

Ranking Member Eddie Bernice Johnson (D-TX) emphasized the importance of ensuring that our federal agencies are best equipped to prevent breaches such as this. In her statement for the record she said, "Cybersecurity will always be about managing risks. No information security system, whether public sector or private sector, can be completely protected. And unfortunately the question is when, not if, a system will get hacked. Therefore, we must ensure that we have the appropriate policies and oversight in place to help federal agencies protect their data, and that we have provided federal agencies with the resources they need to do the job effectively."

OPENING STATEMENT

Ranking Member Daniel Lipinski (D-IL)
Subcommittee on Research and Technology
Committee on Science, Space, and Technology

Is the OPM Data Breach the Tip of the Iceberg
Joint Subcommittee Hearing

July 8, 2015

Thank you Chairwoman Comstock and Chairman Loudermilk for holding this hearing on the recent OPM data breach. I want to thank all the witnesses for being here this afternoon.

Unfortunately, major cyber-attacks are happening more frequently. Today, we are going to talk about the significant breaches at the Office of Personnel Management (OPM). Not to take away from the significance of the OPM breach, I think it is important to note that there have been an increasing number of cyber-attacks in both the private and public sector.

Several years ago I began working on cybersecurity legislation, the *Cybersecurity Enhancement Act,* with my colleague, Mr. McCaul. Our legislation dealt with cybersecurity standards, education, and workforce development. When we started, I said that I had no doubt that threats from individual hackers, criminal syndicates, and even other governments would grow and evolve along with our increased use of the internet. Unfortunately, I was right.

In February, Anthem, one of the nation's largest health insurance companies, announced that it suffered a cyber-breach that compromised the records of 80 million current and former customers. And just last year there were high profile breaches at JP Morgan Chase, eBay, Target, and many others affecting millions of people.

Although I was happy that my bill with Mr. McCaul was enacted at the end of last Congress, there is much, much more to be done in the area of cybersecurity. Cybercrime and cyber-espionage continues to threaten our national security, our critical infrastructure, businesses of all sizes, and every single American. This latest data breach at OPM is just another example of that. In the OPM breach, millions of federal employees' personal information has been compromised, leading to significant concerns about how the stolen information will be used. Additionally, since OPM conducts more than 90 percent of all security clearance background investigations, this breach is an example of how cyber-attacks threaten our national security. We <u>must</u> do better.

It will take a collective effort of both the public and private sector to improve cybersecurity, and I cannot emphasize enough the importance of research into the social and behavioral aspects in this area. Our IT infrastructure is built, operated and maintained by humans, from the average worker at her desktop to the chief information officer of a major company or agency. Most cyber-attacks are successful because of human error, such as unwittingly opening a malicious email or allowing one's credentials to be compromised. Understanding the human element is necessary to combat threats and reduce risk.

To set government-wide guidelines for protecting federal information security systems, Congress passed the *Federal Information Security Modernization Act* or FISMA. FISMA, which was updated at the end of last Congress, requires federal agencies to develop, document, and implement an agency wide information security program.

Along with being responsible for their own information security system, the National Institute of Standards and Technology (NIST) is tasked with developing standards and guidelines for all civilian federal information systems. Since NIST plays a critical role in protecting our nation's information security systems, it is important that they be part of this conversation. I am happy that Dr. Romine is here today to tell us more about how NIST develops FISMA standards and how they work with other federal agencies.

FISMA also requires annual reviews of individual agencies' information security programs as well as reviews of information security policies and the implementation of FISMA requirements government-wide. I hope to hear from our witnesses about the steps necessary to ensure that OPM meets FISMA requirements, as well as how other agencies are doing in this space.

More information security systems—both in the public and private sector—will surely be subject to cyber-attacks in the future. And while it is impossible to completely protect a connected information security system, we must do all we can to protect the personal information of millions of Americans and conduct the oversight to ensure such steps are taken. This hearing is the beginning of a conversation on how we can do that and we must make sure that we follow through with action.

I look forward to our discussion this afternoon. Thank you and I yield back the balance of my time.

OPENING STATEMENT

Ranking Member Don Beyer (D-VA)
Subcommittee on Oversight
Committee on Science, Space & Technology

Is the OPM Data Breach the Tip of the Iceberg?
Joint Subcommittee Hearing

July 8, 2015

Thank you Chairs Comstock and Loudermilk for holding this hearing today. I believe this is an important hearing and I look forward to hearing from our witnesses. I believe this is an important and timely hearing. Earlier today it was reported that the New York Stock Exchange, United Airlines and Wall Street Journal are all suffering from a "computer glitch" that has disrupted their computer networks. Whether this event is determined to be intentional or not it highlights the potential vulnerability of our digital dependence. Today's hearing, however, is about another computer incident at the Office of Personnel Management or OPM.

Deterring, detecting and defending against the multitude of on-line threats that constantly lurk in the cyberspace domain is a critical issue for the federal government and private sector alike. Last year alone federal agencies reported nearly 70,000 individual computer security incidents to the U.S. Computer Emergency Readiness Team or CERT. During the same time period, from October 1, 2013 to September 30, 2014, non-Federal entities reported more than 570,000 incidents and many other incidents are potentially not identified and others not reported at all.

Cyber threats are constant and evolving, some are very sophisticated and many pose serious distress to companies, agencies and individuals. The two recent data breaches of the Office of Personnel Management (OPM) are particularly important to me and my constituents. Representing a congressional district just outside the nation's Capital many of my constituents are federal employees who may have had their personal data compromised as a result of these intrusions. One of those attacks is believed to have compromised the personal information of more than 4 million individuals and the other is suspected to have compromised the data of as many as 14 million people. I am particularly troubled that the data that was reportedly accessed included not just the personnel files but the security files of our defense, homeland security and intelligence community employees. This could potentially jeopardize their financial security, personal safety and ultimately the secrets they are entrusted to help protect for our Nation.

While the facts of this case are still being unraveled, including the motive for the attack, the identities of the perpetrators and the potential damage they may have caused, we should understand too that the federal government is not alone in being victim to cyberattacks. In the past year, hundreds of millions of personal records have been compromised by hackers targeting JP Morgan Chase, Ebay, Home Depot and other private companies.

Still, the OPM breach was significant. I am concerned for the personal and professional impact of this breach on our dedicated federal workforce, particularly those involved in the national security arena. It should not be understated the impact this has on the morale of a workforce that has recently endured – through no fault of their own – a government shutdown, forced furloughs, staffing cuts, and pay freezes. These government employees now have the added insult of a breach of their personal data.

Agency heads should also be mindful and accommodating of impacted federal employees who need time off to mitigate the fallout from the hack. I encourage OPM to communicate with all agencies to ensure workers are accommodated so that they can visit their banks, Social Security offices, and creditors in order to deal with the repercussions of the breach.

I am also concerned that reports of this attack suggest it may have been the result of individuals with ties to foreign entities and I am concerned that it appears a private company working for the government as a security contractor may have been the weak link in the chain of events that ultimately led to a successful attack.

The Federal government is making steady, but slow progress in fortifying our cyber defenses from potential attack. According to the Office of Management and Budget's (OMB's) annual report on the Federal Information Security Management Act (FISMA) sent to Congress in February there has been improvement in federal agencies implementing continuous monitoring of their networks and the authentication of their users, for instance. But the results are still not good enough. Federal Agencies need to do a better job meeting the IT security criteria demanded by compliance with FISMA and they need to apply the cyber security standards recommended by the National Institute of Standards and Technology (NIST) to their networks. At the same time, Congress and the public need to realize that no matter how well protected an Agency or private entity is that they will never be 100-percent secure and that data breaches are bound to occur in the future.

I hope our witnesses can help provide us with advice on closing cyber-security holes when and where they exist and augmenting our security defenses against them.

With that I yield back.

OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)
Committee on Science, Space & Technology

Is the OPM Data Breach the Tip of the Iceberg?
Joint Subcommittee Hearing

July 8, 2015

Thank you Chairwoman Comstock and Chairman Loudermilk for holding this hearing on the recent OPM data breach.

Even though we will continue to learn more details about the breach, we already know that millions of Americans' personal information was compromised. This number includes current and retired federal employees as well as the family members, friends, and co-workers of federal employees.

There are valid concerns about hackers using this data for criminal purposes. Additionally, since security clearance background investigation information was compromised, there are also serious national security concerns.

It is frustrating to learn that OPM knew that they had serious information security systems problems long before this breach. Although addressing their information security systems is a top goal of the new OPM leadership, it is clear that action should have been taken years ago.

Federal computer information systems are guided by FISMA. In this risk management approach, agencies evaluate the type of data in their systems, determine what level of controls are needed, and put together a plan to adequately protect their data.

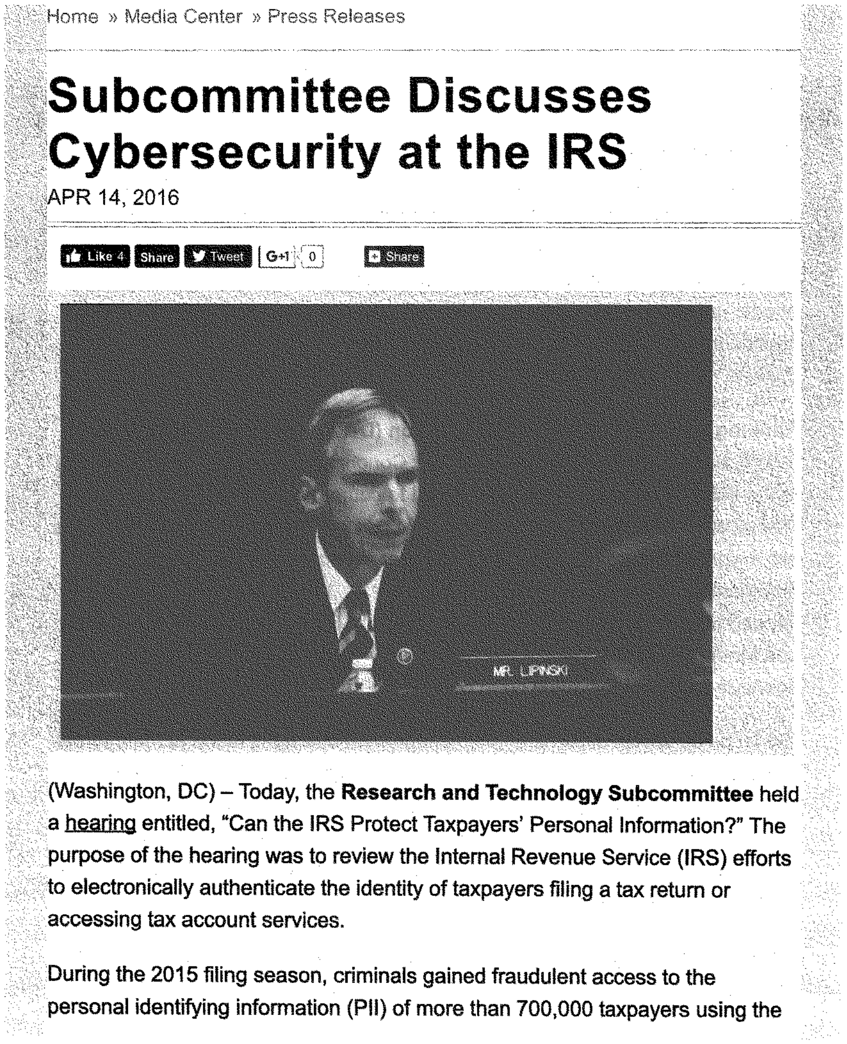
Although NIST is responsible for drafting the standards used by the agencies, they do not oversee the program and are not responsible for enforcing agency compliance with FISMA.

Instead of picking on one federal agency, it is my hope that we can use this data breach as a starting point for addressing federal cybersecurity more broadly. What is working? What is not? What mechanisms need to be in place to better protect individuals' personal information on our federal systems?

I want to end by saying that any conversation about federal cybersecurity must include a discussion about resources. It would be irresponsible for us to mandate additional cybersecurity measures that federal agencies must take without providing them with additional resources.

Cybersecurity will always be about managing risks. No information security system, whether public sector or private sector, can be completely protected. And unfortunately the question is, when, not if a system will get hacked. Therefore, we must ensure that we have the appropriate policies and oversight in place to help federal agencies protect their data, and that we have provided federal agencies with the resources they need to do the job effectively.

I want to thank the witnesses for their testimony and I yield back the balance of my time.



Subcommittee Discusses Cybersecurity at the IRS

APR 14, 2016

(Washington, DC) – Today, the **Research and Technology Subcommittee** held a hearing entitled, “Can the IRS Protect Taxpayers’ Personal Information?” The purpose of the hearing was to review the Internal Revenue Service (IRS) efforts to electronically authenticate the identity of taxpayers filing a tax return or accessing tax account services.

During the 2015 filing season, criminals gained fraudulent access to the personal identifying information (PII) of more than 700,000 taxpayers using the

IRS online application “Get Transcript.” In addition, the IP PIN online tool - specifically intended to protect taxpayers who were already victim to, or at high risk for, identity theft - was breached, possibly allowing criminals to file fraudulent tax returns and steal taxpayers' tax refunds. IRS subsequently shut down these tools.

Ranking Member of the Subcommittee, Daniel Lipinski (D-IL) said in his opening statement, "Data breaches at the IRS are particularly troubling and we should closely examine what IRS has done wrong when it comes to protecting the personal information of Americans, how it can do better in regard to cybersecurity, and what Congress can do to better support IRS cybersecurity efforts. In meeting their obligation to pay taxes, Americans should have confidence that the IRS is taking all possible steps to protect them from cyber thieves."

Ranking Member Eddie Bernice Johnson (D-TX), in her statement for the record, expressed that a series of cuts by Congress over the past several years to the IRS's budget may have contributed to compromised information security, "These spending cuts, which triggered a 14 percent reduction in IRS employees, are a significant factor in weakened taxpayer services, reduced detection and enforcement of fraudulent claims, and the agency's ability to hire qualified staff needed to fulfill its many requirements under the Federal Information Security and Modernization Act. And if the House had its way in recent years, the agency's budget would have been cut even further.

"So let us be critical of some of the management decisions made at the Internal Revenue Service with respect to protecting taxpayers' personal information. And let us be sure they are putting the people, systems, and processes in place to make better decisions going forward. But let us also be willing to provide the agency with the financial resources and other authorities they need to accomplish these goals."

Congressman Lipinski discussed the role of the National Institute of Standards and Technology (NIST) in federal cybersecurity. "In the context of this hearing it is important to talk about NIST, an agency that this subcommittee has jurisdiction over. NIST plays an important role in developing technical standards and providing expert advice to agencies across the government as they carry out their responsibilities under the Federal Information Security Modernization Act."

"It is clear that the IRS did not follow the risk analysis or cybersecurity and authentication standards set by NIST when it set up these portals. The most important question is "why?" Was it a lack of understanding of the standards? In this case, we need to have NIST here to talk about the standards and how to make them clearer. Or are there technical barriers to implementing the NIST standards at all? In this case, we need to have information on why these applications were allowed to go live in the first place. Or was this a strategic decision driven by tradeoffs between consumer convenience and security? In that case, we must be clear: the IRS has a unique role among federal agencies and holds information on taxpayers that few others have. Protection of taxpayer data must be a top-level priority and we must work to ensure that a breach of this nature never happens again."

Commissioner Koskinen discussed the importance of getting streamlined critical pay authority to be able to retain and to hire cybersecurity experts more quickly. He said in his testimony, "An important proposal is the reauthorization of so-called streamlined critical pay authority, originally enacted in 1998, to assist the IRS in bringing in individuals from the private sector with the skills and expertise needed in certain highly specialized areas, including IT, international tax and analytics support. This authority, which ran effectively for many years, expired at the end of FY 2013 and was not renewed."

"The loss of streamlined critical pay authority has created major challenges to our ability to retain employees with the necessary high-caliber expertise in the areas mentioned above. In fact, out of the many expert leaders and IT executives hired under critical pay authority, there are only 10 IT experts remaining at the IRS, and we anticipate there will be no staff left under critical pay authority by this time next year. The President's FY 2017 Budget proposes reinstating this authority, and I urge the Congress to approve this proposal."

Ranking Member Johnson said after the hearing, "At the hearing today, Members stressed the necessity of protecting the U.S. taxpayers' personal information, and I think that we can all agree that is of the utmost importance. We also heard about the series of cuts to the IRS's budget and the lapse of their critical pay authority. If we want the IRS to be in the best position possible to protect the taxpayers, we must give them the resources necessary to do so and the authority they need to hire the best and brightest in the field. I hope we in Congress will take what we heard today to heart and work to renew the critical pay authority and ensure that the IRS has the budget they need to do their jobs and protect the taxpayer."

Witnesses:
The Honorable John Koskinen, Commissioner, Internal Revenue Service
The Honorable J. Russell George, Inspector General, Treasury Inspector General for Tax Administration
Mr. Gregory Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office

OPENING STATEMENT
Ranking Member Daniel Lipinski (D-IL)
of the Subcommittee on Research and Technology

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Can the IRS Protect Taxpayers' Personal Information?"
April 14, 2016

Thank you Chairwoman Comstock for holding this hearing, and welcome to the witnesses. I know this is a busy season for you, and I appreciate you taking the time to appear before us this morning.

Today, we will be discussing cybersecurity breaches at two IRS online service portals. This hearing follows the reports of unauthorized access to the personal information of more than 700,000 American taxpayers, and the theft of money from taxpayers that likely came about as a result. Just about every American can expect to interact with the IRS during his or her life, and the agency's responsibilities make it privy to significant amounts of personal information about all of these individuals. Consequently, data breaches at the IRS are particularly troubling and we should closely examine what IRS has done wrong when it comes to protecting the personal information of Americans, how it can do better in regard to cybersecurity, and what Congress can do to better support IRS cybersecurity efforts. In meeting their obligation to pay taxes, Americans should have confidence that the IRS is taking all possible steps to protect them from cyber thieves.

Cybersecurity remains an evolving challenge across federal agencies as well as the private sector. Standards that were leading edge a year ago may be outdated today. Security is not a one-time goal to be achieved and placed on autopilot; it is a process that requires vigilance, continual learning, and fast dissemination of critical information to prevent and respond to new threats. While no entity, public or private, can protect data with 100% certainty, we must be nimble in learning from failures or missteps in cybersecurity policies and procedures. To this end, we should heed the careful and detailed recommendations of the GAO and the Inspectors General. We must also ensure that decisions on cybersecurity policies are backed by a process that supports accountability, robust and forward-looking decision-making, and a clear sense of the consequences that can stem from data security failures. Unfortunately, it is not at all apparent from the recent breaches at the IRS that the agency's policies were governed by such a comprehensive process. The two breaches that we are discussing today – the Get Transcript application and the Identity Protection PIN application – should not be viewed in isolation. Both of these breaches were facilitated in part by the same security weakness, namely the overreliance on out of the wallet questions derived from credit report data. While in principle the answers to such questions should only be known by taxpayers, in practice they can often be guessed or uncovered from sources such as social media or websites compiling public record data. As a result, a breach in one application should have tipped off the IRS that the other was vulnerable as well. Yet the agency continued to make online IP PIN retrieval available long after shutting down the Get Transcript application because of security concerns. Further, the agency continued to do so even after the Treasury Inspector General for Tax Administration, or TIGTA, warned the IRS to shut down the IP PIN tool as well. We must get clarity on what steps the IRS is taking to ensure internal information sharing so that any breaches and their implications are quickly assessed across the entire organization and not just separate units or staff dealing directly with a problem at hand. Further, we must examine why the IRS ignored or deprioritized the TIGTA recommendation to shut down the IP PIN tool. Simply put, given how one breach built on the other, this should not have occurred.

In the context of this hearing it is important to talk about NIST, an agency that this subcommittee has jurisdiction over. NIST plays an important role in developing technical standards and providing expert advice to agencies across the government as they carry out their responsibilities under the Federal Information Security Modernization Act, of FISMA. It is clear that the IRS did not follow the risk analysis or cybersecurity and authentication standards set by NIST when it set up these portals. The most important question is "why?" Was it a lack of understanding of the standards? In this case, we need to have NIST here to talk about the standards and how to make them clearer. Or are there technical barriers to implementing the NIST standards at all? In this case, we need to have information on why these applications were allowed to go live in the first place. Or was this a strategic decision driven by tradeoffs between consumer convenience and security? In that case, we must be clear: the IRS has a unique role among federal agencies and holds information on taxpayers that few others have. Protection of taxpayer data must be a top-level priority and we must work to ensure that a breach of this nature never happens again.

Finally, I would like to note that successful data security efforts depend on agencies being able to hire experienced cybersecurity professionals as well as having budgetary resources specifically directed toward security infrastructure. While some security failures at the IRS raise oversight questions about decision-making protocols at the management level, we also cannot ignore that successful implementation of good security practices costs money. Although this is beyond the scope of our Committee's jurisdiction, I am concerned that Congress has yet to reauthorize IRS' streamlined critical pay authority which helps the agency compete with the private sector for top cybersecurity talent. And as Congress makes funding decisions for the coming fiscal year, we must ensure that we provide resources to match current IT-specific needs.

I look forward to this morning's discussion, and I yield back the balance of my time.

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Can the IRS Protect Taxpayers' Personal Information?"
April 14, 2016

I want to begin by welcoming the witnesses to today's hearing to discuss the need for stronger information security policies and procedures at the Internal Revenue Service in order to better protect taxpayers' personal information.

I am concerned about the identify theft that has already occurred and might yet occur because of weakness in information security controls at the IRS. Taxpayers have a right to expect that their information will be kept secure when they make use of online services provided by the Internal Revenue Service or any other government agency.

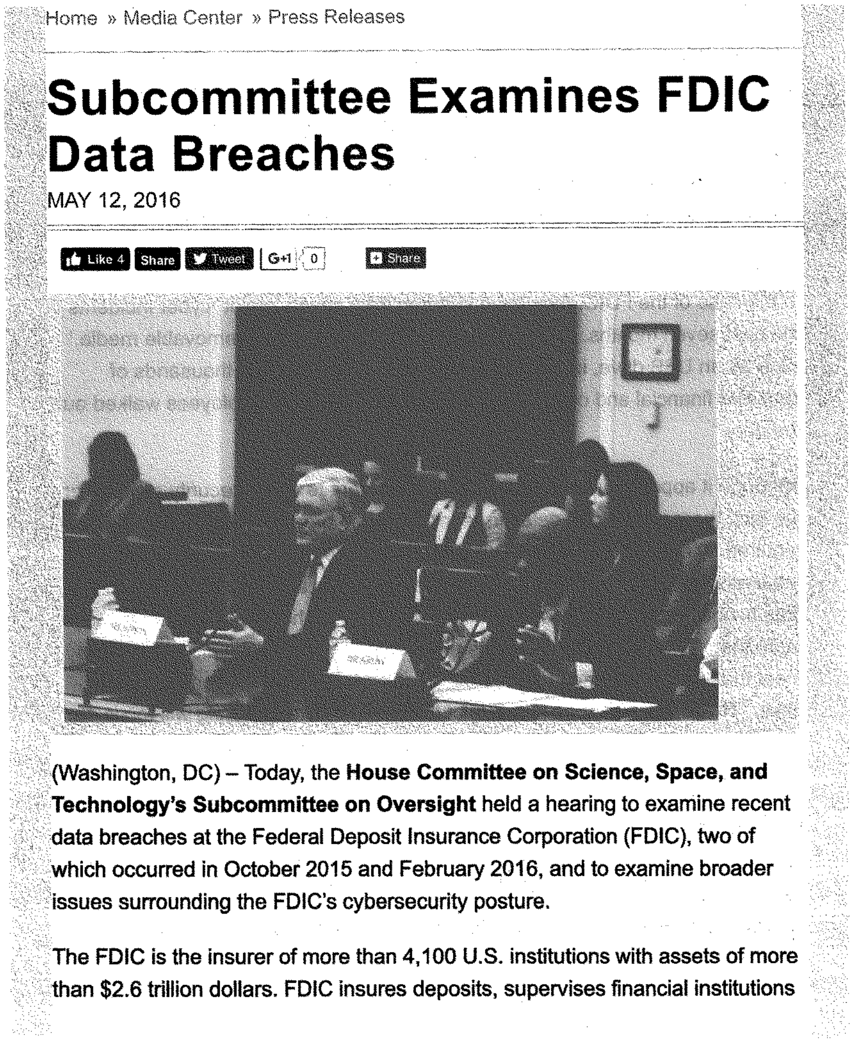
Congressional oversight of these matters is important. I expect that the many IRS hearings being held across Congress this week and next will help improve decision making for information security at the agency. However, I hope that these hearings will also help my colleagues improve Congressional decision making about funding for the Internal Revenue Service.

The Internal Revenue Service's budget has been cut by 17 percent since 2010, after adjusting for inflation, despite a 7 percent increase in the number of tax returns required to be processed, and despite new requirements under the Affordable Care Act and the Foreign Account Tax Compliance Act. These spending cuts, which triggered a 14 percent reduction in IRS employees, are a significant factor in weakened taxpayer services, reduced detection and enforcement of fraudulent claims, and the agency's ability to hire qualified staff needed to fulfill its many requirements under the Federal Information Security and Management Act. And if the House had its way in recent years, the agency's budget would have been cut even further.

So let us be critical of some of the management decisions made at the Internal Revenue Service with respect to protecting taxpayers' personal information. And let us be sure they are putting the people, systems, and processes in place to make better decisions going forward. But let us also be willing to provide the agency with the financial resources and other authorities they need to accomplish these goals.

Finally, cybersecurity is a big challenge that requires effective action by many people and offices at the Office of Management and Budget, the National Institute of Standards and Technology, the Department of Homeland Security, the individual implementing agency, such as the Internal Revenue Service, and their private sector partners. When agencies make poor decisions, we should hold them accountable. However, effective oversight will require more than just a hearing and a press release. If we are serious, this Committee will need to do the hard work of thinking about better, smarter, more effective federal policies to help the agencies meet their information security goals and requirements.

Again, thank you to the witnesses for being here this morning, and I yield back.



Home » Media Center » Press Releases

Subcommittee Examines FDIC Data Breaches

MAY 12, 2016

(Washington, DC) – Today, the **House Committee on Science, Space, and Technology's Subcommittee on Oversight** held a hearing to examine recent data breaches at the Federal Deposit Insurance Corporation (FDIC), two of which occurred in October 2015 and February 2016, and to examine broader issues surrounding the FDIC's cybersecurity posture.

The FDIC is the insurer of more than 4,100 U.S. institutions with assets of more than $2.6 trillion dollars. FDIC insures deposits, supervises financial institutions for soundness, and manages receiverships. Pursuant to its mission, FDIC has access to sensitive information about banks and bank customers.

Ranking Member of the Subcommittee, Don Beyer (D-VA), said in his opening statement, "Defending against cyber threats is a persistent and evolving battle. The cyber hazards that confront the public and private sectors come in various forms. Hackers can and have wreaked havoc on Hollywood studios, global financial institutions, retail outlets, and public agencies alike. No one seems to be immune from the various cyber threats that touch virtually everyone.

In the case of the FDIC, they have suffered from seven 'major' cyber incidents in the past seven months. These breaches involved plugging 'removable media,' such as an USB drive, into an FDIC computer and removing thousands of sensitive financial and other records from the Agency as employees walked out the door."

Although it appears as though FDIC took appropriate cyber security steps after the fact, there was a long delay in reporting these breaches to Congress, as required by OMB Memo 16-03, published on October 30, 2015. This guidance requires federal Agencies to classify cyber breaches as "major incidents" if the data is outside the Agency's control for eight or more hours and if it involves more than 10,000 records or affects more than 10,000 individuals. If incidents meet that criteria they must be reported to Congress within seven calendar days. "That did not happen in either of the two cases this hearing will focus on," said Mr. Beyer, "or the five others that the FDIC just reported to the Committee this week, and I am still unclear why."

Ranking Member Eddie Bernice Johnson (D-TX) said, "In at least one case, according to the FDIC's own records, a former employee who downloaded such data, was evasive about her actions and not cooperative when initially confronted by FDIC staff. Some FDIC employees also suggest it was highly improbable this former employee's actions were accidental. In addition, this former employee is now working for a U.S. subsidiary of a non-U.S. financial services company, which raises additional concerns.

"I hope the IG's office will be able to clarify whether or not all of the recent data breaches were 'inadvertent,' as FDIC has claimed, when the office completes the two audits they are currently working on regarding FDIC's handling of 'major' cybersecurity incidents in the coming weeks. I also hope the IG's office can shed some light on the reasons why the Office of the Chief Information Officer (CIO) and the FDIC failed to inform Congress of these major incidents within the seven-day timeframe required by the guidance from the Office of Management and Budget (OMB) that was issued in late October 2015.

"I believe the FDIC has already taken some positive steps in responding to the recent data breaches, phasing out the use of removable media, for instance. I encourage them to continue to ensure that sensitive data is not intentionally or inadvertently breached. But I would also request the new CIO, Lawrence Gross, to keep Congress appropriately and fully informed, in a timely manner, when 'major' cybersecurity incidents do occur."

Witnesses

- Mr. Lawrence Gross, Jr., *Chief Information Officer and Chief Privacy Officer, FDIC*
- Mr. Fred W. Gibson, *Acting Inspector General*, *FDIC OIG*

OPENING STATEMENT
Ranking Member Don Beyer (D-VA)
of the Subcommittee on Oversight

House Committee on Science, Space, and Technology
Subcommittee on Oversight
"FDIC Data Breaches:
Can Americans Trust that Their Private Banking Information Is Secure?"
May 12, 2016

Thank you Chairman Loudermilk.

Defending against cyber threats is a persistent and evolving battle. The cyber hazards that confront the public and private sectors come in various forms. Hackers can and have wreaked havoc on Hollywood studios, global financial institutions, retail outlets, and public agencies alike. No one seems to be immune from the various cyber threats that touch virtually everyone.

In the case of the Federal Deposit Insurance Corporation, or FDIC, they have suffered from seven "major" cyber incidents in the past seven months. These breaches involved plugging "removable media," such as an USB drive, into an FDIC computer and removing thousands of sensitive financial and other records from the Agency as employees walked out the door. We will be focusing on two of these breaches today as well as the FDIC's cybersecurity practices.

I am glad that FDIC recently installed new software that allowed them to identify these recent breaches and respond to them. Without that technology, known as a Data Loss Prevention (DLP) tool, these incidents, whether inadvertent or intentional, would have gone unnoticed and unaddressed, and Congress would have remained uninformed. I also believe the FDIC Chairman has taken some positive steps in the wake of these breaches, phasing out the use of removable media, such as flash drives and CDs, for instance, that pose increased security risks.

However, I do have questions about why there was such a long delay in notifying Congress about "major" cyber incidents, particularly the one that occurred last October and was not reported to Congress until February 26, 2016. In that instance, it took a Memo from the FDIC Inspector General's office to the FDIC CIO reminding the Agency that they had an obligation to report the incident to Congress. I would add that the IG was not the only one suggesting that the FDIC notify Congress of the incident. It is my understanding that other FDIC employees had also recommended reporting this incident to Congress months earlier.

In addition, I believe the new OMB guidance on "Federal Information Security and Privacy Management Requirements," as detailed in OMB Memo 16-03 last October, is very clear. If it takes eight hours or more to recover sensitive data that comprises 10,000 or more records or affects 10,000 or more people it is considered a "major" cyber incident. Under these guidelines, once an Agency is aware that a breach meets that criteria, the incident should be considered a "major" breach and must be reported to Congress within seven calendar days.

That did not happen in either of the two cases this hearing will focus on, or the five others that the FDIC just reported to the Committee this week, and I am still unclear why. In the October incident the breach included records from eight banks, more than 40,000 individuals and 30,000 entities, including sensitive Bank Currency Transaction Reports and Social Security Numbers. Despite the OMB requirement that Agencies inform Congress of 'major' incidents within seven days, FDIC notified Congress nearly three months after it had enough data to determine that this was a 'major' breach.

I hope that Mr. Gross, the Chief Information Officer (CIO) at FDIC, who is testifying today can help explain FDIC's decision to delay notifying Congress in that October incident. I also hope he can help us understand the Agency's characterization of this incident, which appears to be at odds with some of the information obtained by the Committee. I know the Inspector General has looked at the October incident and the FDIC's response to it, and I am looking forward to IG Gibson's testimony as well.

Lastly, Mr. Gross, I understand you just arrived at FDIC in November and that the CIO's office has suffered from a lack of consistent leadership for some time. You are now the fourth CIO the FDIC has had in the past four years. I hope that you will be able to bring some stability to that office. But equally important is establishing a solid foundation built on reliability and openness with Congress. I hope that you will strive to do that as well.

Thank you to both our witnesses for being here today and I look forward to your testimony.

I yield back.

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Oversight
"FDIC Data Breaches:
Can Americans Trust that Their Private Banking Information Is Secure?"
May 12, 2016

Thank you Chairman Loudermilk, and thank you to our two witnesses for being here today.

All data breaches that expose sensitive personal information should be taken very seriously. In today's digital age our sensitive personal data is everywhere. When we swipe our credit cards at the grocery store, renew our drivers' licenses at the Department of Motor Vehicles and passports at the Department of State, or visit the emergency room at the local hospital or the bank around the corner, our sensitive personal and financial data is processed, stored and entrusted to those entities to safeguard it and ensure it is not inadvertently breached or intentionally stolen.

But that has happened seven times in the past seven months in major cyber breaches at the Federal Deposit Insurance Corporation (FDIC). None of these breaches were the result of sophisticated hackers, foreign adversaries or cyber criminals. And those that downloaded this data, including Social Security Numbers and Suspicious Activity Reports (SARs) did not use high-tech digital tools. They simply plugged in thumb drives and other removable media to their FDIC workstations in the office and downloaded sensitive personal and financial data onto their personal storage devices jeopardized the data security of thousands of individuals, multiple banks and potentially criminal investigations.

In virtually each of these seven instances, the FDIC has said the sensitive data was inadvertently downloaded and that there was no malicious intent. I hope that that is true, but I fear that it is not. In all of these cases the FDIC was able to recover the data, and the former FDIC employees signed affidavits saying they had not shared the data with others.

However, in at least one case, according to the FDIC's own records, a former employee who downloaded such data, was evasive about her actions and not cooperative when initially confronted by FDIC staff. Some FDIC employees also suggest it was highly improbable this former employee's actions were accidental. In addition, this former employee is now working for a U.S. subsidiary of an Indian financial services company, which raises additional concerns.

I would remind FDIC that in 2013 an Inspector General review of another, much more serious, cyber incident at the Agency resulted in one senior official in the CIO's office leaving the Agency and another being demoted. My understanding is that this was not due to FDIC's response to this threat, but the lack of candor by the former officials in the CIO's office in describing the extent of this penetration and the consequences to the Agency to both the Chairman of the FDIC, the IG's office and the Government Accountability Office (GAO).

I hope the IG's office will be able to clarify whether or not all of the recent data breaches were "inadvertent," as FDIC has claimed, or not, when his office completes the two audits they are currently working on regarding FDIC's handling of "major" cybersecurity incidents in the coming weeks. I also hope the IG's office can shed some light on the reasons why the office of the Chief Information Officer (CIO) and the FDIC failed to inform Congress of these major incidents within the seven-day timeframe required by new guidance from the Office of Management and Budget (OMB).

I believe the FDIC has already taken some positive steps in responding to the recent data breaches, phasing out the use of removable media, for instance. I encourage them to continue to ensure that sensitive data is not intentionally or inadvertently breached. But I would also advise the new CIO, Lawrence Gross, testifying before us today, to keep Congress appropriately and fully informed, in a timely manner, when "major" cybersecurity incidents do occur.

Thank you. I yield back.

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
"Evaluating FDIC's Response to Major Data Breaches:
Is the FDIC Safeguarding Consumers' Banking Information?"
July 14, 2016

Thank you Mr. Chairman.

As we have learned over the course of many hearings before this Committee, cybersecurity is a never ending struggle. Public and private entities alike are engaged in a constantly evolving challenge to prevent both intentional data breaches and unintentional dissemination of sensitive information. Since the last hearing we held on data breaches at the Federal Deposit Insurance Corporation (FDIC), just two months ago, 32 million Twitter users had their login credentials compromised, Walmart's corporate headquarters disclosed the unauthorized access to data of more than 27,000 customers, and the medical records of thousands of National Football League (NFL) players were compromised when a laptop computer was stolen from a car.

Today is the Committee's second hearing on the FDIC's handling of several data breaches that occurred since October 2015 when the Office of Management and Budget (OMB) issued new cybersecurity guidance. The OMB memo, known as Memo 16-03, helped to define what constitutes a "major" data breach and requires reporting incidents designated as major to Congress within seven (7) days of such a determination. Data from the FDIC is particularly sensitive, and may include personal banking information and data indicating potential criminal activity, known as Suspicious Activity Reports.

The Agency failed to notify Congress of seven major data breaches within the seven-day timeframe that OMB requires from October 2015 through February 2016. During our Oversight Subcommittee hearing on this topic in May, the FDIC's Chief Information Officer (CIO), described these data breaches as "inadvertent" and occurring without "malicious intent." The FDIC Acting Inspector General Mr. Fred Gibson testified at that hearing and is a witness again today. His office released two audits of the FDIC's data breaches last week and the evidence his office gathered clearly shows that in at least one of the seven breaches the data was not taken accidentally. His office is in the process of conducting a further forensic review of the remaining 6 incidents.

I think it's fair to say that our May hearing yielded bipartisan agreement that the FDIC's interpretation of the OMB guidance was flawed. It is also clear that FDIC did not initially provide all documents responsive to the Committee's requests. However, I do not agree with my Majority colleagues as to what constitutes evidence of intent. The Majority is likely to allege that the CIO intentionally mislead this Committee and that the Agency attempted to obstruct the Committee's investigation into these events. I do not believe the Committee has uncovered convincing evidence to support those allegations. I am not dismissing the testimony of some of the FDIC employees who have been interviewed. But it is our responsibility to make sure we have all of the evidence and have heard from all parties before we begin to wave around serious allegations of criminal intent.

What I do believe is this:

First, the recent reports issued by the Inspector General's office on the data breaches at FDIC point to a series of corrective actions that I hope will improve the agency's ability to appropriately respond to the multiple cybersecurity threats we all face. I do believe the FDIC Chairman takes these issues seriously. He has a strong track record on responding to cybersecurity challenges, including holding his staff accountable.

Second, all federal agencies need a strong, competent and independent Chief Information Security Officer, and I am glad that both the IG's office as well as the Government Accountability Office (GAO) are now engaged in separate reviews about the appropriate role, placement, and authorities of the Chief Information Security Officer at FDIC and other federal agencies.

And finally, while we investigate failures at different agencies to fully and properly implement federal cybersecurity requirements, we should also support agency efforts to continue to strengthen their cybersecurity posture as the technologies and threats rapidly evolve around them.

I look forward to hearing from both Chairman Gruenberg and Acting IG Mr. Gibson.

I yield back.