THE CURRENT STATE OF PRIVATE-SECTOR ENGAGEMENT FOR CYBERSECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MARCH 9, 2017

Serial No. 115–7

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE
26–905 PDF WASHINGTON : 2017

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

COMMITTEE ON HOMELAND SECURITY

Michael T. McCaul, Texas, *Chairman*

Lamar Smith, Texas
Peter T. King, New York
Mike Rogers, Alabama
Jeff Duncan, South Carolina
Tom Marino, Pennsylvania
Lou Barletta, Pennsylvania
Scott Perry, Pennsylvania
John Katko, New York
Will Hurd, Texas
Martha McSally, Arizona
John Ratcliffe, Texas
Daniel M. Donovan, Jr., New York
Mike Gallagher, Wisconsin
Clay Higgins, Louisiana
John H. Rutherford, Florida
Thomas A. Garrett, Jr., Virginia
Brian K. Fitzpatrick, Pennsylvania

Bennie G. Thompson, Mississippi
Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Cedric L. Richmond, Louisiana
William R. Keating, Massachusetts
Donald M. Payne, Jr., New Jersey
Filemon Vela, Texas
Bonnie Watson Coleman, New Jersey
Kathleen M. Rice, New York
J. Luis Correa, California
Val Butler Demings, Florida
Nanette Diaz Barragán, California

Brendan P. Shields, *Staff Director*
Kathleen Crooks Flynn, *Deputy General Counsel*
Michael S. Twinchek, *Chief Clerk*
Hope Goins, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

John Ratcliffe, Texas, *Chairman*

John Katko, New York
Daniel M. Donovan, Jr., New York
Mike Gallagher, Wisconsin
Clay Higgins, Louisiana
Thomas A. Garrett, Jr., Virginia
Brian K. Fitzpatrick, Pennsylvania
Michael T. McCaul, Texas *(ex officio)*

Cedric L. Richmond, Louisiana
Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Val Butler Demings, Florida
Bennie G. Thompson, Mississippi *(ex officio)*

Brett DeWitt, *Subcommittee Staff Director*

CONTENTS

Page

Statements

Witnesses

Appendix

THE CURRENT STATE OF PRIVATE-SECTOR ENGAGEMENT FOR CYBERSECURITY

Thursday, March 9, 2017

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:09 a.m., in room HVC–210, Capitol Visitor Center, Hon. John Ratcliffe (Chairman of the subcommittee) presiding. Present: Representatives Ratcliffe, Katko, Donovan, Gallagher, Fitzpatrick, Richmond, Jackson Lee, Langevin, and Demings.

Mr. RATCLIFFE. The Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection will come to order.

The subcommittee is meeting today to receive testimony regarding the current state of DHS's private sector engagement for cybersecurity.

I now recognize myself for an opening statement.

Cybersecurity touches every aspect of the world that we live in. It is central to every sector of our economy. It is vitally important to the protection of all Americans' most sensitive information and it is one of the foremost National security challenges of our time.

Our collective ability to combat these threats with Government and the private sector working together will be one of the defining public policy challenges of our generation.

Today, the Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection meets to hear from key stakeholders on the current state of private-sector engagement for DHS's cybersecurity mission.

As Chairman of this subcommittee, I don't take the responsibility that we as lawmakers in this room have lightly. In a world of rapidly-evolving threats, we have been entrusted to be part of the solution, and I believe that today's hearing will be an important piece of this on-going effort.

DHS's cyber mission includes a robust portfolio of existing private-sector partnerships, including information-sharing and analysis organizations, the Cyber Information Sharing and Collaboration Program, Sector Coordinating Councils and the Automated Indicator Sharing Program.

Specifically, we hope to learn how these partnerships can be improved and what more DHS can be doing to ensure that these programs and activities are meaningful, substantive, and effective.

Today, the private-sector entities, including U.S. critical infrastructure owners and operators, are on the front line of conflict in cyber space. Our civilian networks face countless attacks every day from bad actors who seek to infiltrate our trusted systems, cripple our commerce, and expose Americans' personal information.

Every day, these bad actors are using more advanced tactics, techniques, and procedures, and higher-quality information. It is only through constant and vigilant innovation that their attacks can be prevented, identified, and mitigated.

While DHS has made headway in this space and has strengthened many initiatives in its role as the civilian interface and coordinator across 16 critical infrastructure sectors for cybersecurity, very clearly more work needs to be done. It is not enough to simply have programs in place. Instead, we must be constantly measuring, benchmarking, and setting goals associated with their outcomes.

Additionally, DHS needs to become fully operational so that it can effectively carry out the cybersecurity authorities that Congress deliberately gave the Department just over a year ago.

Today is the start of a new conversation that needs to occur in a new world on this new battlefield, and the start of a new administration provides a clean slate, a perfect opportunity to regroup and reassess before moving forward, an opportunity to ensure that our efforts and resources are aligned with the threat landscape that we face right now.

Several weeks ago in a homeland security hearing in this room, I was pleased to have the opportunity to discuss with Secretary Kelly the importance of DHS's cyber mission. What I told him and what I know the rest of this subcommittee joins me in reinforcing is that we stand ready to pedal as fast as his agency and the entire Trump administration demands because the stakes are too high to do anything less right now.

In the cyber domain, we are constantly learning new lessons. It is only by incorporating the knowledge into existing programs and processes that we can continue to move toward greater collaboration and better-secured networks. Because, while the private sector is on the front lines of our cyber challenges, the Federal Government, and DHS in particular, has an important role to play as a force multiplier to provide the private sector with every advantage available to defend itself.

In the 115th Congress, this subcommittee will be legislating and conducting rigorous oversight to further strengthen DHS's civilian cyber mission. While the various DHS touch-points with the private that we will discuss today range in levels of sophistication and size of participant base, they all depend on quality information flowing at a rate that makes it timely and actionable.

Marked changes in the security of our country's cybersecurity posture will only occur in concert with the advancement of the collaborations that we are going to be discussing today. The combination of information, capacity, and technical expertise needs to be leveraged in partnership at every turn.

We look forward to hearing from the witnesses on these private-sector engagement efforts at DHS. Our goal on this topic is to make sure that the private sector has every opportunity and every reason to take full advantage of DHS's cybersecurity programs so we can continue to work to secure cyber space.

Again, thanks to our witnesses for your willingness to be here today to share your expertise.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

Cybersecurity touches every aspect of the world we live in. It's central to every sector of our economy. It's vitally important for the protection of all Americans' most sensitive information, and it's one of the foremost National security challenges of our time. Our collective ability to combat these threats—with the Government and the private sector working together—will be one of the defining public policy challenges of our generation.

Today the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection meets to hear from key stakeholders on the current state of private-sector engagement for DHS's cybersecurity mission. As Chairman of this subcommittee, I don't take the responsibility the lawmakers in this room have lightly. In a world of rapidly-evolving threats, we have been entrusted to be part of the solution, and I believe today's hearing will be an important piece of this on-going effort.

DHS's cyber mission includes a robust portfolio of existing private-sector partnerships—including Information Sharing and Analysis Organizations, the Cyber Information Sharing and Collaboration Program, Sector Coordinating Councils, and the Automated Indicator Sharing Program. Specifically, we hope to learn how these partnerships can be improved and what more DHS can be doing to ensure that these programs and activities are meaningful, substantive, and effective.

Today, private-sector entities—including U.S. critical infrastructure owners and operators—are on the front line of the conflict in cyber space. Our civilian networks face countless attacks every day from bad actors who seek to infiltrate our trusted systems, cripple commerce, and expose Americans' personal and sensitive information. Bad actors are using more advanced tactics, techniques, and procedures, and higher quality information. It is only through constant and vigilant innovation that their attacks can be prevented, identified, and mitigated.

While DHS has made headway in this space and has strengthened many initiatives in its role as the civilian interface and coordinator across the 16 critical infrastructure sectors for cybersecurity, more work needs to be done. It is not enough to simply have programs "in place." Instead, we must be constantly measuring, bench-marking, and setting goals associated with their outcomes. Additionally, DHS needs to become fully operational so it can most effectively carry out the cybersecurity authorities Congress deliberately gave the Department just over a year ago.

Today is the start of a conversation that needs to occur in this new world with this new battlefield. And the start of a new administration provides a clean slate—a perfect opportunity to regroup and reassess before moving forward. An opportunity to ensure that our efforts and resources are aligned with the threat landscape we face.

Several weeks ago in a Homeland Security hearing, I was pleased to have the opportunity to discuss with Secretary Kelly the importance of DHS's cyber mission. What I told him, and what I know the rest of this subcommittee joins me in reinforcing, is that we stand ready to pedal as fast as his agency and the Trump administration demands. Because the stakes are too high to do anything less.

In the cyber domain, we are constantly learning new lessons, and it is only by incorporating that knowledge into existing programs and processes that we can continue to move toward greater collaboration and better-secured networks. Because while the private sector is on the front lines of our cyber challenges, the Federal Government, and DHS in particular, has an important role to play as a force multiplier to provide the private sector with every advantage available to defend itself.

In the 115th Congress, this subcommittee will be legislating and conducting rigorous oversight to further strengthen DHS's civilian cyber mission. While the various DHS touchpoints with the private that we will discuss today range in levels of sophistication and size of participant base, they all depend on quality information flowing at a rate that makes it timely and actionable.

Marked changes in the security of our country's cybersecurity posture will only occur in concert with the advancement of the collaborations that we will be discussing today. The combination of information, capacity, and technical expertise needs to be leveraged in partnership at every turn.

We look forward to hearing from the witnesses on these private-sector engagement efforts at DHS. Our goal on this topic is to make sure that the private sector has every opportunity and every reason to take full advantage of DHS cybersecurity programs so we can continue to work together to secure cyber space.

Again, thank you to our witnesses for your willingness to share your expertise.

Mr. RATCLIFFE. The Chair now recognizes the Ranking Minority Member of the subcommittee, the gentleman from Louisiana, Mr. Richmond, for his opening statement.

Mr. RICHMOND. Thank you, Chairman Ratcliffe, for holding this hearing to examine how the Department and the private sector work together on cybersecurity.

As this is the first subcommittee hearing, I would like to start off by welcoming the gentlelady from Florida, Mrs. Val Demings, to the subcommittee.

Cybersecurity issues dominated the 2016 election, from the security of Secretary Clinton's server to Vladimir Putin ordering cyber attacks on the U.S. election systems to Wikileaks publishing the private emails of prominent Democratic figures. America got a crash course in cybersecurity.

Before he was sworn in, President Trump said he would direct the Department of Defense and the Joint Chiefs to develop a comprehensive plan to protect America's vital infrastructure from cyber attacks and all other forms of attacks. This was on his first day in office.

While I share the President's desire to better protect critical infrastructure, directing the Pentagon to take on cybersecurity in the private sector would represent a radical departure from how the Government manages cybersecurity.

Since 2001, DHS has been the lead agency responsible for coordinating Federal efforts to protect critical infrastructure and, in that capacity, has made major strides in cyber information sharing among critical infrastructure owners and operators.

Then, 2 years ago, with input from some of the witnesses assembled on this panel, legislation was signed into law codifying DHS's role as the lead civilian interface for information sharing. Since that time, DHS has ramped up its efforts to partner with critical infrastructure.

We often say on this committee that the threat landscape is constantly evolving. When it comes to cybersecurity, the volume, the complexity, and scale of attacks grow exponentially with each passing day.

To meet this challenge, the culture around cyber information sharing needs to shift, just as it needed to shift after 9/11 when Federal law enforcement and intelligence agencies moved from a need-to-know to a need-to-share culture.

As we work to enhance the quality of information sharing, we must not lose sight of the obligations of all involved to protect the personal information of Americans or impacted networks.

I am glad to see that Ms. Greene is here to talk with us about these obligations. I also look forward to talking with all the witnesses about what, from their perspectives, DHS and specifically NCCIC could be doing better.

Last year, Congress enacted legislation I authored to make sure DHS is carrying out its diverse portfolio of cybersecurity responsibilities in a strategic manner. In a couple of weeks, DHS should be transmitting to Congress its first ever Department-wide cybersecurity strategy. When we see the strategy, I may want to engage with you all on your thoughts.

Finally, while I recognize that the long-awaited Executive Order on cybersecurity has not yet been issued, it will be good to hear your thoughts on what we have seen so far from President Trump's administration on cybersecurity.

With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

MARCH 9, 2017

Cybersecurity issues dominated the 2016 election. From the security of Secretary Clinton's server, to Vladimir Putin ordering cyber attacks on U.S. election systems, to WikiLeaks publishing the private emails of prominent Democratic figures—America got a crash-course in cybersecurity.

Before he was sworn in, President Trump said he would direct the Department of Defense and the Joint Chiefs to develop "a comprehensive plan to protect America's vital infrastructure from cyber attacks, and all other form of attacks" on his first day in office.

While I share the President's desire to better protect critical infrastructure, directing the Pentagon to take on cybersecurity in the private sector would represent a radical departure from how the Government manages cybersecurity.

Since 2001, DHS has been the lead agency responsible for coordinating Federal efforts to protect critical infrastructure and, in that capacity, has made major strides in cyber information sharing among critical infrastructure owners and operators.

Then two years ago, with input from some of the witnesses assembled on this panel, legislation was signed into law codifying DHS's role as the lead civilian interface for information sharing. Since that time, DHS has ramped up its efforts to partner with critical infrastructure.

We often say on this committee that the threat landscape is constantly evolving. When it comes to cybersecurity, the volume, complexity, and scale of attacks grow exponentially with each passing day. To meet this challenge, the culture around cyber information sharing needs to shift—just as it needed to shift after 9/11, when Federal law enforcement and intelligence agencies moved from a "need to know" to "need to share" culture.

As we work to enhance the quality of information sharing, we must not lose sight of the obligations of all involved to protect the personal information of Americans on impacted networks. I am glad that Ms. Green is here to talk with us about these obligations. I also look forward to talking with all the witnesses about what, from their perspectives, DHS (and specifically the NCCIC) could be doing better.

Last year, Congress enacted legislation I authored to make sure DHS is carrying out its diverse portfolio of cybersecurity responsibilities in a strategic manner. In a couple of weeks, DHS should be transmitting to Congress it's first-ever Department-wide cybersecurity strategy. When we see the strategy, I may want to engage with you on your thoughts.

Finally, while I recognize that the long-awaited Executive Order on cybersecurity has not yet been issued, it would be good to hear your thoughts on what we've seen so far from President Trump on cybersecurity.

Mr. RATCLIFFE. I thank the gentleman.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statements of Ranking Member Thompson and Honorable Jackson Lee follow:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 9, 2017

Cybersecurity is at the forefront of American politics in a way that, in my 24 years in Congress, I have never seen. On this committee, we regularly gather to hear from cybersecurity leaders on the most pressing security vulnerabilities to our Nation and the novel ways our enemies seek to exploit them. This past fall, details began to emerge about an entirely new attack vector—a hacking campaign designed to impact the Presidential election.

Even before the election, the Secretary of Homeland Security and the Director of National Intelligence warned that Russian President Vladimir Putin directed hackers to penetrate the email accounts of high-ranking Democratic party officials to acquire information to be used to embarrass and undermine the candidacy of Secretary Clinton.

The full scale of this state-sponsored hacking campaign is still not fully known but what we do know is that in addition to hacking private email accounts of prominent Democrats, the Russian hackers tried infiltrate vital networks and equipment maintained by state election authorities.

The Russian cyber campaign sought to strike at the heart of our democracy. As such, legitimate questions about contacts between President Trump's inner circle and associates of the Putin regime need to be brought to light. That is why I support an independent 9/11-style commission to investigate the Russian cyber campaign.

It has been disheartening to see President Trump display a somewhat dismissive attitude about this very significant cyber attack, even as DHS and its Federal partners work to raise the level of cyber awareness and hygiene across the country.

I continue to be troubled by how long it took President Trump to accept the facts presented by the intelligence committee about the Russians orchestrating the hacking campaign. What seems to be lost on this man who has repeatedly expressed support for our Government using cyber offensive capabilities is that there can be no retribution without attribution.

I am pleased that we have with us today representatives from private sector that know a thing or two about the nature of the evolving cyber threat and the importance of attribution.

I would like to also take a moment to welcome Robyn Greene who this committee has come to count on for counsel when it comes the privacy challenges associated with cyber information sharing. I look forward to hearing from the panel on how DHS helps private entities secure their networks against intrusion.

Statement of Honorable Sheila Jackson Lee

March 9, 2017

Chairman Ratcliffe and Ranking Member Richmond, thank you for convening this opportunity for the Homeland Security Committee Subcommittee on Cybersecurity & Infrastructure Protection on the topic of "The Current State of DHS Private Sector Engagement for Cybersecurity."

Today's hearing will give Members an opportunity to hear from individuals outside the Government about how the Department of Homeland Security (DHS) works with private entities to improve their network security and contribute to the overall health of the cyber ecosystem.

I thank today's witnesses :

- Daniel Nutkis, CEO, HITRUST Alliance
- Scott Montgomery, V.P. and Chief Technical Strategist, Intel Security Group, Intel Corporation
- Jeffrey Greene, Senior Director, Global Government Affairs & Policy, Symantec
- Ryan Gillis, V.P. of Cybersecurity Strategy & Global Policy, Palo Alto Networks
- Robyn Greene, Policy Counsel & Government Affairs Lead, New America—Open Technology Institute (Democratic Witness).

In the first few weeks of this Congress I introduced a number of measures on the topic of cybersecurity to address gaps in our Nation's cyber defensive posture:

- SCOUTS Act—H.R. 940;
- CAPITALS Act—H.R. 54;
- SAFETI Act—H.R. 950;
- Terrorism Prevention and Critical Infrastructure—H.R. 945; and
- Cybersecurity and Federal Workforce Enhancement Act—H.R. 935.

H.R. 940, the "Securing Communications of Utilities from Terrorist Threats" or the "SCOUTS Act," directs the Secretary of Homeland Security, in coordination with the sector-specific agencies, to work with critical infrastructure owners and operators and State, local, Tribal, and territorial entities to seek voluntary participation on ways that DHS can best defend against and recover from terrorist attacks that could have a debilitating impact on National security, economic stability, public health and safety, or any combination thereof.

H.R. 940, is relevant to today's hearing because it addresses the need for a two-way communication process that enables private-sector participants in information-sharing arrangements with DHS to communicate their views on the effectiveness of the information provided; the method of information sharing; and their particular needs as time passes.

Specifically the bill establishes voluntary listening opportunities for sector-specific entities to communicate their challenges regarding cybersecurity, including what needs they may have for critical infrastructure protection; and how DHS is helping or not helping to meet those needs.

The Society of Maintenance and Reliability Professionals have endorsed H.R. 940, and input on the legislation included the Edison Electric Institute, an electric utility association.

H.R. 54, the Department of Homeland Security's Cybersecurity Asset Protection of Infrastructure under Terrorist Attack Logistical Structure or CAPITALS Act, which directs the Department of Homeland Security (DHS) to produce a report to Congress regarding the feasibility of establishing a DHS Civilian Cyber Defense National Resource.

H.R. 950, requires a report and assessment regarding Department of Homeland Security's response to terrorist threats to Federal elections. The Comptroller General of the United States is directed to conduct an assessment of the effectiveness of Department of Homeland Security actions to protect election systems from cyber attacks and to make recommendations for improvements to the actions taken by DHS if determined appropriate.

H.R. 935, The "Cybersecurity and Federal Workforce Enhancement Act" identifies and trains people already in the work force who can obtain the skills to address our Nation's deficit in the number of workers and positions available for those with needed skills.

H.R. 940, the "Securing Communications of Utilities from Terrorist Threats" or the "SCOUTS Act," is the relevant to today's hearing because this bill focuses on the communications sent by DHS to sector-specific entities and the ability of these entities to communicate to the agencies their perspective on the usefulness of the information; the form of communication that would be most helpful; and requires a report to Congress by DHS on the views of critical infrastructure owners and operators on the information-sharing process related to cybersecurity.

Later today I will be introducing the Prevent Zero Day Events Act, which will help DHS in working with sector-specific entities to better understand the detection of undiscovered or unreported vulnerabilities in software and firmware that if exploited could pose a serious threat to our Nation's power grid; telecommunications systems; financial system; health care delivery; water supply or disrupt the ability of Federal agencies to function.

I look forward to your testimony and the testimony of the second panel for today's hearing.

Thank you.

Mr. RATCLIFFE. We are pleased today to have a very distinguished panel of witnesses before us on this vitally important topic. Mr. Daniel Nutkis is the chief executive officer of the HITRUST Alliance.

Dan, good to have you back before our committee.

Mr. Scott Montgomery is the vice president and chief technical strategist at Intel Security Group.

We are glad to have you, Mr. Montgomery.

Mr. Jeff Greene is the senior director of global government affairs and policy at Symantec.

Jeff, good to see you again. Thanks for being here.

Mr. Ryan Gillis is the vice president of cybersecurity strategy and global policy at Palo Alto Networks.

Mr. GILLIS. welcome and we look forward to your testimony today.

Last but not least, Ms. Robyn Greene is the policy counsel and government affairs lead of the Open Technology Institute at New America.

Welcome back, Ms. Greene.

I would now like to ask the witnesses all to stand and raise your right hand so that I can swear you in to testify.

[Witnesses sworn.]

Mr. RATCLIFFE. Please let the record reflect that the witnesses all answered in the affirmative. You may be seated.

The witnesses' full written statements will appear in the record. The Chair now recognizes Mr. Nutkis for 5 minutes for an opening statement.

STATEMENT OF DANIEL NUTKIS, CHIEF EXECUTIVE OFFICER, HITRUST ALLIANCE

Mr. NUTKIS. Good morning, Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee.

I am pleased to appear today to discuss the health industry's experiences in engaging with the Department of Homeland Security relating to cyber information sharing and other cyber initiatives, and a role we believe provides the greatest benefit to industry.

For a little context for the subcommittee, for the last 10 years we have developed and updated a privacy and security framework and risk management practices for the health care industry, which were the most widely adopted. Five years ago, we established the HITRUST CTX which is the health care industry's most active and robust information sharing and analysis organization, or ISAO.

While I prepared my written statement for the record, in my testimony today I will highlight how HITRUST helps elevate the industry's cyber awareness, improves cyber preparedness, and strengthens the risk management posture of the health care industry.

At today's hearing, I would like to highlight three programs we have pioneered with industry that showcase the positive efforts under way in collaboration with DHS, and then speak to our concerns over Government's interference and disregard for key industry cybersecurity efforts.

The first is the enhanced indicator of compromise program, the second is the sector guidance for implementing the NIST cybersecurity framework, and the third is the automated indicator sharing with DHS. I will touch on each one of these briefly.

A review in 2015 highlighted a number of gaps and deficiencies in our cyber information sharing approaches and led to the development of an enhanced criteria to improve the collection and sharing of IOCs and maximize its benefits. The net results is that the HITRUST CTX, which is part of our ISAO, continues to improve on the number of unique IOCs it shares across the health care industry, going from 186 unique IOCs in September 2015 to over 5,100 in September 2016. Additionally, there were substantial improvements in timeliness, accuracy, and usability.

I reference this program to illustrate that the private sector is willing to do its part in facilitating the collection and dissemination of IOCs and other cyber threat information. I see DHS as having a vital role in facilitating the collection and dissemination of other information-sharing organizations in a streamlined, secure, and efficient manner.

Last year, the Health and Public Health Sector Coordinating Council and the Government Coordinating Council with input from

HITRUST and other sector members, including the DHS critical infrastructure cyber community, developed the health sector implementation guide for the NIST cybersecurity framework.

DHS was an integral partner and commenter during the development of the sector guide. It should be noted that the HPHSCC, which was formed under the DHS Critical Infrastructure Sector Partnership Program, is an example of industry innovation, leadership, and collaboration across the entire industry on a number of topics relevant to critical infrastructure, including cyber.

The HITRUST CTX is fully integrated with AIS and supports bidirectional cyber threat indicator exchange to better aid organizations in reducing their cyber risk. In fact, HITRUST was the first non-Government entity connected to and sharing cyber threat indicators with DHS AIS program. HITRUST believes DHS acting as the hub for cyber information sharing benefits the entire industry. Our engagement with DHS has been both collaborative and productive.

Despite all the progress the public/private sector has made in recent years, there are Government efforts underway to undermine private-sector information-sharing programs and ISAOs like that of HITRUST.

Even though CISA and the Executive Order made clear that ISAOs would be established and enable private companies to decide which ISAO to engage when sharing with DHS, there are efforts to require health care organizations to only share information directly with the Department of Health and Human Services or their designated ISAO, an agency not even identified in CISA's affording safe harbor liability protections.

This is certainly troublesome and we find these efforts alarming and are contrary to the original intent of CISA. We recognize that there is a large role for Government to play in supporting information sharing. The private sector should be considered an equal party and the Government partners should take a universal and consistent approach when engaging with industry.

We recognize that each industry is unique with regards to CTI sharing. In health care, they include health information, organizational size, technical maturity, control systems, medical devices, but that doesn't warrant interjecting another intermediary and certainly not one that regulates, audits, and has responsibility for imposing fines and other financial penalties.

The market should drive innovation and Government should promote the role of industry without changing the rules.

Thank you again for the opportunity to share these insights. With that, Mr. Chairman, I am pleased to answer the committee's questions.

[The prepared statement of Mr. Nutkis follows:]

Prepared Statement of Daniel Nutkis

March 9, 2017

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee, I am pleased to appear today to discuss the health industry's experiences in engaging with the Department of Homeland Security relating to cyber information sharing and other cyber initiatives and the role we believe provides the greatest benefit to industry. I am Daniel Nutkis, CEO and founder of the Health Information Trust Alliance, or HITRUST. HITRUST was founded in 2007, after industry recognized the need to formally and collaboratively address information privacy and security for health care stakeholders representing all segments of the industry and organizational sizes. HITRUST endeavored—and continues to endeavor—to elevate the level of information protection in the health care industry and those it collaborates with, ensuring greater collaboration between industry and Government, raising the competency level of information security professionals, while maintaining trust with consumers and patients regarding their health information, and promoting cyber resilience of industry organizations.

In my testimony today, I will highlight how HITRUST helps elevate the industry's cyber awareness, improve cyber preparedness and strengthen the risk management posture of the health care industry. In particular, I will explain how programs like cyber information sharing, cyber threat catalogues, and guidance on implementing the NIST Cybersecurity Framework[1] are integral to this process, as is the role for the Department of Homeland Security.

In 2012, HITRUST established the HITRUST Cyber Threat XChange or CTX, the health industry's Information Sharing and Analysis Organization, or ISAO. The HITRUST CTX has consistently and effectively enabled cyber information sharing across the entire industry and with Government, while continuously evaluating and enhancing its services to ensure better collection, analysis, and consumption of actionable cyber threat information.

At today's hearing, I would like to highlight three programs we have pioneered with industry that showcase the positive efforts under way in collaboration with DHS and then speak to our concerns over Government's interference, underperformance or disregard as to the industry's cybersecurity efforts. Concerns, I anticipate this committee and the new administration will share and appropriately address.

The first of the programs is the Enhanced Indicator of Compromise (IOC) Program; second, is Sector Guidance for Implementing the NIST Cybersecurity Framework; and third, is Automated Indicator Sharing with DHS. I will touch on each one of these briefly.

ENHANCED INDICATOR OF COMPROMISE (IOC) PROGRAM

Since it began an IOC-sharing program over 6 years ago, HITRUST has been a leader in information sharing and continuously evaluates the effectiveness of its cyber information-sharing program against stated goals. A review in 2015 highlighted a number of gaps and deficiencies in our cyber information-sharing approaches, and led to the development of an Enhanced IOC criteria to improve the collection and sharing of IOCs and maximize its benefits. These criteria defined specific requirements in terms of completeness, timeliness, and accuracy of IOCs contributed. We then established a pilot to evaluate the effectiveness of this approach, which demonstrated significant improvements, highlighted in the findings below:

1. During the pilot period, over 80% of the IOCs collected were unique and not seen or known by any other open-source, commercial, DHS CISCP, or user-contributed feeds available to the HITRUST CTX.
2. The pilot group of eight organizations using Enhanced IOC sharing reported 45% more IOCs than a comparable group of over 800 existing CTX participants using current sharing practices.
3. 100% of organizations reported IOCs to the HITRUST CTX compared to only a small percentage of organizations—5%—that contributed using current sharing practices during the same period.
4. IOCs were reported to the HITRUST CTX on average 13.1 days before being seen or identified by any other open-source, commercial, DHS CISCP, or user-contributed feeds to the HITRUST CTX. Some indicators were seen in the pilot program up to 123 days before being reported by other feeds.
5. IOCs were submitted in a matter of minutes to the HITRUST CTX compared to an average of 7 weeks after detection using current sharing practices.
6. 95% of the IOCs contributed to the HITRUST CTX had metadata (e.g., malicious IPs, URLs or domains) that made them actionable for use by others, which is defined as being useful in allowing preventative or defensive action to be taken without a significant risk of a false positive. Using current sharing practices, only 50% of the IOCs contributed to the HITRUST CTX were considered actionable.

The net result is that the HITRUST CTX continues to improve on the number of unique IOCs it shares across health care organizations each month—going from 186 unique IOCs in September 2015 to 5,158 in September 2016.

[1] *https://www.us-cert.gov/ccubedvp.*

In addition, the enhanced IOC pilot improved situational awareness and predictive threat modeling with the ability to correlate IOCs and Indicators of Attack (IOAs) between organizations, identify attack patterns, and alert participants about IOCs and IOAs. These results are positive with regards to mitigating cyber risk, but don't speak to the investment required.

To better understand the return on investment, HITRUST is undertaking a study to quantify the value of information sharing as a tool in mitigating cyber risk, to aid organizations in prioritizing and justifying their participation. We are undertaking an ROI study to evaluate information sharing and the incremental benefits of leveraging the Enhanced IOC criteria. We look forward to updating the committee on the results of this study in the near future.

Another important finding is that threat information sharing does not need to be limited to the largest organizations and that the scalable sharing of IOCs can be achieved throughout health care organizations of varying size, intelligence appetite, and the maturity of an organization's security program. This was evaluated by integrating the HITRUST CTX with the CyberAid program.[2]

The results of the Enhanced IOC Collection Pilot indicate that health care organizations can dramatically improve the timeliness, completeness, usability, and volume of IOCs contributed to the HITRUST CTX by implementing the enhanced IOC criteria. In response to these findings, HITRUST is expanding the Enhanced IOC program and announced enhancements to the CTX platform to aid organizations in reducing their cyber risk.

I reference this program to illustrate that the private sector is willing to do its part in facilitating the collection and dissemination of IOCs and other cyber threat information (CTI), and sees DHS as having a vital role in facilitating the collection and dissemination from other information-sharing organizations in a streamlined and efficient manner.

SECTOR GUIDANCE FOR IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK

Last year, the Health and Public Health Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), along with input from HITRUST, and other sector members including the DHS Critical Infrastructure Cyber Community (C3) developed the Health Sector implementation guide for the NIST Cybersecurity Framework, specifically referred to as "Healthcare Sector Cybersecurity Framework Implementation Guide."

The Sector Guide supports implementation of a sound cybersecurity program that addresses the five core function areas of the NIST framework to ensure alignment with National standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with other information security and privacy risk management activities in the Health Care Sector. The Health Care Sector leverages the HITRUST risk management framework, including the HITRUST CSF and CSF Assurance Program to effectively provide the sector's implementation of the NIST Cybersecurity Framework.

DHS was an integral partner and commenter during the development of the Sector Guide. The HPH SCC, which was formed under the DHS Critical Infrastructure Sector Partnership Program, is an example of industry innovation, leadership, and collaboration across the entire industry on a number of topics relevant to the protection of critical infrastructure including cyber.

AUTOMATED INDICATOR SHARING (AIS)

The HITRUST CTX is fully integrated with AIS and supports bi-directional cyber threat indicator exchange to better aid organizations in reducing their cyber risk. In fact, HITRUST was the first non-Government entity connected to and sharing cyber threat indicators with the DHS AIS Program.

AIS has the potential to facilitate the sharing of crucial cyber threat information from across organizations, corporations, and Federal agencies in real time. Given the recent rise in cyber threats targeting the health care industry, HITRUST believes bi-directional integration into the AIS program will ensure relevant and timely CTI from HITRUST and Government is available to all industries—ultimately bolstering the overall cyber posture of the Nation's critical infrastructure.

Of note, HITRUST's role as an ISAO with strong industry engagement enabled us to quickly and efficiently address any concerns regarding the liability of sharing with Government. It was also our continued evaluation and enhancements to our infrastructure with our technology partners that enabled us to integrate with AIS

[2] HITRUST CyberAid is an example of enabling information sharing with smaller organizations—*https://hitrustalliance.net/documents/cyberaid/CyberAidInfographicPresentation.pdf.*

and meet the future needs of information sharing. Both the Cybersecurity Act of 2015 (CISA) and Executive Order (EO) 13691 intended ISAOs to take up this role in an effort to help move the private sector in the right direction and enable them to robustly engage with Government. AIS integration demonstrates that HITRUST, with its DHS partnership, continues to evolve, improve, and lead by innovating and ensuring cyber threat information sharing is providing the most value to the broadest group of constituents while reducing overall cyber risk.

As a non-Governmental organization, sharing with AIS was not without initial challenges, we did encounter some technical and operational issues. They have since been addressed, but we would encourage greater engagement by DHS with AIS participants to ensure alignment with on-going and future requirements.

HITRUST is of the opinion that DHS—acting as the hub for cyber information sharing—benefits the entire industry, and our engagement with the DHS AIS has been both cooperative and very productive.

However, despite all the progress the public and private sectors have made in recent years, as I referenced earlier, there are Government efforts underway to undermine private-sector information-sharing programs and ISAOs like that of HITRUST. Even though CISA and the EO make clear that ISAOs would be established and enable private companies to decide which ISAO to engage when sharing with DHS, there are efforts under way that will deviate from this effort by requiring health care organizations to only share information directly with the Department of Health and Human Services—an agency not even identified in CISA as affording safe harbor liability protections.

This is certainly troublesome, as we can all agree that CISA placed DHS at the center of information sharing with the private and civilian sector. HITRUST supported this effort enthusiastically and continues to do so. In fact, as we have outlined in our testimony, we have invested heavily in elevating our information-sharing capabilities to help industry achieve the goal of working collaboratively with the Government.

Since HITRUST has led the industry in the collection of IOCs through the development of enhanced standards and collection practices, and was the first health care organization to begin sharing bi-directionally with DHS's AIS program, we find these efforts unnerving as they are certainly contrary to the original intent of CISA and Government's commitment to partner with industry through the ISAO program.

HITRUST has always approached its role as an ISAO with the entrepreneurial spirit of innovation and leadership. While we recognize that there is a large role for Government to play in supporting information sharing and ensuring liability protection, the private sector should be considered an equal partner, and our Government partners should take a universal and consistent approach when engaging with industry.

We appreciate and recognize that each industry has unique dynamics and challenges with regards to CTI sharing, in health care they include organizational size, technical maturity, medical devices, and other control systems, but that doesn't warrant interjecting another intermediary and certainly not one that regulates and has responsibility for fines and other financial penalties.

HITRUST was an early supporter of CISA and continues to support the role of Government to foster transparency by establishing guidance, clarifying roles and responsibilities, and encouraging industries and segments to determine how to engage more extensively based on their value and performance. The market should drive innovation and Government should promote the role of industry without changing the rules. We are seeing the opposite occur, and this was never the intent of CISA or the Executive Order. CISA established a role for the private sector around cyber information sharing, a role for ISAOs and associated liability protections offered through DHS. Unfortunately after supporting, committing, and engaging along that path, we find the Department of Health and Human Services establishing guidelines and approaches that are inconsistent and without appropriate consideration and recognition of industry activities in support of CISA and the Executive Order.

HITRUST, through its many programs, remains committed to ensuring the health care industry can properly address these challenges. Cyber information sharing is, and will continue to be, a key component in HITRUST's approach to cybersecurity and cyber risk management, and we are excited about pioneering these approaches. Information sharing is only one tool that impacts risk management for an organization. HITRUST continues to develop innovations such as the Health Care Sector *Cybersecurity Framework Implementation Guide*, and enhance its security and privacy framework and assurance programs. We value the partnership of DHS in these efforts and look forward to their continued support.

Thank you again for the opportunity to join you today and share these insights. I look forward to your questions.

Mr. RATCLIFFE. Thank you, Mr. Nutkis.

Mr. Montgomery, you are recognized for 5 minutes.

STATEMENT OF SCOTT MONTGOMERY, VICE PRESIDENT AND CHIEF TECHNICAL STRATEGIST, INTEL SECURITY GROUP, INTEL CORPORATION

Mr. MONTGOMERY. Good afternoon, Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee.

Thank you for the opportunity to testify today.

Intel is global leader in computing innovation, designing and building the essential foundational technologies that support the world's computing devices.

Governments, businesses, and consumers face a cybersecurity threat landscape that is constantly evolving with each new technology that is brought to market at a faster pace than ever before.

The challenges we face are too significant for one company, even as large as Intel Corporation, or entity to address on its own. Real change on cybersecurity requires leadership from Washington and a true public/private partnership with industry.

Our own contribution at the new McAfee, currently known as Intel Security, is based on an open communication fabric that will enable all of us in cybersecurity, both public and private, to work together in ways never before thought possible.

Cyber defense technologies' effectiveness, it peaks really shortly after it is released and degrades very, very quickly after its initial release. Actors take little notice, but once the technology is deployed at scale, they adopt evasion techniques and countermeasures, causing the effectiveness to significantly degrade quickly.

This creates situations where defenders are creating dozens of disparate tools to solve for micro conditions rather than macro conditions.

Technology efficiencies are already declining by the time the lengthy purchase and integration cycles are complete and trained labor is insufficient to deal with the complexity of supporting all these technologies. It is a strong collaboration that plays a key role in how we go forward.

Mobile threats, migration to the cloud, and in particular, the explosion of the number of internet-enabled devices, commonly known as IOT, the Internet of Things, are going to test and exacerbate the limits of our ability to work in real time rather than assist them.

With respect to the partnership model, Intel and Intel Security have been active in public/private partnerships managed by DHS and other agencies for more than 10 years. We have leadership roles in the President's National Security Telecommunications Advisory Committee, also known as NSTAC, the Information Technology Information Sector Coordinating Council, Information Technology Information Sharing and Analysis Center, National Cybersecurity Alliance, and the National Cybersecurity Center of Excellence.

With respect to a few policy recommendations to improve public/private partnerships, the first one is a move toward more real-time sharing.

As we talked about a little bit earlier, the drive and the number of devices, the drive and the number of internet-enabled technologies is going to scale quickly past our ability to encompass them in real time as workers. We need these mechanisms to be automated.

With the passage of the Cybersecurity Information Sharing Act, DHS was directed to deploy the Automated Indicator Sharing Program. The program allows both the private and public sectors to share indicators of compromise, but these indicators of compromise are like breadcrumbs. It is only when you aggregate them in the context that you see what the meal is. The sharing of individual indicators of compromise without context leaves practitioners asking more questions than having them answered.

Second, the NIST cybersecurity framework process should be used as the model—the model—for public/private partnerships. The framework for improving critical infrastructure security, known as the NIST cybersecurity framework, is widely acknowledged as a highly successful model of public/private partnership.

Here is our analysis of why. The need was real, the process was open, NIST listened more than they talked. They were prepared. They engaged stakeholders of a variety of different sizes, of a variety of different financial investments, in a variety of different sectors, both public and private.

The framework was voluntary, not regulatory. Very, very important for private organizations to particulate.

Then last, we would like to seek innovative ways to further grow the information-sharing ecosystem. When we share, for example, with the Cyber Threat Alliance, including Check Point, Cisco, Fortinet, Palo Alto, and Symantec, my erstwhile comrades on the panel, the point of it was to share faster than we could learn ourselves. It is for the whole to be greater than the sum of the individualized parts.

Examples of successes include cracking the code on CryptoWall version 3, one of the most lucrative ransomware families in the world, totaling more than $325 million ransomed.

Our disruption of the CryptoWall forced criminals to develop a CryptoWall 4, which we uncovered quickly and it resulted in a much less successful attack, a prime example of where the whole was greater than the sum of the individual vendor parts.

Given that the rapid change continues, public and private-sector organizations cannot go it alone. We look for the encouragement of DHS and their participation in helping us drive to greater wholes and less individual parts.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Montgomery follows:]

PREPARED STATEMENT OF SCOTT MONTGOMERY

MARCH 9, 2017

Good afternoon, Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee. Thank you for the opportunity to testify today. I am Scott Montgomery, vice president and chief technical strategist, Intel Security Group, part of Intel Corporation.

I am pleased to address the subcommittee on the value and effectiveness of current private-sector engagement with the Department of Homeland Security (DHS) given its importance in helping DHS achieve its mission of enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure. My testimony will address Intel Security's commitment to cybersecurity, our assessment of the global threat environment, the state of various DHS public-private partnerships and private-sector partnership innovation. Finally, I will make a number of public policy suggestions to help the new administration shore up the capabilities and effectiveness of DHS public-private partnerships.

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity. I work for the Intel Security Group Chief Technology Officer (CTO) and manage the world-wide team of experts that carry CTO titles. Together we drive the company's technical innovation; evangelize our expertise, thought leadership, and offerings to public and individual audiences; and work to increase the public trust by cooperating with law enforcement on cyber criminal investigations and disruption. With more than 20 years in content and network security, I bring a practitioner's perspective to the art and science of cybersecurity. I have designed, built, tested, and certified information security and privacy solutions for such companies as McAfee, Secure Computing, and a wide variety of public-sector organizations.

INTEL SECURITY'S COMMITMENT TO CYBERSECURITY

Intel is a global leader in computing innovation, designing and building the essential foundational technologies that support the world's computing devices. Combining Intel's decades-long computing design and manufacturing experience with Intel Security's market-leading cybersecurity solutions, Intel Security brings a unique understanding of the cybersecurity challenges threatening our Nation's digital infrastructure and global e-commerce. Governments, businesses, and consumers face a cybersecurity threat landscape that is constantly evolving with each new technology that is brought to market at a faster pace than ever before. The sharp rise of internet-enabled devices (known as "Internet of Things" or "IoT") in Government, industry, and the home exacerbates this already difficult challenge. The challenges we face are too significant for one company or entity to address on its own. Real change on cybersecurity requires leadership from Washington, DC, and a true public-private partnership with industry.

Collaboration will be the driving force behind what soon will be the new McAfee (currently known as Intel Security)—planned to be a stand-alone company this year. It's also why we recently announced a whole new ecosystem of integrated platforms, automated workflows, and orchestrated systems based on an open communications fabric that will enable all of us in cybersecurity to work together in ways never before thought possible.

To be successful, it is important to understand the market-like forces that drive the effectiveness of cybersecurity defense. Most information technologies continuously improve over time. Paradoxically, cyber defense technologies do not follow this pattern. Their effectiveness peaks shortly after release and then degrades. When a new defensive capability is first released, bad actors take little notice, but once deployed at scale, they adopt evasion tactics and counter-measures, causing the effectiveness to significantly degrade.

Where does that leave us? We see the current paradigm of constant integration of point products—individual software applications—as ineffective and unsustainable. Not only are technology efficiencies already declining by the time the lengthy purchase and integration cycles are complete, but organizations are unable to deal with the complexity of supporting upwards of 30 to 40 independent tools and technologies. That's a losing game, but it's the one security practitioners find themselves playing.

We need a different approach where technology—enabled with strong collaboration—can be deployed rapidly to security platforms so they can communicate with each other over open communication protocols. Such technology can be guided by the strategic intellect that only humans can provide. Thus, the only way to have a winning cybersecurity strategy is to bring technology, the cybersecurity industry, and the efforts between Government and the private sector together. This is what real collaboration is all about.

As we collaborate with our public partners, it's important to highlight how the threat landscape has changed over the years. It's a top-tier issue for Government leaders because of the critical role IT systems play in our National security, economy, and daily lives.

THE INTERCONNECTED THREAT LANDSCAPE

Increasing Sophistication of Attackers Threatens Organizations of Every Size

The threat landscape is ever-changing, and it's getting only more complex with the sharp rise in internet-enabled devices (IoT) and industry's shift to new computing paradigms such as cloud computing. What we call the "attack surface" continues to grow. This means that organizations—and more importantly, individuals—are now more vulnerable in more places. Adversaries are increasingly capable of attacking strategic assets and critical infrastructure. Traditional platforms such as phones, tablets, laptops, and servers continue to be high-value targets, but we must expand our thinking to include all devices that are "smart" and connected. Modern computing runs our factories, flies our planes, drives our cars, and runs our homes. Almost every aspect of what our country runs on is potentially vulnerable to a cyber attack.

The attacker community has matured enough to support a vibrant criminal underground economy. On-line web stores on the "Dark Web" now sell hacking tools to any would-be attacker, and on-line markets make it easy and efficient to sell stolen credit card and other personal information. Attackers are also busy developing new techniques that are substantially more difficult to detect and stop, setting their sights beyond the operating system or applications and instead focusing on the underlying virtual machines, firmware, and hardware. The growing sophistication of these tools and methods of attack has unsurprisingly placed a tremendous amount of pressure on today's security processes, tools, and people.

Innovative Technologies Bridge Resource Gaps for Public and Private-Sector Organizations, but also Magnify Threats

It should come as no surprise that cyber criminals closely follow the latest technology trends because that's where the targets are the most promising. Technological innovations can help organizations deliver better overall security and operations but can simultaneously expose new avenues for attack, such as:

Mobile Threats.—All organizations are relying more on mobile devices to improve communication and business processes, and this trend will undoubtedly continue. At the same time, malware written specifically to attack mobile devices is proliferating, creating new challenges as organizations attempt to secure mobile as well as traditional computing platforms.

Migration to the Cloud.—Organizations can reduce costs, improve offerings, eliminate complexity, and reduce reliance on on-site technical staff by outsourcing their IT and communications systems to the cloud. At the same time, however, they must be careful not to sacrifice security to achieve these new efficiencies.

IoT and the Explosion in Number of Devices.—The exponential increase of Internet-enabled and networked devices known as the Internet of Things (IoT) is expanding both risks and rewards. Organizations are using networked metering devices, sensors, appliances, and point-of-sale systems to deliver better customer service and streamline business processes, but must also be aware that many IoT devices were not designed with security in mind and could introduce unnecessary risk to vital IT networks and systems.

Bring Your Own Device (BYOD) Environments.—Given the mobile nature of today's workforce, as well as the increasing use of BYOD programs, employees at companies of all sizes commonly access organizational resources from external networks such as hotspots and home networks. The result is often that company-owned network equipment will be simply unable to inspect the growing amount of traffic and devices connected to internal IT networks.

Performance Issues Preempt Security.—Customers are increasingly choosing to forego bulkier security features like firewalls in favor of maximizing network performance levels, creating a tug-of-war between security and performance priorities.

Adversaries Enjoy Significant Advantages.—Our research and analysis reveals that cyber adversaries benefit from and exploit several key advantages, including:

- The ability to enhance the tools and capabilities used in an attack quickly through a community of innovators and service providers. This has an outsized impact on small organizations, who may not have the resources to deploy the latest adaptive technologies, or are not deploying risk management-based solutions at all.
- A working knowledge of how organizations implement defenses, including knowledge of specific product deployment models, industry architectures and even specific vulnerabilities. While an attacker only has to be right once, organizations must be impenetrable 100 percent of the time—a statistic that is unrealistic even for the most well-resourced security vendors or large corporations.

INTEL SECURITY'S VIEW OF PUBLIC-PRIVATE PARTNERSHIPS

Our Commitment to the Partnership Model

Given the current cybersecurity threat environment, organizations across the spectrum cannot manage their protective defenses alone. Security is a shared goal carrying a shared responsibility. As a result, the strategic partnerships that have grown between public and private-sector entities over the last two decades have never been more important.

At a National level, critical industry sectors supporting the safety, security, and economic growth of the United States were among the first to self-organize in partnership with Government agencies to assess and mitigate threats to U.S. critical infrastructure. These public-private partnerships are fueled by a joint commitment to defend critical infrastructures against increasingly sophisticated cyber attacks, and they thrive on sharing threat indicators, best practices, and incident response in a mutual, non-regulatory environment.

Intel and Intel Security have been active in public-private partnerships managed by DHS and other agencies for more than 10 years. We have leadership roles in the President's National Security Telecommunications Advisory Committee (NSTAC), Information Technology Information Sector Coordinating Council, Information Technology Information Sharing and Analysis Center, National Cyber Security Alliance, and National Cybersecurity Center of Excellence (NCCoE). Through these partnerships, Intel Security works to provide hardware, software, and training to advance the rapid adoption of secure technologies around the country. In addition, we remain actively engaged in the development of new cybersecurity guidelines to help public and private-sector organizations evaluate their security postures and conduct risk assessments, regardless of size or sophistication.

As these partnerships grow and mature, our company will continue to invest, engage, and contribute. The challenge is never-ending, but we have no doubt the public-private partnership model will continue to protect and serve our National interests well into the future. However, public-private partnerships, as any partnership, benefit from regular reviews, gap analyses, and a commitment to continual improvement.

Policy Recommendations to Improve Public-Private Partnerships

1. Move to Real-Time Threat Information Sharing

The administration needs to solidify its information-sharing strategy. Sharing threat information has been a necessity since I started in cybersecurity, yet we still are not focused on sharing threat information that will provide real benefits in a meaningful way. With the passage of the Cybersecurity Information Sharing Act (CISA), DHS was directed to deploy the Automated Indicator Sharing (AIS) program. This program allows both the private and public sectors to share indicators of compromise (IOC) and mitigation with each other. CISA also does an admirable job of requiring companies and Government agencies to strip out personal identifiable information (PII) and put in place thoughtful processes and policies to protect citizen privacy.

While the overall program has been a strong step in the right direction, it still provides far too little real value. IOCs are just the breadcrumbs that network security staff look for to uncover clues as to what may be occurring inside their organizations. Typical IOCs are registry keys, MD5 hashes of potential malware, IP addresses, virus signatures, unusual DNS requests, URLs, etc. While these can be useful, they are really not enough to provide the defensive information needed to protect an organization. Today, AIS does not provide a means for enriching the information it shares. It simply shares minimal IOC information.

To defend our institutions properly, defenders need to understand cybersecurity threats and their components as a whole. Indicators, incidents, tactics, techniques, and procedures used, threat actors, associated campaigns, what is being targeted, malicious tools being used, software vulnerabilities being exploited, courses of action to mitigate the threat, are all components of a cyber threat that need to be understood. Instead of trying to share simple breadcrumbs, we need to be sharing with a focus on providing a platform for enriching specific threat information so we can see and understand more about the threat.

Often one company may discover an IOC, another may be able to associate it with a specific vulnerability, and still another may be able to provide a correlation between the known threat items and a past or similar attack that could lead to a potential remediation, thus mitigating the threat. Today we have no way to share enriched threat data effectively. We need information sharing with a focus on enhancing our abilities to protect our organizations. The administration should double down on working with the private sector to further evolve the way cyber threat information is represented, enriched, and distributed in a timely fashion. Cyber criminals are excellent at information sharing; the Government and private sectors must be as well.

2. Encourage Full Utilization of and Update Government Procurement Rules to Enable DHS to Compete with Hackers

There are significant gaps at DHS that preclude it from competing with hackers, cyber criminals, and other bad actors who innovate and share information quickly, often using state-of-the-art technology. Thus, it is critical that DHS and other Federal agencies have access to the same tools. This can only be achieved by encouraging full use of current procurement rules, and by looking for opportunities to update those rules where necessary. Currently, there are five ways Federal agencies can acquire products and services rapidly:

- Under the Federal Acquisition Streamlining Act of 1994 (FASA), Congress mandated, to the maximum extent practicable, the use of simplified acquisition procedures (SAPs) for products and services not exceeding the simplified acquisition threshold.
- The Competition in Contracting Act of 1984 (CICA) allows Federal agencies to accelerate the acquisition process where there is an urgent need, or where requiring full and open competition could compromise National security.
- The U.S. General Services Administration (GSA) maintains a supply schedule for information technology (Schedule 70), where pre-vetted vendors with pre-negotiated terms offer cybersecurity products.
- Congress authorized the Continuous Diagnostics and Mitigation (CDM) program at DHS, which allows Federal agencies to expand their CDM capabilities through the acquisition of commercial off-the-shelf tools, with robust terms for technical modernization as threats change.
- Congress has granted 11 agencies (including DHS) the ability to enter into “other transaction agreements,” which generally do not follow a standard format or include terms and conditions normally found in contracts or grants, in order to meet project requirements and mission needs.

In addition to encouraging Federal agencies to fully use these procedures, procurement policy and acquisition procedures must evolve more rapidly to match the pace of information technology development and adoption by hackers, criminals, and other bad actors. Currently, little guidance exists in the Federal Acquisition Regulations (FAR) regarding the procurement of cybersecurity technology; rather, the FAR leaves cybersecurity implementation to each individual Federal agency. Agency officials and contractors must consult a myriad of different agency regulations to ascertain if and how other agencies have implemented their acquisition regulations regarding cybersecurity. This diversity in agency cybersecurity regulations undermines security requirements and policies governing Federal procurements. Harmonizing cybersecurity acquisition requirements would allow agencies to: (i) Target security to highest-priority data and threats; (ii) obtain greater value through reduced compliance obligations and increased contractor focus on high-value cybersecurity investments; and (iii) enhance agency cybersecurity through the adoption of best practices, tempered through public review and comment.

3. Create Additional Incentives to Participate in Information-Sharing Partnerships

A critical provision of CISA is that it gives liability protections to private companies that share cyber threat information (CTI) and defense measures (DM) on a voluntary basis with DHS. Recent guidance from DHS on CISA clarifies that private entities also receive liability protection under section 106(b)(1) for sharing CTI and DM information with other private entities. Policy makers have done an admirable job of using the incentive of liability protections, and relaxing antitrust rules, to help incent broad-based information sharing between the private sector and the Government, and among private-sector entities. However, too few companies are actively sharing threat information with DHS and among themselves to fully realize the aim of CISA—a high-functioning eco-system of information sharing that enables the public and private sectors to compete with global networks of sophisticated hackers.

We need to recognize the disincentive that threat intelligence’s “free rider” problem has imposed on public and private-sector information sharing. Every organization benefits from consuming threat intelligence but gains no direct value from providing it unless the right organizational structure and incentives are put in place to eliminate the free rider problem.

While DHS has made progress, it still needs to improve the quality and the quantity of the threat data it shares with the private sector to address this issue of the free rider. DHS should thus declassify larger categories of threat data and actively share them with the private sector. DHS should issue many more security clearances to qualified company representatives to enable access to the most sensitive, and potentially most valuable, pieces or classes of threat data.

Finally, the new administration should pass into law The Cyber Information Sharing Tax Credit Act—sponsored by Senators Moran and Gillibrand—that would incentivize businesses of all sizes to join sector-specific information-sharing organizations, known as Information Sharing and Analysis Centers (ISACs), by providing refundable tax credits for all costs associated with joining ISACs. The effort should not just focus on ISACs but should also include Information Sharing and Analysis Organizations (ISAO) as well. ISAOs are not limited to individual critical infrastructure sectors as ISACs are, and they allow diverse organizations to share cyber-related threat information.

4. Use the NIST Cybersecurity Framework Process as a Model for Public-Private Partnerships

The Framework for Improving Critical Infrastructure Cybersecurity, known as the NIST Cybersecurity Framework, is widely acknowledged as a highly successful model of public-private partnership. The Office of Management and Budget is already working to encourage Federal agencies to adopt the Framework, the new administration's draft Executive Order mandates Government agencies to deploy the Framework, and the private sector is rapidly adopting it. Here's our analysis of why:

- The need was real;
- The process was open;
- NIST listened first;
- They were prepared;
- They engaged all stakeholders;
- The framework was voluntary—not regulatory.

I'd like to expand on each of these aspects, not simply to compliment NIST but to offer the process as a model for future public-private partnerships.

The need was real

PPPs created around a topic or issue that is real to both the public and the private sectors has a much better chance of getting the exposure and participation needed to achieve the goal of the partnership. In the case of the Cybersecurity Framework, it was obvious to both groups that the need existed. While NIST had a hard time frame to be successful in—1 year—they had a long history in risk management and understood the need well. For too long regulatory compliance had forced industry to spend valuable security dollars to prove something to the regulators instead of using those resources to help protect enterprises. The cost of compliance was impacting our ability to secure ourselves.

Openness of the process

From the very beginning, NIST made it clear this was going to be a very open process. In the initial meeting, NIST staff described what would be occurring, from the RFI-submitted comments being made public on a NIST project website, to the anticipated workshop process and general time line for various milestones. Along the way, NIST staff were quick to ensure that industry participants understood what was happening so there would be no surprises. This created a growing sense of trust as the effort evolved and made the process more effective during the development of the Framework.

Listening

One of the more interesting and effective parts of the development was the way NIST staff listened to the workshop participants. They used a moderated dialog approach that allowed all attendees to voice their opinions to a set of topics the NIST staff wanted to learn about. There were very active discussions that were highly informative from members of various sectors and industries. Dr. Gallagher, NIST's Director at the time, stated quite clearly this was not NIST's Framework; this was the community's Framework. Having the public side of a public-private partnership listen instead of dictate allowed private-sector participants to voice their opinions in a much more open and direct way. This too built trust as the effort went along.

Being prepared

Each of the workshops seemed very well organized, and the topics, panels, questions and outcomes were well thought-out before each workshop began. This gave participants reassurance their time was being well spent. Open forums with no direction or planning do not give those involved much confidence the effort will succeed. Being prepared also meant participants needed to do their homework as well. While not always the case, as the workshops advanced, they did so.

Engaging all

One of the smartest things NIST did as part of the Framework development process was to understand they needed to get outside the Beltway for the effort to be successful. They held the workshops in different locations around the country so the local owner/operators of the critical infrastructure could have their voices heard. This ensured there was a diverse group at each of the workshops and all were able to participate. The processes used during the workshops encouraged all in the room to contribute and they did. A highly interactive, collaborative environment is one where real dialog can occur and produce positive results.

Voluntary, non-regulatory nature

The fact that NIST is a non-regulatory body also helped their credibility and the private sector's attitude toward participating and contributing. This was a topic area that had a lot of people concerned initially, but as the effort progressed, more and more private-sector participants relaxed and believed in the voluntary intent of the effort. NIST also made it clear in each workshop that they were requiring a non-attribution from any and all regulators in the room. Each agreed to the rules, making it much more comfortable for real open and honest dialog to occur.

While others have tried to copy the NIST success, often they have left out one or more of the characteristics that made the Cybersecurity Framework effort a success. In reality, both the public and the private-sector participants must buy in. To do so requires trust in the process, the effort and the vision for the outcome to be successful

5. Seek Innovative Ways to Further Grow the Information-Sharing Eco-System

Company-to-company information sharing is growing in certain parts of the economy. An example is the Cyber Threat Alliance (CTA). Intel Security, along with Check Point, Cisco, Fortinet, Palo Alto Networks and Symantec, worked together to start and build the CTA. This is a group of cybersecurity practitioners from organizations that have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member organizations and their customers. The key to the success of this effort is that each organization must supply threat information to all the members in order to receive threat information. This allows each of the member organizations to incorporate the others' threat information into their products' protection mechanisms. This is an example of valuable and actionable shared threat information having a direct and positive impact on improving their customers' environments. The member organizations have decided to participate in the Alliance for the betterment of the ecosystem they serve.

The CTA is also showing that with the right organizational construction—with the right incentives to collaborate—real progress in private-sector information sharing can be made. Examples of successes include cracking the code on Crypto Wall version 3, one of the most lucrative ransomware families in the world, totaling more than US$325 million ransomed. CTA's disruption of Crypto Wall 3 forced cybercriminals to develop Crypto Wall version 4, which the CTA also uncovered and resulted in a much less successful attack. This is a prime example where creating an operationally holistic view of the threat and how to address it has had an extremely positive impact on our ability to protect ourselves.

To further incentivize companies to share threat information among themselves, policymakers should amend The Cyber Information Sharing Tax Credit Act. Such an incentive would help speed the growth of existing private sector-to-private sector information-sharing coalitions and help start news ones, particularly in some sectors of the economy that have been slow to realize the benefits of sharing threat information with partners and competitors.

CONCLUSION

Given the rapidly-changing threat environment, public and private-sector organizations cannot go it alone. The challenge is never-ending, but I have no doubt that the public-private partnership model will continue to protect and serve our National interests well into the future. Public-private partnerships benefit from regular reviews, gap analysis, and a commitment to continual improvement. The subcommittee should be commended for taking such a thoughtful approach to reviewing the successes and challenges of DHS-managed public-private partnerships.

As stated earlier, DHS deserves much praise. It manages a thriving number of public-private partnerships that serve the National interest. At the same time, real-time information sharing needs to be implemented on a grand scale, IT procurement rules should be updated, DHS partnerships need to be benchmarked against other successful ones on a regular basis and additional incentives should put in place to help grow the information-sharing eco-system. Intel Security—soon to become McAfee—is committed to continue to invest, engage, and contribute to support the long-term success of the partnership model. Our collective security depends on making the promise of "together is power" a reality.

Mr. RATCLIFFE. Thank you, Mr. Montgomery.

Mr. Greene, you are recognized for 5 minutes.

STATEMENT OF JEFFREY GREENE, SENIOR DIRECTOR, GLOBAL GOVERNMENT AFFAIRS AND POLICY, SYMANTEC

Mr. JEFFREY GREENE. Thank you. Chairman Ratcliffe, Ranking Member Richmond, Members of the committee, thank you for the opportunity to testify today.

As Mr. Montgomery mentioned, the threat landscape is constantly evolving. In the current situation, there is no company or no government that can go it alone. We are therefore pleased to see your continued focus on how DHS can work with the private sector in new and innovative ways.

I want to start by talking briefly about the current cyber threat environment. You will see a lot of headlines about cyber attacks focused on massive data breaches or cyber espionage, but it is important not to lose sight of the other types of attacks that can have major consequences.

The incidents we see today range from increasingly sophisticated forms of ransomware, in particular ransomware being targeted at the enterprise as opposed to the individual, to massive distributed denial-of-service attacks, DDoS attacks, that were launched from connected or internet-of-things, IOT, devices.

We at Symantec have a long-standing relationship with DHS. From our perspective, the Department has made significant progress engaging with the private sector over the past few years.

The Cyber Information Sharing and Collaboration Program, or CISCP, allows participants to share information about incidents, cyber threats, and known vulnerabilities.

One example I would point to is last October we shared research from a group that we had discovered that was trying to steal money from banks by exploiting the SWIFT messaging system. This is the same attack that was used to steal $81 million from the Bangladesh central bank.

CISCP managers took the information that we provided, developed an indicator bulletin, and pushed that out to all CISCP participants.

CISCP also convenes practitioners at quarterly advanced technical threat exchanges. For the most part, we have found the exchanges useful. Last year, we did a presentation at one of them focused on new and emerging ransomware. Included in this presentation was in-depth analysis and specific indicators of compromise that were then available to all participants to use to try to upgrade their systems if necessary.

But also beyond the technical information that is shared, these are opportunities for Government and industry to sit down face-to-face, develop trusted relationships, both between Government and the private sector and also within the private sector itself.

Many of DHS's reports and bulletins include substantive analysis and actionable information, but at times some do fall short. In some cases, reports have included indicators of compromise that were not fully vetted or, as Mr. Montgomery mentioned, didn't have the context around them. Sometimes some private-sector companies have used these without proper research on their end, and there has been in a couple of instances a high degree of false positives based on them.

To DHS's credit, though, when that has happened they have been responsive to industry concerns and at times have issued revised reports.

As DHS moves to machine-speed sharing through the Automated Indicator Sharing Program, the need for context and vigorous vetting is just going to grow. This is going to put something of a burden on DHS and its partner agencies because, on the one hand, they are being told to share more and to share faster, but on the other hand they are being told to be very careful about what you share and vet it before you do so. So this is a balance that is not easy to strike and it is going to require constant tuning.

We also engage with DHS informally. An example, last week we had 10 of DHS's cyber analysts out at our operations center in Herndon to discuss a few specific threats. Face-to-face meetings like this can alleviate another concern that you may have heard that too often the information flow is one way just from the private sector to the Government. In-person discussions can lead to a more complete and bilateral exchange of ideas.

In addition to DHS, we work with the FBI and other agencies to assist efforts to fight cyber crime and take down botnets. There is more information in our written testimony, but I do want to highlight one case. This is our work on unearthing an international criminal gang that was called Bayrob.

Bayrob evolved over a decade. We spent a year tracking them and, in part based on the information we provided to the FBI, they built a case that led to the arrest and extradition from Romania of three of Bayrob's key actors. So I think we need to consider broader than just DHS and how DHS works with other agencies as well.

Finally, the partnership among private-sector companies is alive and well. As Mr. Montgomery mentioned and Mr. Gillis may discuss, we are part of what is called the Cyber Threat Alliance that shows how even competitors can work together to improve the overall safety and security of the internet and that of our customers.

As Members of this committee know better than most, we still face significant challenges in our efforts to improve cybersecurity and to fight cyber crime. Cybersecurity is first and foremost a team sport, and at Symantec we are committed to improving the internet security and will continue to work with industry and Government collaboratively on ways to do so.

Thanks again for the opportunity to be here. I am happy to take any questions.

[The prepared statement of Mr. Greene follows:]

PREPARED STATEMENT OF JEFFREY GREENE

MARCH 9, 2017

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, my name is Jeff Greene and I am the senior director, global government affairs and policy at Symantec. I am responsible for Symantec's global public policy agenda and Government engagement strategy, and represent the company in key public policy initiatives and partnerships. I also serve as a member of the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board (ISPAB), and recently supported the President's Commission on Enhancing National Cybersecurity. Prior to joining Symantec, I served as senior counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused on cybersecurity and homeland defense issues.

Symantec Corporation is the world's leading cybersecurity company. We help organizations, governments, and people secure their most important data wherever it resides. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud, and infrastructure. Likewise, a global community of more than 50 million people and families rely on our Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing us to see and protect against the most advanced threats. We maintain nine Security Response Centers and six Security Operations Centers around the globe and every day we scan 30 percent of the world's enterprise email traffic and process more than 1.8 billion web requests. All of these resources combined allow us to capture world-wide security data that give our analysts a unique view of the cyber threat landscape.

No government or company can go it alone in this environment, and we are happy to see the subcommittee focusing on how the private sector engages with DHS and other government agencies to help defend against growing cyber threats. Lasting improvements in cybersecurity require the combined efforts of Government and industry together. In my testimony today, I will discuss:

- The current and emerging threat landscape;
- DHS and Private-Sector Engagement; and
- How we partner with our industry counterparts to stop cyber attacks.

I. THE CURRENT AND EMERGING CYBER THREAT LANDSCAPE

Many of the recent headlines about cyber attacks have focused on massive data breaches and cyber espionage across the spectrum of industries and governments. These headlines remind us that no organization or government entity is impervious when targeted by a motivated and skilled attacker. Yet while the focus on data breaches and the personal information exposed is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and that can have damaging consequences. There is a wide set of tools available to the cyber attacker, and the incidents we see today include increasingly sophisticated forms of ransomware, massive distributed denial of service (DDoS) attacks by "Internet of Things" (IoT) devices, sophisticated (and potentially destructive) intrusions into critical infrastructure systems, and the weaponization of personal information. The economic impact to an organization can be immediate, through the theft of money or the payment of ransom, or more long-term and structural, such as through the theft of intellectual property. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the internet and their Government.

The attackers run the gamut and include highly-organized criminal enterprises, nation-states, disgruntled employees, individual cyber criminals, so-called "hacktivists," and state-sponsored groups. The motivations vary—criminals generally are looking for some type of financial gain, hacktivists are seeking to promote or advance some cause, and state actors can be engaged in espionage (traditional spycraft or economic) or infiltrating critical infrastructure systems. These lines, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills to the highest bidder.

Attack methods vary, and the only constant is that the techniques are always evolving and improving. Spear phishing, or customized, targeted emails containing malware or malicious links, is the most common form of attack. Many of these attacks are extremely well-crafted; in the case of one major attack, the spear-phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it—and exposed his company to a major breach. Social media is an increasingly valuable tool to criminals as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to wonder if that feed may have been compromised or spoofed. We have also seen the rapid growth of targeted web-based attacks, known as a "watering hole" attack. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cyber criminals lie in wait on legitimate websites that they compromise and use to try to infect visitors. Most of these attacks rely on social engineering—simply put, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychological as they are technological.

One particularly concerning trend is the recent use of IoT devices in DDoS attacks. By taking advantage of poor security and design practices, criminals were able to compromise hundreds of thousands, if not millions, of devices and aggregate them as a single army of zombie devices—the world's first major IoT botnet, known as Mirai. In October 2016, cyber criminals used the Mirai botnet to launch a massive DDoS Attack on DNS provider Dyn, which disrupted some of the internet's biggest websites, including Spotify, Twitter, PayPal, Reddit, and others. Mirai's "bots" were primarily compromised webcams and digital video recorders, but also included routers and other internet-connected devices. This attack was quickly followed by at least two others, each record-breaking in its size.

How did these IoT-based attacks happen? Very easily, unfortunately. The average IoT device is scanned for vulnerabilities just 2 minutes after it is connected, and when one is found that device is promptly compromised. The most common method is simple—criminals take advantage of pre-programmed, default usernames and passwords and simply log onto devices and commandeer them. With the explosion of insecure internet-connected devices hitting the market, this type of attack will only continue to grow and become more effective.

II. DHS AND PRIVATE-SECTOR ENGAGEMENT

The Department of Homeland Security has made considerable progress in recent years engaging with the private sector, especially in the area of information sharing. The Cyber Information Sharing and Collaboration Program (CISCP) is DHS's primary structure for private companies to share information about incidents, cyber threats and known vulnerabilities. This information is then shared among participating industry partners in an anonymized fashion to help secure their own networks. In addition, CISCP convenes cybersecurity practitioners at quarterly Advanced Technical Threat Exchanges (ATTE). We have been active in these exchanges, and late last year presented our research on ransomware, which included an in-depth analysis of new infection trends and payload execution. We provided a list of specific indicators that participants could use to further research and ensure their own systems were protected. We have also presented on how companies and governments can leverage threat intelligence to reduce "Indicator of Compromise (IoC) noise." Beyond the technical information shared, the ATTEs are helpful in building trusted relationships and contacts between Government and private industry, and even within the private sector itself. These exchanges often lead to follow-on collaboration and, in some cases, joint research.

Another notable example of effective information sharing through the CISCP program came in October of last year when Symantec published a report exposing a hacking group that was trying to steal money from banks by exploiting the financial-based SWIFT messaging system used to identify electronic transactions in the global financial system. In one of the highest-profile attacks of the year, attackers used this same method to steal $81 million from the Bangladesh Central Bank. Similar to the Bangladesh attack, Symantec found a previously-unknown malware variant (called Odinaff) being used against financial institutions. This particular malware can delete customer logs of SWIFT transactions, allowing attackers to hide their tracks. We passed along our in-depth, technical research to CISCP managers along with a list of indicators including hashes, command-and-control nodes, and domains. The CISCP team then used our indicators to create an Indicator Bulletin (IB) and pushed it out to all CISCP participants for their use.

The quality of DHS's analysis reports can vary. Many reports include substantive analysis and actionable information, while some have fallen short. In those instances, many of the IoCs included in the report were unvetted, and companies that used them without proper care saw a high volume of false positives. In some cases the IoCs proved to be unrelated to the threat itself. To its credit, DHS is generally responsive to industry concerns and has on occasion issued updated reports with more information.

The importance of carefully vetting indicators is of increased importance as DHS moves to Automated Indicator Sharing (AIS). The AIS program allows the two-way exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. This means that as soon as a company or a Federal agency identifies a threat, that indicator is shared in real time with all of the AIS participants. However, with an emphasis on velocity and volume, appropriate context and more vigor in vetting is necessary. Added context allows recipients to understand how to use an IoC or how to calibrate their internal response. To be sure, DHS and its partner agencies are in a difficult spot—the private sector is demanding both timely and vetted information, and this balance is not easy to strike. Industry has conveyed these concerns to DHS, which has worked to improve both its analysis and the quality of the indicators.

Another program DHS has implemented to engage with industry is the Critical Infrastructure Cyber Community or C^3. The C^3 is a voluntary program that helps critical infrastructure operators improve their cybersecurity and actively encourages the adoption of the Framework for Improving Critical Infrastructure Cybersecurity, commonly known as the NIST Cybersecurity Framework (CSF). The CSF was developed in collaboration with the private sector, and Symantec was part of that effort. We began using the CSF when it was still in draft form and was one of the first companies to map our internal security to it. We support DHS's efforts to encourage use of the CSF, both for companies with existing cybersecurity programs and for those who are building one from scratch.

In addition to the Department's formal programs, we work with DHS informally. For instance, just last week, we hosted a group of ten cyber threat analysts at our Herndon Security Operations Center to discuss specific threats and to explore potential areas to coordinate in the future. Among other topics, we discussed Shamoon, a family of destructive malware that we have tracked for years. Shamoon was used in attacks against the Saudi energy sector in 2012[1] and recently we have been tracking a fresh wave of attacks hitting the Middle East.[2] The opportunity to sit face-to-face and discuss threats often alleviates another concern among many private-sector security companies, that too-often the information flows just one way—from industry to the Government. In-person exchanges often lead to a more complete and bilateral interchange of ideas.

Other Government Partnerships

Partnerships can lead to concrete results. One recent example came in December 2016, when Symantec concluded a decade-long research campaign that helped unearth an international cyber criminal gang dubbed "Bayrob." The group is responsible for stealing up to $35 million from victims through auto auction scams, credit card fraud and computer intrusions. Through our research, we discovered multiple versions of Bayrob malware, collected voluminous intelligence data, and tracked Bayrob as it morphed from on-line fraud to a botnet consisting of over 300,000 computers used primarily for cryptocurrency mining. Over time, Symantec's research team gained deep technical insight into Bayrob's operations and its malicious activities, including its recruitment of money mules. These investigations and countermeasures were crucial in assisting the Federal Bureau of Investigation (FBI) and authorities in Romania in building their case to arrest three of Bayrob's key actors and extradite them to the United States.

Indeed, in recent years we have seen a string of successful arrests and prosecutions of some of the most notorious cyber criminals in the world. In July 2015, a New York judge sentenced Alexander Yucel, the creator of the "Black Shades" Trojan to 5 years in prison and the forfeiture of $200,000. Yucel was swept up by the FBI and Europol last year along with dozens of other individuals in the United States and abroad. Symantec worked closely with the FBI in this coordinated take-down effort, sharing information that allowed the agency to track down those suspected of involvement. In June 2015, Ercan "Segate" Findikoglu, who prosecutors say orchestrated one of the biggest cyber bank heists in American history, was extradited to the United States to stand trial for stealing more than $55 million by hacking bank computers and withdrawing millions in cash from ATMs.

Additionally, Government and private-sector cooperation has led to take-down operations against prominent financial fraud botnets. In June 2014, the FBI, the United Kingdom (UK) National Crime Agency, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet Gameover Zeus and the ransomware network Cryptolocker. Gameover Zeus was the

[1] *The Shamoon Attacks*, Symantec Security Response, 8/16/12; *https://www.symantec.com/connect/blogs/shamoon-attacks*.

[2] *Shamoon: Multi-staged destructive attacks limited to specific targets, Symantec Security Response*, 2/27/17; *https://www.symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets*.

largest financial fraud botnet in operation in 2014 and is often described as one of the most technically sophisticated variants of the ubiquitous Zeus malware. Symantec provided technical insights into the operation and impact of both Gameover Zeus and Cryptolocker, and worked with a broad industry coalition and the FBI during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cyber criminals behind both threats.

III. PRIVATE-SECTOR PARTNERSHIPS TO ENHANCE CYBERSECURITY—THE CYBER THREAT ALLIANCE

While DHS continues to engage industry, the private sector is not just waiting on the Government to solve the problem. Industry partnerships have proven to be highly effective in fighting cyber crime. The Cyber Threat Alliance (CTA) is an excellent example of the private sector banding together to improve the overall safety and security of the internet. In 2014, Symantec, Fortinet, Intel Security, and Palo Alto Networks formed the CTA to work together to share threat information. Since that time, Cisco and Checkpoint have joined the CTA as founding members. The goal of the CTA is to better distribute detailed information about advanced attacks and thereby raise the situational awareness of CTA members and improve overall protection for our customers.

Prior industry-sharing efforts were often limited to the exchange of malware samples, and the CTA sought to change that. Over the past 3 years the CTA has consistently shared more actionable threat intelligence such as information on "zero day" vulnerabilities, command-and-control server information, mobile threats, and indicators of compromise related to advanced threats. By raising the industry's collective intelligence through these new data exchanges, CTA members have delivered greater security for individual customers and organizations. In short, the CTA is not about one vendor trying to gain advantage—we are all contributing and sharing with the community.

Because of the success of the CTA, the founding members decided to take it to the next level and earlier this year formally incorporated it as a non-profit organization. Working together, CTA members have developed a new platform designed to automate intelligence sharing in near-real time. Through this effort we hope to solve some of the problems created by isolated and manual approaches to cyber threat intelligence. The new CTA has three purposes:

1. To share threat information in order to improve defenses against advanced cyber adversaries across member organizations and their customers;
2. To advance the cybersecurity of critical information technology infrastructures; and
3. To increase the security, availability, integrity, and efficiency of information systems.

CTA is also committed to engaging in discussions around policy initiatives that will improve cybersecurity for individuals and governments. As CTA moves forward with its mission, it intends to explore how to best partner with U.S. and international Government organizations in furtherance of its mission.

CONCLUSION

As the Members of this subcommittee know better than most, we still face significant challenges in our efforts to improve cybersecurity and fight cyber crime. Cybersecurity is a team sport and effective public-private partnerships with DHS and other Government agencies are essential. DHS and industry have made notable progress over the last several years—trust has improved—but there is still room for growth. Attackers are always evolving, becoming more sophisticated, and both Government and industry recognize the imperative for cooperation to fight cyber crime. At Symantec, we are committed to improving internet security across the globe, and will continue to work collaboratively with industry and Government partners like DHS on ways to do so. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

Mr. RATCLIFFE. Thank you, Mr. Greene.

Mr. Gillis, you are recognized for 5 minutes.

STATEMENT OF RYAN M. GILLIS, VICE PRESIDENT OF CYBERSECURITY STRATEGY AND GLOBAL POLICY, PALO ALTO NETWORKS

Mr. GILLIS. Chairman Ratcliffe, Ranking Member Richmond, Members of the committee, it is an honor to be here today to discuss DHS's interface with the private sector.

It is tough to go forth after this group of individuals. I would like to start by thanking the committee for your leadership in cybersecurity. The legislation that you have helped lead over the last several years has not only helped foster responsible cyber threat information sharing, it has also strengthened the statutory responsibilities and statutory authorities that DHS has to execute its mission, both within the Federal Government and to interface with the private sector. So that has been a critical challenge that DHS has faced in standing up its cyber capabilities.

My name is Ryan Gillis. I am pleased to represent Palo Alto Networks. We are newer than some of our other industry colleagues up here, but within the 10 years since we have shipped our first product we have become one of the largest cybersecurity companies in the world.

Also happy to offer some historical perspective as I spent over a decade within the National Security Council at the White House and Department of Homeland Security. So this public/private experience that I have gone through I think represents the broader operational reality which is that, as you said, Chairman, cybersecurity is a fundamentally distributed responsibility. There are capabilities in the private sector and authorities within the U.S. Government and governments around the world that can complement each other. DHS is central to that.

DHS's role in not only protecting civilian networks and interfacing with the private sector, helping to secure critical infrastructure, is essential. That is a policy decision that has been made by consecutive administrations and in a bipartisan way through Congress to ensure that there is a civilian interface for that role and mission and to build-up the capability within DHS, whether it is through informal sharing examples I will go through, as well as programs such as CISP and AIS.

Let me give you a quick perspective that we have on the cyber threat landscape, which is that right now attacks are overly automated. The bad guys are working together. They are using free tools and cheaply available tools to launch automated attacks. So the cost is too low right now to be successful.

The business model is frequently, whether you don't have the capability to develop your own attacks, but you are using those freely available things that can bring you into the ecosystem, or if you are a sophisticated nation-state, you are generally going to use the least sophisticated attack that can accomplish your goal. So what we need to do is flip that cost curve by automating defenses and making sure that we are collectively working together.

On a company level, we deploy technology that stops attacks at certain points within the attack life cycle. It constantly requires updates, as Scott talked about earlier. So just on a corporate level, we provide 1.1 million new preventative measures to our technology around the world on a weekly basis, pushed out in as little as 5 minutes. One company alone, as you have heard today, can't do that adequately, so we need to find partnerships throughout the ecosystem.

On an industry level, you have heard about the Cyber Threat Alliance. To give a little bit more of an example of how the Cyber Threat Alliance worked on this CryptoWall example that Scott talked about, $300 million had been extorted in ransomware through this CryptoWall campaign. The vendor community, through the Cyber Threat Alliance, came together and shared what we knew about the infrastructure, defended all of our collective clients against those attacks. Prior to publishing that report, we called up Department of Homeland Security to ensure that we were collaborating on that.

DHS had FBI on the phone that night. They made sure that U.S. Government networks were similarly protected against those types of attack. They did notifications to internet service providers and to victims to help clean up. Most of the attacks were coming from unknowing victims that didn't know that their systems were being repurposed for attack.

Then in an actual, quantifiable example of information given back from the Government, we got an additional 170 command-and-control nodes, parts of the infrastructure that we as vendors had not identified as part of the context of that attack, and we were able to further protect all of our collective customers.

So it is one example of how we can share, as Scott said, more context and become more effective overall. What we need to move to is in programs like CISP and AIS, getting closer to machine speed with those types of examples.

So there is opportunity to expand on the nascent capabilities that DHS has rolled out through AIS and CISP and make us more effective overall.

I think the other thing that you are going to see as well is that I believe the U.S. Government is never going to be quick at declassifying some of its most valuable information. What the U.S. Government may not realize, however, is that we in the vendor community may see trial balloons of that most sophisticated technology in a few places and in unclassified ways.

If we can share that with the U.S. Government, we can obviate that whole what they call the tear line process, where the U.S. Government has to declassify that information, and the U.S. Government can point to the financial sector or the energy sector, whoever they think may be targeted by that particularly pernicious campaign, and say you need to focus on this, we have seen it out in the wild, and we think bad guys are going to go after it.

So this collective public/private, DHS will be at the center of that. Ultimately, we think things like the Cyber Threat Alliance are crucial to taking that next step.

[The prepared statement of Mr. Gillis follows:]

Prepared Statement of Ryan M. Gillis

March 9, 2017

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee: Thank you for the opportunity to appear before you today to discuss how the Department of Homeland Security engages with the private sector. My name is Ryan

Gillis, and I serve as the vice president of cybersecurity strategy and global policy at Palo Alto Networks.

I would like to begin today by recognizing the tremendous leadership this committee has shown on the issue of cybersecurity. I have seen first-hand this committee's central role in passing a range of cybersecurity legislation that promotes responsible cyber information sharing and strengthens the Department of Homeland Security's (DHS) statutory authority to execute its mission. The committee is directly responsible for helping shape legal clarity to expand cyber information sharing, provide appropriately targeted liability protections for companies, and establish necessary privacy protections in the Cybersecurity Act of 2015. The end result reflects this committee's sound understanding of how critical public-private trust and cooperation is to effective information sharing, and I'm honored to support this committee's continued oversight responsibilities. So, let me first say thank you for your leadership and for the opportunity to speak with you today.

For those not familiar with Palo Alto Networks, we have become one of the world's largest cybersecurity companies just 10 years after our first product shipped, actively preventing successful cyber attacks for more than 37,000 corporate and Government enterprise customers in more than 150 countries world-wide. Our collaboration with DHS ranges from strategic policy development to operational initiatives, starting with a commitment from the top of our organization. Our CEO and chairman, Mark McLaughlin, just completed consecutive 2-year terms as chairman and vice chairman of the President's National Security Telecommunications Advisory Committee (NSTAC). Founded during the Reagan Administration and administered by DHS, NSTAC brings industry chief executives together to provide counsel on National security policy and technical issues for the president and other U.S. Government leadership.

Since joining Palo Alto Networks in January of 2015, my principal role has been to work with governments, companies, and organizations around the world to develop and implement strategies, policies, and operational partnerships that prevent successful cyber attacks. Candidly, this approach to cybersecurity builds naturally upon the years I spent at the DHS and on the National Security Council at the White House, and it reflects the operational reality that cybersecurity is fundamentally a shared and distributed challenge that can only be effectively addressed through collaboration, which leverages the unique capabilities and authorities of companies, individuals, and governments.

To that end, we maintain a regular cadence with appropriate government and law enforcement stakeholders around the world. The U.S. Department of Homeland Security is the cornerstone of these government engagements because of its mission to collectively prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents. Our robust and multi-faceted partnership with DHS includes participation in formalized programs, as well as more informal collaboration mechanisms built on trust and personal relationships. We engage with DHS as an individual company and as part of broader collectives of private-sector entities.

My testimony today will address the full spectrum of this DHS relationship, framing why public-private sector collaboration is so critical to improving our cybersecurity as a Nation—and what collective actions we believe private industry and Government must take to effectively leverage information sharing as a tool to achieve the desired outcome of increased cybersecurity. Finally, I'll outline specific examples of our collaboration with DHS—including information sharing, policy development, and cybersecurity exercises. In doing so, I'll highlight several tangible success stories of public-private partnerships; opportunities for potential improvements; and, not only what Congress has done to incentivize these partnerships, but also what can be done to further enable progress in these areas.

WHY PUBLIC-PRIVATE SECTOR CYBERSECURITY COLLABORATION IS IMPORTANT

Before providing an assessment of the current state of DHS and private-sector cybersecurity collaboration, it is critical that we clearly define the objectives we are seeking to achieve through this partnership. As arguably the most developed mechanism of public-private sector cooperation, cyber information sharing provides a valuable use case for this discussion.

As the concept of information sharing has received wide-spread attention in recent years, the term has adopted an increasingly broad and varied definition. Because of this, it is critical to clearly define how Palo Alto Networks approaches information sharing, and how it fits into our broader mission of raising costs for our adversaries and actively preventing cyber attacks. This approach recognizes that cyber threat information sharing, while critical, is not a panacea. Information sharing is one necessary tool within a much larger strategy that leverages people, process, and technology to tangibly reverse the attackers' current advantage in cyber space.

The Palo Alto Networks perspective on cybersecurity is built on a relatively simple premise: We believe that cybersecurity is a correctable math problem that, at present, overwhelmingly favors the attackers. As the cost of computing continues to decline, our adversaries have been able to conduct increasingly automated, successful attacks at minimal cost. In fact, many free and open-source tools are available on-line that enable repeatedly successful attacks against poorly-defended networks. In the face of this automated onslaught, the network defender is generally relying on legacy security technologies, often cobbled together as multiple layers of "point" products that solve discreet problems but do not interoperate in a way that can holistically reduce priority risks across an organization's entire network infrastructure. This increased technological complexity creates a dependence on people—one of the least scalable resources in any organization—to manually defend against automated, machine-generated attacks. Network defenders are simply losing the economics of the cybersecurity challenge.

To flip this equation and gain back leverage against our adversaries, we need to collectively embrace integrated approaches that simplify and automate network defense to actively prevent cyber attacks. This is a critical point: If we focus on preventing attacks in the correct locations—informed by sophisticated and integrated detection capabilities—we can deter malicious activity by making it more expensive in terms of resources, time, and personal impact for our adversaries to launch a successful attack. True integration across the cybersecurity ecosystem—leveraging initiatives like automated information sharing and technology orchestration—can be the catalyst in reversing this current unsustainable dynamic that exists in cyber space.

Our approach to automated integration begins within our own technology platform. We build technology that prevents attacks at the key tactical and strategic places where cyber attackers need to take action to be successful, and we update our global customer base with the latest protections in as little as 5 minutes. As a matter of scope, we generate more than 1 million new preventive measures each week as we identify new, or "zero-day," cyber threats. This is not to imply that we—nor any one company or Government—can alone see and prevent all the evolving automated threats facing network defenders. Consequently, we partner with other companies and appropriate Government agencies whose competencies complement ours to help gain the leverage required to disrupt attackers and their tools.

At its core, our company's network defense and information-sharing philosophy closely mirrors the ultimate vision for information sharing championed by this committee. Our approach is focused on three primary objectives: (1) Protect against all known cyber threats; (2) turn unknown threats into known threats as quickly as possible; and (3) automatically leverage this new threat knowledge to create preventive countermeasures that are shared broadly within the ecosystem to prevent other entities from falling victim to similar attacks. This last component is critical. As this committee knows well, information sharing is too often a time-intensive process that requires a human to read, interpret, and manually create prevention controls based on technical cyber threat indicators provided in a non-machine-readable format like a PDF or email. This manual process simply can't scale to the speed and sophistication of the modern cyber threat environment.

Sophisticated cybersecurity companies can uniquely contribute to this challenge because we collectively have the physical infrastructure and processing ability to automatically deploy preventive measures based on new threat information to a broad customer base across multiple sectors. For these reasons, Palo Alto Networks and other sophisticated cybersecurity companies can bring a degree of actionability to information sharing that is critical for achieving our ultimate goals of raising adversary costs and tangibly improving cybersecurity across the ecosystem.

Our approach to automated integration doesn't end with our own platform or even our own company. In 2014, Palo Alto Networks was a founding member of the Cyber Threat Alliance (CTA). The CTA was incorporated in January 2017 as an independent, non-profit organization focused on cybersecurity information sharing. It is the first information-sharing organization specifically among cybersecurity vendors. Michael Daniel, the former special assistant to the President and White House cybersecurity coordinator, was just appointed as the CTA's first president. The CTA now includes six of the largest global cybersecurity companies as founding members—Check Point, Cisco, Fortinet, McAfee, Palo Alto Networks and Symantec—underscoring the philosophy that we can be force multipliers in support of a coordinated threat-sharing effort against cyber adversaries.

To fulfill its core mission, the CTA has built an automated information-sharing platform with the goal of enabling and incentivizing the sharing of high-quality, actionable threat information. The CTA and its platform embody a major step forward in transforming shared threat information into effective preventive measures that can automatically be deployed by CTA members to their respective customers. This isn't purely conceptual; the CTA platform is actively working to protect its members and their customers in near-real-time.

For example, recently, a single shared sample from one CTA member allowed another member to build protections before that organization's customers were targeted—preventing successful attacks against 29 subsequent organizations. In another instance, data shared through the CTA from one member allowed another member to identify a targeted attack against its customer and release additional indicators to defend that organization. The CTA and its platform have shown that a well-designed and well-built information-sharing program can foster the sharing of high-quality threat information among competitors, with members finding that 40 to 50 percent of shared data is new and directly actionable.

The CTA model directly addresses many of the aspects that have limited the effectiveness of other information-sharing relationships, both formal and informal. First, the CTA addresses the problem of information-sharing "free riders" that join information-sharing groups and simply receive information without sharing. Universal contributions are achieved by establishing mandatory sharing minimums for CTA members: Initially on a quantitative basis (1,000 unique cyber indicators/per day) and now evolving into a scoring system that measures the qualitative value of shared data. Second, the CTA is focused on sharing indicators related to an adversary's playbook—a more limited and predictable series of steps an adversary must take to complete a successful cyber attack. This is a key departure from many information-sharing organizations, which focus instead on sharing malware samples that can be polymorphic and exist in an exponentially larger quantity than the number of unique adversary playbooks. Third, because the CTA members' collective customer base spans all industry sectors, the impact of sharing can protect a large percentage of the global ecosystem. This type of broad-based sharing of widely-used threat techniques can help neutralize unsophisticated actors and force sophisticated adversaries, such as nation-states, to develop new (and therefore costlier) techniques. This narrowing of the threat landscape can make attribution easier and enable governments to more effectively target high-priority and advanced persistent adversaries and threats.

Government has a complementary and equally critical role to play in fostering information sharing across the ecosystem by leveraging its unique authorities and capabilities. DHS, for example, has the ability to amplify and distribute cyber threat information to a wide cross-section of industry and critical infrastructure operators.

Historically, there have been many efforts by the U.S. Government to more quickly declassify cyber threat information for distribution to the broader community. However, given the rapid pace in which cyber threats mutate and spread, the largely manual declassification process is rarely fast enough to simultaneously outpace the threat and avoid disclosures of intelligence sources and methods. Infused with a much wider set of Unclassified information from the private sector, Government could be able to more quickly add valuable insight and perspective without declassifying information. Leveraging the unique visibility they possess from Classified information, governments can instead help direct private-sector attention and resources to publicly available information on priority threats, such as nation-state activity that may target a particular sector, like energy or finance, in a way that doesn't reveal Classified information.

PALO ALTO NETWORKS ENGAGEMENTS WITH DHS ON CYBERSECURITY ISSUES

The Palo Alto Networks collaboration with DHS takes many forms—both formal and informal—and is related to a broad range of policy and operational activities. Operationally, our formal and informal collaboration with DHS has ranged from programmatic relationships to targeted sharing of threat intelligence reports generated by Unit 42, the Palo Alto Networks threat intelligence team. These efforts highlight threat information sharing conducted as an individual company and as a founding member of the Cyber Threat Alliance.

Cyber Threat Sharing Examples.—Prior to our joining the two DHS formal sharing programs, the Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Indicator Sharing (AIS) program, we established informal processes to share threats, vulnerabilities, and malicious cyber threat campaign information with DHS based on personal relationships and our knowledge of their mission and capabilities. When appropriate, we share advanced copies of significant threat reports with DHS cyber policy leadership and operational teams at the National Cybersecurity and Communications Integration Center (NCCIC). I'd like to highlight just a few specific examples of these information-sharing success stories that embody the type of public-private cooperation this committee has sought to encourage.

- In December 2016, Palo Alto Networks threat intelligence team, Unit 42, discovered new samples of Disttrack—an evolution of the same malware that was used in the August 2012 "Shamoon" cyber attack that destroyed over 30,000 hard drives at a Saudi Arabian energy company. The original Shamoon attack is widely considered one of the most significant and destructive cyber attacks in history. Prior to our report's public release, we coordinated with DHS to enable them to take preventive action. Based on several reports by Palo Alto Networks and other researchers, DHS: (1) Issued two Information Bulletins to the CISCP community of network defense stakeholders, (2) updated their Indicators of Compromise (IOC) databases, and (3) created EINSTEIN signatures related to the threat to protect other Federal Government civilian agencies.
- In early 2016, the Palo Alto Networks threat intelligence team released a report entitled Scarlet Mimic, identifying a long-running cyber campaign targeting minority activists in China, as well as Russian and Indian government organizations responsible for tracking activist and terrorist activities. Palo Alto Networks reached out directly to DHS to share indicators related to Scarlet Mimic, allowing them to deploy preventive countermeasures across their community of network defense partners. Specifically, DHS indicated its intention to: Update their Indicators of Compromise databases, vet IOCs against the intelligence community's Classified databases to determine threat group attribution, create EINSTEIN signatures to protect other Federal civilian agencies, and generate STIX™ files for automated distribution to their private-sector CISCP partners.
- In other instances, we coordinate our outreach to DHS as part of remediation efforts with public disclosure of new vulnerabilities that our threat intelligence team discovers in publicly-available technology across the ecosystem. For example, in early 2015, our threat intelligence team identified a new vulnerability in Android™ operating systems. We rapidly shared the information with Google®, so they could take steps to remediate the vulnerability, and then contacted DHS as we published the report. DHS used the provided information to generate a US–CERT alert and push the notification to their public website and their broad community of network defender partners.
- As part of the Cyber Threat Alliance, Palo Alto Networks coordinated with DHS as well as other U.S. and international government stakeholders to share threat information about CryptoWall v3—a ransomware campaign that had extorted over $300 million from victims in under 1 year. Based on CTA's shared cyber threat indicators, DHS and the FBI were able to notify victims whose websites were unknowingly compromised; contact internet service providers to disrupt compromised infrastructure; and send alerts to their network defense partners, including the international CERT community, to protect against CryptoWall v3 tactics. Subsequently, the U.S. Government shared back 170 unique CryptoWall indicators with the CTA, beyond the roughly 850 indicators the CTA report initially identified. This CryptoWall example is distinct as a tangible illustration with quantifiable metrics of two-way sharing of cyber threat information between the Government and private sector.

While each of these represents an individual success story and an illustrative use case, we need to focus our collective effort on ensuring these success stories are the rule rather than the exception. We can accomplish this by continuing to build trust among partners, refining the processes, enhancing the existing sharing infrastructure, and remaining committed to automating threat sharing in a way that can effectively scale to the pace of the cyber threats.

DHS Cyberthreat Sharing Programs.—Regarding formal information-sharing partnerships, Palo Alto Networks is a member of DHS's two primary cybersecurity information-sharing programs: The Cyber Information Sharing and Collaboration Program (CISCP) and the Automated Indicator Sharing (AIS) program.

- CISCP is a program established to promote robust information-sharing and analytic collaboration between DHS and vetted private-sector partners, especially the critical infrastructure community.
- Implemented in accordance with the Cybersecurity Act of 2015, AIS is a DHS-developed capability to enable the automated exchange of anonymized cyberthreat indicators among a wider range of private-sector entities and the U.S. Federal Government.

AIS is intended to provide threat indicators at "machine speed" aligns directly with our efforts to increasingly automate threat sharing, as outlined above. We applaud the concept of AIS and view it as both complementary and reinforcing to the type of automated information sharing that is already responsibly occurring at Palo

Alto Networks and within entities like the Cyber Threat Alliance. DHS should be commended for their continued progress in maturing these information-sharing program capabilities, but there are certainly tangible opportunities for improvement.

As discussed with DHS, we believe that the administrative process for joining these programs could certainly be easier and more efficient. Because programs like AIS are dramatically enhanced by the number of contributing members, DHS would benefit from investing in resources that streamline on-boarding processes and generally make these private sector-interfacing programs more customer service-focused. Specifically, DHS should develop a clear step-by-step guide for on-boarding, publish those requirements broadly, and promote a singular "help desk"-type contact for all questions related to the programs. To their credit, DHS senior officials recognize these shortcomings, and plan to take concrete steps to implement personnel and process reforms that should ultimately make the AIS program more customer service-centric.

Operationally, both AIS and CISCP have initial baseline capabilities and value, but they also could benefit from incorporating best practices from industry information-sharing efforts, such as the Cyber Threat Alliance's platform. According to DHS, AIS has delivered over 218,000 unique indicators since March 2016. Additionally, CISCP published 283 Indicator Bulletins in 2016, including nearly 1,300 indicators of compromise, with a recognition they need to refine their ability to provide useful, Unclassified context. However, DHS could further engage industry to leverage vendor-neutral technology and techniques that more rapidly share larger volumes of actionable cyber-threat information with context about how individual malware is used as part of broader campaigns.

Information-Sharing Analysis Organizations (ISAO).—Regarding cyber-threat information-sharing policy development, Palo Alto Networks had a leadership role in DHS's effort to establish and identify standards and best practices for Information-Sharing Analysis Organizations (ISAO), following a 2014 Presidential Executive Order establishing ISAOs. Specifically, our chief security officer, Rick Howard, led the effort on information privacy and security in one of six working groups that wrote and published the official ISAO standards in September 2016.

National Security Telecommunications Advisory Committee (NSTAC).—Previously, I referenced our broader policy engagements with DHS, such as our CEO Mark McLaughlin's current membership and former leadership roles in the President's National Security Telecommunications Advisory Committee (NSTAC). Administered by DHS, the NSTAC has recently grown to become an increasingly relevant policy forum for collaboration between private industry and the U.S. Government. Senior cybersecurity officials representing the White House and the Department of Homeland Security have repeatedly acknowledged the direct impact of NSTAC studies on the formulation of U.S. policy. The NSTAC has also played an important role in fostering relationships between Government and the private-sector technology community. For example, in mid-2016, the NSTAC hosted the first-ever meeting in its 34-year history in Silicon Valley, with significant U.S. Government participation, including the Secretaries of Commerce, Defense, and Homeland Security, as well as Admiral Rogers, Director of NSA and Commander of U.S. Cyber Command.

Information Technology Sector Coordinating Council (IT–SCC).—Palo Alto Networks is an Executive Committee member of the IT-Sector Coordinating Council, the principal entity for coordination between the Department of Homeland Security and IT sector companies and associations on a range of critical infrastructure protection and cybersecurity issues. The IT–SCC provides another official mechanism for Palo Alto Networks to collaborate with IT sector companies and DHS senior cyber officials on a range of sector-relevant policy, and cybersecurity issues.

Cyber Storm V.—Palo Alto Networks was also actively engaged in the planning and execution of Cyber Storm V in early 2016. The biannual National cyber exercise is led by DHS and brings together over 1,100 U.S. Government and private-sector participants to test the cyber incident coordination processes that helped test and inform operational procedures and subsequent National policies. We commend DHS for their leadership and execution of these complex exercises, and would like to increasingly add realistic technical components to future iterations. Planning for Cyber Storm VI in 2018 has recently commenced, and we look forward to again working closely with DHS on this critical initiative.

LEGISLATIVE SUCCESSES AND CONGRESSIONAL OVERSIGHT OF DHS INFORMATION-SHARING INITIATIVES

As discussed in my introduction, this committee has played a central role in passing a range of cybersecurity legislation that promotes responsible cyber-threat information-sharing and strengthens DHS's statutory authority to execute its mission.

The information-sharing portion of the Cyber Act (Title I) understandably garners most of the attention, and today's hearing demonstrates the need for oversight to ensure that Congress and DHS continue to identify areas of both progress necessary further improvements in its implementation.

In general, efforts to promote more direct engagement between DHS and the private-sector technology community to address homeland security mission requirements should be encouraged. This can take the form of new legislation, such as Chairman Ratcliffe's recently introduced bill on leveraging emerging technologies, to oversight of existing laws, such as Title II of the Cybersecurity Information Sharing Act of 2015.

Thank you very much for the opportunity to testify before you today. I look forward to any questions you may have and your continued partnership on this critical issue.

ATTACHMENT 1.—LUCRATIVE RANSOMWARE ATTACKS: ANALYSIS OF THE CRYPTOWALL VERSION 3 THREAT [1]

ATTACHMENT 2.—SHAMOON 2: RETURN OF THE DISTTRACK WIPER [2]

ATTACHMENT 3.—SCARLET MIMIC: YEARS-LONG ESPIONAGE CAMPAIGN TARGETS MINORITY ACTIVISTS [3]

ATTACHMENT 4.—ANDROID INSTALLER HIJACKING VULNERABILITY COULD EXPOSE ANDROID USERS TO MALWARE [4]

Mr. RATCLIFFE. Thank you, Mr. Gillis.

Ms. Greene, you are recognized for 5 minutes.

STATEMENT OF ROBYN GREENE, POLICY COUNSEL AND GOVERNMENT AFFAIRS LEAD, OPEN TECHNOLOGY INSTITUTE, NEW AMERICA

Ms. ROBYN GREENE. Thank you, Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee for the opportunity to testify today.

As a policy council and government affairs lead at New America's Open Technology Institute, I specialize in issues related to privacy, cybersecurity, and surveillance.

My statement today will cover three subjects: First, outstanding privacy concerns in the Cybersecurity Information Sharing Act, CISA; second, how DHS's balanced approach to implementing CISA has improved cybersecurity and protected privacy; and third, that a more holistic approach to cybersecurity, beyond information sharing, is essential.

CISA provides important improvements for many previous iterations of information-sharing legislation. Many of those improvements are the result of this committee's hard work and leadership to protect privacy while improving cybersecurity.

But despite this committee's laudable efforts, certain privacy concerns remain unaddressed, like imprecise definitions for the terms like "cybersecurity threat" and "cyber threat indicator," and a weak requirement for the removal of personal information.

These shortfalls raise concerns that CISA may threaten privacy and undermine security by resulting in the sharing of unnecessary

[1] *https://www.cyberthreatalliance.org/pdf/cryptowall-report.pdf.*

[2] *https://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/.*

[3] *https://researchcenter.paloaltonetworks.com/2016/01/scarlet-mimic-years-long-espionage-targets-minority-activists/.*

[4] *https://researchcenter.paloaltonetworks.com/2015/03/android-installer-hijacking-vulnerability-could-expose-android-users-to-malware/.*

information, like information related to false alarms or communications content and other irrelevant personal information.

Also troubling are CISA's over-broad use authorizations for law enforcement to use information it obtains from companies shred for a cybersecurity purpose, for investigations and prosecutions that are entirely unrelated to cybersecurity.

This undermines Fourth Amendment protections because it allows law enforcement to use information that it would obtain ordinarily pursuant to a warrant or a court order.

Finally, CISA includes a provision that allows the President to undermine DHS's role as the lead portal for information sharing by establishing a second portal, possibly at a law enforcement or intelligence oversight agency, like the FBI or the Office of the Director of National Intelligence. This would harm civil liberties and threaten user trust, which is essential for companies to feel comfortable participating in the information-sharing program.

With all of that said, DHS has done a good job of promulgating guidelines and procedures under CISA that protect privacy and strengthen cybersecurity. DHS has provided clear interpretations and applications of vague definitions and requirements.

Additionally, DHS leveraged STIX in its automated indicator-sharing system to establish standardized fields of information sharing and it retained human review of personal information that is shared.

With these steps, DHS has minimized the risk of unnecessary sharing and dissemination of Americans' personal information. The committee should continue to support DHS in this important work.

Since information sharing is not a panacea, more must still be done to improve cybersecurity. The Government must take a multi-pronged, holistic, and outcomes-based approach. DHS must increase the amount of information it shares with the private sector, including getting more threat indicators declassified.

To protect ourselves from another OPM-style data breach, Congress must ensure that the Federal Government has the resources needed to modernize its IT infrastructure, to maintain up-to-date and secure devices and systems, and to hire a robust work force of security and technology policy experts.

Recent reporting suggests that the Government is struggling to fill open cybersecurity positions and that this shortage may be threatening collaboration with industry.

The Federal Government can also help to improve overall security by finding ways to incentivize the private sector and individuals to update software with patches for vulnerabilities and by formalizing its approach to vulnerabilities management.

Wikileaks' disclosure of CIA hacking tools earlier this week highlight that it is possible for vulnerabilities to be publicly released and for individuals, industry, and the Government alike to be left exposed to malicious actors when this happens. This drives home how important it is for Congress to codify a process for the Government to disclose zero-day vulnerabilities as soon as possible so that they can be patched.

The Government should also help to shrink the size of the zero-day market by minimizing its participation in it.

Last, the Government should use its bully pulpit to champion the wide-spread use of security tools, like two-factor authentication and encryption, and it should incentivize companies to offer those tools by default, along with automatic software updates, as part of an effort to encourage privacy and security by design.

Thank you very much, and I look forward to your questions.

[The prepared statement of Ms. Greene follows:]

PREPARED STATEMENT OF ROBYN GREENE

MARCH 9, 2017

Thank you for the opportunity to testify today on "The Current State of DHS Private-Sector Engagement for Cybersecurity." I represent New America's Open Technology Institute (OTI), where I am a policy counsel and Government affairs lead on privacy, surveillance, and cybersecurity issues.

New America is a nonpartisan, nonprofit, civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences. OTI is a program at New America that works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators. Our current focus areas include surveillance, privacy and security, net neutrality, broadband access, and consumer privacy.

In December 2015, Congress passed the Cybersecurity Information Sharing Act (CISA).[1] The law provides private-sector entities with liability protection for sharing information about cybersecurity threats with one another and with the Government. Throughout the debate over information-sharing legislation, OTI voiced significant concerns about the scope of sharing permitted and the insufficient privacy protections for internet users both before and after information is shared. We also urged Congress to take a more holistic approach to cybersecurity policy, rather than focus solely on information sharing.[2]

My testimony will cover three topics: (1) OTI's outstanding privacy concerns related to how much information can be shared, with whom, and how it can be used under CISA; (2) the ways in which the Department of Homeland Security (DHS) has worked in its implementation of the law to protect privacy and simultaneously enhance cybersecurity, and (3) additional steps that the Government could take to strengthen public-private partnerships related to cybersecurity, and to incentivize or encourage the private sector to adopt best practices, to meaningfully protect privacy and improve overall security.

OUTSTANDING CONCERNS REGARDING THE CYBERSECURITY INFORMATION SHARING ACT (CISA)

Information-sharing legislation was extremely controversial for the entire time that Congress debated it, even up to the point that CISA became law. The most significant point of contention was always how to adequately protect privacy and civil liberties. CISA's predecessor, the Cyber Intelligence Sharing Protection Act (CISPA), contained no meaningful privacy protections when it was first introduced.[3] After years of advocacy by privacy and security experts, and several iterations of legislation, the final version of CISA included important improvements and protections. Nevertheless, certain privacy concerns were left unaddressed or inadequately addressed. Those shortfalls include imprecise definitions, a too-weak requirement to remove personal information before sharing cyber threat indicators, overbroad allowances for law enforcement to use shared data for purposes unrelated to cyberse-

[1] Cybersecurity Information Sharing Act, 6 U.S.C. 1501 et. seq., Public Law No: 114–113, H.R. 2029 Division N, Title I, 114th Cong. (2015), *https://www.Congress.gov/114/plaws/publ113/PLAW-114publ113.pdf*.

[2] Robyn Greene, *Congress Must Focus on More Than Information Sharing*, The Hill, Jan. 30, 2015, *http://thehill.com/blogs/congress-blog/technology/231190-congress-must-focus-on-more-than-information-sharing*.

[3] Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2011), *https://www.Congress.gov/112/bills/hr3523/BILLS-112hr3523ih.pdf*; see also Letter from the ACLU to Hon. Mike Rogers & Hon. C.A. "Dutch" Ruppersberger, Dec. 1, 2011, *https://www.aclu.org/other/aclu-opposition-hr-3523-cyber-intelligence-sharing-and-protection-act-2011*.

curity, and the possibility that the President will undermine DHS's role as the lead information-sharing portal by establishing a second authorized portal.[4]

CISA's overbroad definitions threaten privacy because they can result in over-sharing of personal or otherwise unnecessary information. This is the case for the definition of "cybersecurity threat," which triggers the authorization to share. The law defines a cybersecurity threat as anything that "may result in an unauthorized effort to adversely impact" a device or system.[5] It covers any potential threat and does not require that a company make a determination that the purported cyber threat is likely to cause harm before sharing their users' information.

This low threshold could spur sharing of unnecessary information, like that concerning false alarms, which would threaten privacy if the sharer transmits personal information as part of the cyber threat indicators shared. It could also undermine security. Unnecessary sharing of personal information can expose internet users to new threats should their information be successfully targeted and exfiltrated by malicious actors after being shared under CISA. Additionally, it can undermine security by creating "white noise" that distracts from imminent threats.[6]

Over-sharing could also result from the insufficiently narrow definition for "cyber threat indicator" and the inadequate requirement to remove personal information before sharing. Cyber threat indicators include "information that is necessary to describe or identify . . . the actual or potential harm caused by an incident . . . [or any] attribute of a cybersecurity threat" so long as disclosure of the underlying attribute is not otherwise legally prohibited.[7]

A broad interpretation of this definition could include personal information or content of on-line communications that is not needed to detect or protect against a threat. This is because information that could be deemed necessary to describe a threat or potential harms caused by an incident could still be unnecessary to identify or protect against the threat. For example, while it might be reasonable to share an IP address that is associated with malicious activity, the breadth of this definition might also permit a company to share any information they might have associated with that IP address that identifies a particular account holder or location because they claim it is necessary to describe the IP address. In the case of botnets, this identifying information might not necessarily belong to the malicious actor; it could belong to a botnet victim.

Similarly, under the law, companies can share any personal information so long as it is "directly related to a cybersecurity threat."[8] This could be interpreted in a manner that undermines privacy by allowing a company to share victim information or other personal information unnecessary to identify or protect against a threat. For example, a broad interpretation of this requirement could allow for a company to share the personal information of the victim of a cyber incident, like information about the recipient of a phishing email, since that information could be deemed to be "directly related" to the threat, even though it may not be necessary to identify or protect against the threat.[9]

In addition to insufficiently narrow definitions and weak front-end privacy protections, CISA overbroadly authorizes law enforcement to use the shared information for non-cybersecurity investigations. Under the statute, any information that is shared with the Government for a cybersecurity purpose may be used by law enforcement in investigations and prosecutions entirely unrelated to cybersecurity or computer crimes. Authorized uses include investigations and prosecutions into Trade Secrets Act and Espionage Act violations, undefined "serious economic

[4] Robyn Greene, *The Knock-Down, Drag-Out Fight Over Cybersecurity Legislation*, Slate, Jan. 15, 2016, *http://www.slate.com/articles/technology/future_tense/2016/01/how_the_privacy_community_made_cyber_security_legislation_better.html*.

[5] Supra note 1 at § 1501(5).

[6] See Letter from security experts to Sen. Dianne Feinstein, et al concerning information-sharing bills (Apr. 16, 2015), *https://cyberlaw.stanford.edu/files/blogs/technologists-_info_sharing_bills_letter_w_exhibit.pdf*.

[7] Supra note 1 at § 1501(6).

[8] Supra note 1 at § 1503(d)(2).

[9] As I discuss in the next section of this statement, DHS has done a good job of protecting privacy in its promulgation of guidance to companies on information sharing. It addresses this specific concern, making clear that companies should not share this kind of victim information. However, that guidance, and thus DHS's strict interpretation of the requirement to remove personal information, is subject to change. To better protect privacy, Congress should amend the law to address this concern. See Dep't of Homeland Security & Dep't of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measure with Federal Entities under the Cybersecurity Information Sharing Act of 2015* 5 (2016), *https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_(Sec%20-105(a)).pdf* [hereinafter "Company Guidance"].

harms," and certain violent crimes irrespective of whether the threat is imminent.[10] This undermines Fourth Amendment protections because it allows law enforcement to use information in investigations and prosecutions that it would ordinarily only be able to obtain pursuant to a warrant issued by a judge based on a finding of probable cause. Information sharing is subject to no judicial oversight, and thus no judge ever makes a finding of probable cause before law enforcement uses the information it receives under CISA, even where investigations are unrelated to cybersecurity.

Finally, CISA includes a provision that could call into question DHS's important and proper role as the lead civilian portal for private-sector information-sharing with the Government. Under CISA, if a company wants to receive liability protection for sharing cyber threat indicators with the Federal Government, it must share that information through an authorized portal.[11] Currently, DHS is the only authorized information-sharing portal. However, CISA authorizes the president to establish a secondary portal at any Federal entity except for the Department of Defense and the National Security Agency.[12]

If the President were to exercise this authority at a law enforcement or intelligence oversight agency like the Federal Bureau of Investigation or the Office of the Director of National Intelligence, it would significantly threaten privacy and undermine Americans' trust in the Federal Government's information-sharing program. Additionally, it would introduce operational weakness by further decentralizing information sharing and undermining DHS's role and authority as the Federal Government lead on domestic cybersecurity and private-sector engagement, which Congress just formally established in 2014.[13]

OTI believes that these outstanding flaws in CISA pose a clear threat to both privacy and effective cybersecurity practice, and hopes that Congress will consider amending it to address those concerns. However, despite those flaws, on the whole, DHS has done a good job of promulgating guidelines and procedures under CISA that protect privacy and strengthen cybersecurity. Congress should support DHS in this important work.

DHS IMPLEMENTATION OF CISA HAS BEEN EFFECTIVE AND PRIVACY-PROTECTIVE, BUT MORE SHOULD BE DONE TO IMPROVE INFORMATION SHARING

DHS has taken a reasonable and measured approach to implementing CISA that balances privacy and security. This is clear from how DHS set up its Automated Indicator Sharing system (AIS), and how its promulgation of procedures and guidelines clarified ill-defined terms and standards in the statute.

When DHS rolled out AIS, it leveraged Structured Threat Information eXchange (STIX) to establish standardized fields of information that can be shared and Trusted Automated eXchange of Indicator Information (TAXII) as the secure, automated method for sharing information.[14] This was an important step, because by setting out specific, standardized fields of information that can be shared, STIX limits the potential for sharing unnecessary personal information.

It is still possible for unnecessary personal information to be shared under CISA, because there are STIX fields that could include it or that allow a submitter to copy and paste communications content, and because a submitter could choose to send an email in lieu of submitting information via AIS. DHS mitigates this privacy risk by ensuring that any personal information included in one of those three types of submissions is subject to human review to determine if it is necessary to describe or identify the threat. The personal information is then either removed if it does not meet the standard or further disseminated if it does. DHS also discourages the use of e-mail to submit cyber threat indicators.[15]

Additionally, DHS guidance on how to determine if personal information must be removed is effective at protecting privacy, considering the requirements of the stat-

[10] Supra note 1 at § 1504(d)(5)(A).

[11] Supra note 1, at § 1505(b).

[12] Id. at § 1504(c)(2)(B).

[13] Robyn Greene, *Dangerous for Cybersecurity and Privacy: Cotton Amendment No. 2581*, New America's Open Technology Institute (Aug. 25, 2015), *https://www.newamerica.org/oti/blog/dangerous-for-cybersecurity-and-privacy-cotton-amendment-no-2581/* [analyzing a proposed amendment to CISA that would have authorized the FBI as an additional covered information-sharing portal]; and National Cybersecurity Protection Act of 2014, 6 USC 148 note, et seq., Public Law No: 113–282.

[14] *Company Guidance*, supra note 9 at 22.

[15] Dep't of Homeland Security & Dep't of Justice, *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government 8*, 10 (2016), *https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_(105(a)).pdf* [hereinafter "Final Proocedures"].

ute. DHS establishes a clear application of the test for removal of such information in its guidance to Federal entities. It lays out the critical three-part test: (1) Do you know it is "personal information of a specific individual or information that identifies a specific individual"? (2) If yes, is it directly related to the threat? (3) If yes, then the entity may share it, and if no, then it must be removed prior to dissemination.[16]

Importantly, DHS also narrowly interprets the standard for removal of personal information in company guidance and in privacy guidelines for Federal entities. It does so by offering a clear explanation of what is "directly related" to a cybersecurity threat. DHS provides that "Information is not directly related to a cybersecurity threat if it is not necessary to detect, prevent, or mitigate the cybersecurity threat."[17] It also offers examples to illustrate what kinds of personal information can and cannot be shared. Both documents highlight that personal information related to victims of cyber attacks, such as information that identifies the recipient of a phishing email, is not directly related to a cybersecurity threat, and must be removed before sharing or dissemination.[18]

The standard for removal of personal information before sharing or dissemination of cyber threat indicators was one of the most contentious aspect of the debate. Opponents of a strict removal requirement were concerned that a higher standard would slow down sharing and raise questions about when liability protections under the law are triggered. These concerns have been largely put to rest. In the vast majority of cases, speed of information sharing is not a determining factor in preventing an attack. The most recent Verizon data breach report concluded that 93 percent of successful attacks took minutes to breach a device or network, but organizations took weeks to discover them, leaving ample time for the attacker to have identified and stolen the sought-after data in most cases.[19]

DHS's application of this standard for removal is also aligned with Congress' goal in passing CISA: to enhance security while simultaneously protecting privacy. Personal information is constantly targeted by hackers, as we have seen in countless data breaches, whether they be at Government agencies like the Office of Personnel Management (OPM), health care providers like Anthem, retailers like Target and Home Depot, financial institutions like J.P. Morgan, or technology companies like Yahoo.[20] The more personal information is shared with more entities, the larger the target for malicious hackers and nation-states seeking to breach our defenses.[21] Thus, by reducing the amount of personal information shared under CISA, DHS is serving a critical security function, as well as protecting privacy.

Privacy is not only essential to data security but also to trust. To the extent that information sharing is an important element of a holistic cybersecurity strategy, having adequate standards in the law and its application are essential to expanding its reach and impact. Companies will be uncomfortable sharing information if they worry their users will see it as harmful to their privacy. Indeed, 2 months before CISA's final passage, many leading technology companies and trade associations

[16] Dep't of Homeland Security & Dep't of Justice, *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015* 12 (2016), *https://www.us-cert.gov/sites/default/files/ais__files/Privacy__and__Civil__Liberties__Guidelines__(Sec%20105(b)).pdf* [hereinafter "Privacy Guidelines"].

[17] *Company Guidance* supra note 9, at 5.

[18] Id. See also *Privacy Guidelines* supra note 16, at 12.

[19] Verizon, *2016 Data Breach Investigations Report: Executive Summary 2* (2016), *http://www.verizonenterprise.com/resources/reports/rp__dbir__092016-executive-summary__xg__en.pdf*. Full report available at *http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/*.

[20] See Brian Naylor, *One Year After OPM Data Breach, What Has The Government Learned?, NPR, Jun. 6, 2016, http://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned*; Steve Ragan, *Anthem: How Does a Breach Like This Happen?* CSO, Feb. 9, 2015, *http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html*; Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZD Net, Feb. 2, 2015, *http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/*; Julie Creswell & Nicole Perlroth, *Ex-Employees Say Home Depot Left Data Vulnerable*, NY Times, Sept. 19, 2014, *https://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?partner=rss&emc=rss&__r=2*; Matthew Goldstein, Nicole Perlroth & Michael Corkery, *Neglected Server Provided Entry for JPMorgan Hackers*, NY Times, Dec. 22, 2014, *https://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?__r=1*; and Asha McLean, *Yahoo Says 32m User Accounts Were Accessed via Cookie Forging Attack*, ZD Net, Mar. 2, 2017, *http://www.zdnet.com/article/yahoo-says–32m-user-accounts-accessed-via-cookie-forging-attack/*.

[21] Robyn Greene, *Is CISA Gift-wrapped for Hackers and Nation-State Actors?* The Hill, Aug. 3, 2015, *http://thehill.com/blogs/pundits-blog/technology/250070-is-cisa-gift-wrapped-for-hackers-and-nation-state-actors*.

specifically cited its insufficient privacy protections as their grounds for opposition to the bill.[22]

Though DHS has done a good job implementing CISA in a manner that protects privacy and enhances security, Congress should address the outstanding concerns outlined above by codifying these sensible implementations in the law itself. This would provide the public and the private sector with the assurance that the protections as applied by the various guidelines and procedures will not be altered or reinterpreted in a manner harmful to privacy by this or any future administration.

Finally, more must still be done to increase information sharing by the Government with the private sector. Throughout the debate on information sharing security experts were clear that CISA would likely have only a modest impact on security, if it had any impact at all, because it focuses on increasing information sharing from the private sector to the Government or to other private-sector entities. These experts argued that in order to enhance cybersecurity by increasing information sharing, the Government needs to improve its system for sharing actionable information with the private sector. Specifically, experts called on the Government to declassify more information and share it with a broader set of stakeholders, to speed up its declassification process, and to expand the pool of stakeholders that are cleared to receive Classified indicators.[23] Congress should look to how it can help DHS address these concerns.

While improving information sharing can be an important element to cybersecurity, it is just one of many steps that must be taken overall. Ultimately, the only effective approach to cybersecurity will be a holistic approach.

ADDITIONAL STEPS TO STRENGTHEN PRIVATE SECTOR-PUBLIC SECTOR PARTNERSHIPS TO IMPROVE CYBERSECURITY AND PROTECT PRIVACY

OTI has long argued that while information sharing can have value, it is only a part of the more holistic approach to cybersecurity that Congress, the Federal Government, and the private sector must take. That approach necessitates more resources for the Federal Government, as well as more public education about cybersecurity threats and how to defend against them. The Federal Government also needs to take a “whole-of-Government” approach to cybersecurity issues. This is especially needed in two areas: The establishment of policies on vulnerabilities management, and identifying ways to encourage users and private companies to adopt security best practices, like increasing the use of multi-factor authentication and encryption.

Ensuring that all agencies have sufficient resources to buy newer, more secure hardware and software systems, and to recruit and retain a robust staff of skilled security and technology policy experts, has been a long-standing problem. This was one of the problems that led to the OPM breach that resulted in the exfiltration of over 20 million records. Ann Barron-DiCamillo, DHS lead on the team that investigated the breach, stressed that “[OPM] had older systems, that needed to be modernized . . . They had neglected networks from the perspective of putting in the cybersecurity sensors and technologies that they need to find adversaries in the network.”[24]

Less than a year after the OPM breach became public, the previous administration announced the establishment of the President’s Commission on Enhancing National Cybersecurity.[25] The commission concluded its work with the issuance of the Cybersecurity National Action Plan (CNAP). Many of the Commission’s recommendations focused on adequately resourcing the Federal Government. They recommended increasing the cybersecurity budget to $19 billion in fiscal year 2017, including investing $3.1 billion in information technology modernization to ensure that Federal devices and networks would be compatible with modern security tools; and allocating an additional $62 million to training and hiring new cybersecurity personnel.[26]

[22] Robyn Greene, *Tech Industry Leaders Oppose CISA as Dangerous to Privacy and Security*, The Hill, Oct. 21, 2015, *http://thehill.com/blogs/pundits-blog/technology/257601-tech-industry-leaders-oppose-cisa-as-dangerous-to-privacy-and*.

[23] Sara Sorcher, *Security Pros: Cyberthreat Info-sharing Won’t Be as Effective as Congress Thinks*, Christian Sci. Monitor, Jun. 12, 2015, *http://www.csmonitor.com/World/Passcode/2015/0612/Security-pros-Cyberthreat-info-sharing-won-t-be-as-effective-as-Congress-thinks*.

[24] *One Year After the Government Data Breach*, supra note 20.

[25] Michael Daniel, Ed Felten, & Tony Scott, *Announcing the President’s Commission on Enhancing National Cybersecurity*, The White House, Apr. 13, 2016, *https://obamawhitehouse.archives.gov/blog/2016/04/13/announcing-presidents-commission-enhancing-national-cybersecurity*.

[26] Press Release, Office of the Press Secretary, White House, Fact Sheet: Cybersecurity National Action Plan (Feb. 9, 2016), *https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan*.

These recommendations to significantly increase Federal spending related to cybersecurity are well taken, considering the scale of attacks on Federal Government networks in recent years and the difficulty the Federal Government has hiring and retaining cybersecurity experts.[27] As Congress drafts the budget for fiscal year 2017, it should allocate whatever resources will be necessary to hire a skilled workforce, and to modernize Federal Government networks and harden them against attacks.

In addition to proper resourcing, the Federal Government, including DHS, should continue its efforts to educate industry and the public about how to better protect themselves on-line. Increased education on how to identify social engineering attacks is particularly needed. Internet users' susceptibility to these kinds of threats has proven to be a somewhat intractable problem over the years. The most recent Verizon data breach report found that 30 percent of recipients of phishing emails opened them (a 23 percent increase from the prior year), and 12 percent of those people downloaded the malicious attachment or clicked on the malicious link.[28] Nonetheless, raising awareness of these threats via campaigns like "Stop. Think. Connect." may be the first step to reducing the threats' effectiveness.[29]

While resourcing and education are important, DHS must also be part of a whole-of-Government approach to cybersecurity and engagement with the private sector. Two areas that could most positively impact our Nation's cybersecurity are vulnerability management and wide-spread adoption of security best practices.

One key aspect of vulnerability management is incentivizing the private sector and individuals to protect themselves against known vulnerabilities by regularly updating their software so that known vulnerabilities are patched. Yet for 8 years, Congress focused almost entirely on how to increase information sharing about those vulnerabilities, without doing anything to help ensure that they are patched. Indeed, CISA explicitly states that a company is not required to act on the threat information it receives.[30]

Unsurprisingly, the private sector often only takes action to update their systems after a massive breach, but maintaining updated software would protect against the vast majority of threats. Approximately 85 percent of successful exploits used the same 10 vulnerabilities, all of which have patches available.[31] In order for CISA to have its intended impact, the Government and the private sector must turn information sharing into action by encouraging more and more regular patching of known vulnerabilities.

Another critical aspect to vulnerabilities management concerns how the Federal Government and Congress approach laws and policies impacting vulnerability research and disclosure, and Government participation in the market for previously undiscovered vulnerabilities, called "zero-days." Last year, OTI published a research paper called "Bugs in the System" that serves as a primer on the vulnerabilities ecosystem. We concluded that the leading factors hindering effective vulnerabilities management were a lack of clarity about how best to disclose newly-discovered vulnerabilities in order to see them patched; the chilling effect that out-of-date technology laws have on security researchers; and the existence of and U.S. Government participation in the zero-day market.[32]

We made five recommendations as to how Congress and the Federal Government could most effectively address these issues:

1. The U.S. Government should minimize its participation in the zero-day market: The zero-day market incentivizes selling vulnerability information to the highest bidder rather than disclosing it to the vendor so it can be fixed, and it caters to the intelligence and law enforcement arms of democratic governments and repressive regimes alike, as well as spies and criminals. The U.S. Government can significantly shrink this market simply by abstaining from it and instead relying on and growing resources and technical expertise at agencies like the NSA;[33]
2. The U.S. Government should establish strong, clear procedures for Government disclosure of the vulnerabilities it buys or discovers: When the Govern-

[27] Dustin Volz & Warren Strobel, *NSA Risks Talent Exodus Amid Morale Slump, Trump Fears,* Reuters, Feb. 28, 2017, *http://www.reuters.com/article/us-usa-cyber-nsa-idUSKBN1672ML.*

[28] Supra note 19, at 3.

[29] *Stop. Think. Connect.*, Dep't of Homeland Security, *https://www.dhs.gov/stopthinkconnect* (last visited Mar. 5, 2017).

[30] Supra note 1 at § 1505(c)(1)(B).

[31] Supra note 19 at 10.

[32] Andi Wilson, Ross Schulman, Kevin Bankston & Trey Herr, *Bugs in the System*, New America's Open Tech. Institute (July 2016), *https://na-production.s3.amazonaws.com/documents/Bugs-in-the-System-Final.pdf.*

[33] Id. at 21.

ment discovers or purchases vulnerabilities that put American internet users and companies at risk, it should ensure that they are disclosed and patched as soon as possible. While there is a process, called the Vulnerabilities Equities Process (VEP), to decide when the Government should disclose vulnerabilities, little is known about how that process works, how often it is used, and how effective it is at ensuring vulnerabilities are disclosed. Congress should investigate this issue, and then codify a process that agencies would be required to follow, and that heavily favors disclosure;[34]

3. Congress should establish clear rules of the road for Government hacking in order to protect cybersecurity in addition to civil liberties: Government hacking is as privacy-invasive as wiretapping, and it introduces a set of unique risks to security and to civil liberties, such as Government malware spreading to innocent people's computers, or resulting in unintended damage or the creation of new vulnerabilities. Yet, Congress has not established a clear legal framework for Government hacking, with rules and constraints that address these unique concerns, as it did to address concerns associated with wiretapping;[35]

4. Government and industry should support bug bounty programs as an alternative to the zero-day market and investigate other innovative ways to foster the disclosure and prompt patching of vulnerabilities: We can improve security by creating more avenues through which security experts can disclose vulnerabilities and diverse incentives for disclosing them, like through Vulnerability Reward Programs, often referred to as bug bounty programs. These programs also provide an outlet for researchers who do not want to participate in the zero-day market; and[36]

5. Congress should reform computer crime and copyright laws, and agencies should modify their application of such laws, to reduce the legal chill on legitimate security research: Out-of-date laws like the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), and the Digital Millennium Copyright Act (DMCA), chill security research. This is because under these laws, security researchers are threatened with criminal and civil penalties for their efforts to identify vulnerabilities and fix them.[37]

Finally, in addition to improving vulnerabilities management, the Federal Government must work with the private sector to help drive a cultural shift in Government and industry that embraces privacy by design, and that fuels wide-spread adoption of security best practices. OTI recently launched a project called "Do the Right Thing" in which we studied the factors that led to the wide-spread industry adoption of now common, though not yet ubiquitous, security tools like transit encryption by default and offering two-factor authentication. We found that Government was often influential in spurring increased adoption of these tools.[38]

DHS and other relevant Federal agencies should champion the use of multi-factor authentication and of encryption to protect stored data and communications in transit.[39] DHS should also work with relevant Federal entities and industry leaders to encourage a "privacy by design" approach to product development, including employing security mechanisms like automatic software updates and offering multi-factor authentication and encryption services by default. Thinking about security holistically and from the ground up will be especially important as more devices become connected and the internet of things morphs into simply "the internet."

[34] Id. at 21–22.

[35] Id. at 23.

[36] Id.

[37] Id. at 24.

[38] Kevin Bankston, Ross Schulman & Liz Woolery, *Getting Internet Companies To Do The Right Thing*, *https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/* (last visited Mar. 5, 2017). For a summary of all of the most common factors spurring the spread of three privacy and security best practices, see Kevin Bankston, Ross Schulman & Liz Woolery, *Key Lessons*, *https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/key-lessons/* (last visited Mar. 5, 2017).

[39] The question of how to address law enforcement access to encrypted communications has been the subject of intense controversy for several years. OTI strongly opposes any policy proposal that would amount to a mandate for exceptional access to encrypted communications, commonly referred to as encryption backdoors. For a detailed explanation of OTI's position on exceptional access for law enforcement, see Kevin Bankston, Written Statement to the House Committee on Oversight & Gov't Reform Subcommittee on Information Technology. *Encryption Technology and Possible U.S. Policy Responses*, Hearing, Apr. 29, 2015, *http://oversight.house.gov/wp-content/uploads/2015/04/4-29-2015-IT-Subcommittee-Hearing-on-Encryption-Bankston.pdf*. For more materials on OTI's position on encryption, see *Read this Before You Rail Against Encryption*, New America's Open Tech. Institute (Nov. 19, 2015), *https://www.newamerica.org/weekly/101/read-this-before-you-rail-against-encryption/*.

In conclusion, while CISA improved in some areas over the course of the Congressional debate, the final law left certain privacy concerns unresolved and in need of reform. CISA also addresses only a fraction of what Congress and industry should be thinking about as they work to enhance cybersecurity. The focus must now turn to an outcomes-based approach. Congress must ensure that all Federal agencies, including DHS, have the resources necessary to hire robust teams of security and technology policy experts, and maintain modern and up-to-date systems and equipment. It will also be essential to find ways to incentivize the private sector and individuals to take action based on new information, such as patching known and newly-discovered vulnerabilities and clarifying the Government's approach to vulnerabilities management in general. Finally, the relevant Federal agencies should take advantage of their bully pulpit to encourage broader adoption of security best practices like the use of encryption and two-factor authentication.

Mr. RATCLIFFE. Thank you, Ms. Greene.

Thanks all the witnesses for your testimony.

I now recognize myself for 5 minutes to ask questions.

In my opening remarks, I talked about the fact that we have got a new administration and with that provides us an opportunity to regroup and reassess.

I want to ask a broad question and give you all an opportunity to answer this.

To the extent that, you know the President's cybersecurity advisers, maybe even Secretary Kelly are listening to our hearing today or are subsequently briefed on it, if you had the opportunity to tell them to focus on one or two of the highest priorities or specific action items that you think that this administration ought to be focused on with respect to its DHS mission, what would that be? It could relate to private-sector relationships for cybersecurity or protection of our critical infrastructure at large.

But if you had that message to give, what would it be?

So let me start with you, Mr. Nutkis.

Mr. NUTKIS. Thank you, Mr. Chairman.

So I think from an ISAO perspective, the guidance we want is, what are the expectations and the role? I think, as the other testifiers have presented, we in industry are willing to step up and provide a lot of the interface. So with regards to AIS, we do that directly. So everyone in industry connects with us, we connect with DHS. We deal with a lot of the anonymization, a lot of the accuracy issues. So for us, it is guidance in working with what the expectations are.

We deal with a lot of the—we were sharing before the liability protections in CISA. We would like to see those increased and better guidance. So we would like to see clarity around the expectations from industry.

Then with regards to the framework, I will echo those sentiments is, it is voluntary and each industry has its own interpretation of the guidance and the guidelines that are established.

So the cybersecurity framework is a high-level framework. Each industry then has to customize it for their own requirements and then it has got to be customized specifically to the organization.

I just want to make sure there is clarity that one size does not fit all. There has got to be the ability for industries and organizations to be able to implement that based on the specific needs in a voluntary basis.

Mr. RATCLIFFE. Thank you.

Mr. Montgomery.

Mr. MONTGOMERY. Thank you. It is labor, labor, trained labor. As we have all talked about, the size and scale of the footprint, the impact upon our lives, the cyber impact upon our lives, it grows by leaps and bounds every minute. The notion that we are going to out-labor this one person at a time is preposterous.

So if we break labor into two buckets, bucket No. 1 is, certainly there is a shortfall, not only, as Ms. Greene pointed out, in the public sector, but also in the private sector. We are having trouble hiring people, too. So an intense focus upon education, making cyber a desirable career and an accessible career across a wide, disparate labor force that wants to work in cyber is essential.

But also, the need for reduced labor. We are not going to out-labor this problem one person at a time. So information sharing, automation, the ability to act at machine speed.

Our adversaries, as Mr. Greene pointed out earlier, they already utilize machines in order to further their campaigns and make it more automated. We need to be doing the same thing, not only with information sharing, but how we act on behalf of critical infrastructure.

Mr. RATCLIFFE. Thank you.

I will just say we have talked about the cyber work force as a priority of this subcommittee going forward, so I was glad to get your remarks.

Mr. Greene.

Mr. JEFFREY GREENE. So focusing on DHS, I think we need a clear statement. I would like to see a clear statement from the administration that there will be a civilian lead for, you know, continuing DHS, a civilian lead for the civilian cyber effort. I think it is important to send a message both to the companies that have developed relationships with DHS to know those are going to continue and also around the globe.

Secondarily is something that you mentioned in your opening statement, look at the operationalization of DHS. From our perspective having a long relationship, we know where the touch points are. We know who does cyber in DHS, who we reach out to for a specific issue. But if you don't know the structure and you are on the outside looking in, it is really hard to discern who does cyber, where you want to go to.

I do think aggregating the functions in a central place and providing an operational context to it is important.

Mr. RATCLIFFE. Thank you, Mr. Greene.

Mr. Gillis.

Mr. GILLIS. So I would focus very much on implementation. We are at a place right now where there aren't massive statutory barriers to executing the cybersecurity mission. We need to implement more effectively.

We have had a 10-year discussion within this country about roles and missions of DHS, of DOD, of the intelligence community, of law enforcement, how all of those entities can work together with the private sector and internally. And not re-litigating that and moving forward with being more effective on the operational environment under that broad policy construct would be essential.

So what we have seen in at least some of the publicly-available iterations of the draft Executive Order on cybersecurity I think has been a progression to get back under that framework, where the roles and responsibilities reflect continuity from the Bush administration, CNCI, Comprehensive National Cybersecurity Initiative, through the Obama administration policy, through the bipartisan legislation that this committee has led. So not re-fighting the turf battles and the roles and missions and getting to a point where we can execute in a way that is automated and efficient is where I would focus.

Mr. RATCLIFFE. Terrific, thanks very much.

Ms. Greene.

Ms. ROBYN GREENE. Thank you. I think the things that I would convey would be in terms of the guidance that DHS promulgated to implement CISA. I hope that this committee and the administration will continue to support DHS in that important work and not do anything to water down the protections or articulations of the definitions in the guidance.

As we know, privacy and security are inextricably intertwined. As Mr. Gillis pointed out, it is very important that information be actionable. I think that one of the things DHS did very well in promulgating this guidance is ensuring that companies focus on sharing actionable information. So supporting that effort will be critical.

Additionally, making sure that information is a two-way street, ensuring that DHS starts to do a better job of getting information to the private sector and doesn't just rely on information sharing be from private sector to the Government.

I would also agree with the need to increase resources and to ensure that agencies have the funding that they need to hire the best people and to update their systems, as I noted in my opening statement.

Finally, empowering DHS to work with Federal agencies to shore-up their systems. One of the things that had been contemplated in the Executive Order is bringing the Department of Defense more into that work. I think that would be a mistake.

Having civilian control over domestic cybersecurity was one of the main points of contention during the debate over CISA and, as Ryan just pointed out, has been settled. I think that we should start moving forward instead of moving back and re-litigating past debates.

Mr. RATCLIFFE. I thank you all. I think you gave some very thoughtful, helpful, and constructive answers. So I appreciate that.

The Chair now recognizes the Ranking Minority Member, Mr. Richmond, for his questions.

Mr. RICHMOND. Thank you, Mr. Chairman.

Ms. Greene, I will start actually where you were leaving off in terms of the guidance that DHS was able to issue. But I guess my question would be, are there privacy issues that DHS did not or could not rectify through guidance? If so, what were they?

Ms. ROBYN GREENE. Thank you, that is a really important question. So there were a few areas that DHS was not able to address through its guidance, primarily the over-broad law enforcement use authorizations and the potential for the President to establish a second authorized portal for information sharing.

I will elaborate on why the potential for a second portal is particularly concerning. First, having that second portal would decentralize the information-sharing process, which is anathema to the purpose of CISA. It would reduce situational awareness.

Second, it would create confusion as to the DHS's role as the civilian lead in the Federal Government in information sharing with the private sector.

It would also waste taxpayer dollars. It would result in bypassing the work and resources that have been put into standing up the NCCIC in order for them to develop the relationships that they have developed with the private-sector entities.

Finally, if the second portal was set up in a law enforcement agency or an intelligence oversight agency, like at the FBI or the director of national intelligence, it would undermine user trust, which is just essential for companies to feel comfortable engaging in the information-sharing program.

Mr. RICHMOND. Do you expect the administration to address any of that? Or what are you hearing?

Ms. ROBYN GREENE. I haven't heard anything with regard to how the administration will be approaching changing DHS's implementation of its guidance or sort-of reopening CISA to amend these problems. I would certainly encourage Congress to start thinking about whether it would be possible to amend CISA to address those concerns.

But most importantly, I hope that this committee will work to bolster DHS in its efforts to implement CISA in the manner that it is done, which is balancing privacy and security.

Mr. RICHMOND. Thank you.

I will ask this question to the panel since we have a whole bunch of experts here.

We hear a lot about whether DHS's automated indicator sharing is or isn't working. For instance, whether the data is timely, whether the volume of data is manageable and the cost of running the program.

So from your perspective, can you tell us what is fact and what is fiction in terms of the automated indicator sharing?

Mr. Nutkis, if you want to start.

Mr. NUTKIS. Sure. So having been involved in information sharing now for 5 years within the industry and now with Government, it is an iterative process. So ourselves in industry had a substantial problem in trying to collect IOCs. We went from 4 percent of the organizations contributing to 100 percent through the enhanced IOC program and accuracy. So we realize it is iterative.

Our experiences are quite positive. We had initial technical issues. We realized, by the way, that there aren't a substantial number of organizations that are sharing. But we have seen more and more that are sharing and we are getting better and better indicators back.

No question that it is not as effective as it could be. But based on where we were 5 years ago, they certainly have made a lot more progress in a short amount of time. So we actually have high hopes that if they can encourage other organizations to share, and that is really what it comes down to, you know, we see a ton of situational awareness across our sector, we would like to see more across the other sectors. We certainly would like to see more information disclosed from Government. But the progress we have seen is positive.

Mr. MONTGOMERY. I will give you both the good and the bad. I agree with Mr. Nutkis. What I think is good is that we are establishing the right kinds of muscle memory.

Ten years ago, 15 years ago, the idea of sharing an information security tidbit with a third party was anathema. I mean, it wasn't done. In fact, it was considered counterproductive. So I think we are establishing very, very good muscle memory. The sharing of IOCs among disparate third-party public and private organizations, that is good muscle memory.

On the downside, what is actually being shared and its usefulness and its timeliness, yes, we do need to improve. For example, if you were an auto mechanic and I handed you a bolt and said, OK, fix it, you wouldn't really understand where the bolt was from on the car or what kind of manufacturer it was from or whether it was a car or a truck. You would just understand that I had a problem. I think once we say, hey, this bolt fell off of my 1967 Fiat, now you are starting to understand the context that is required.

I believe the muscle memory and the sharing will get us toward those, but certainly we need some better guidelines about what constitutes good data coming in.

Mr. JEFFREY GREENE. I would echo what Mr. Montgomery said. I think probably one of the most significant wins is that we now have a formal process, we are not relying on just relationships.

We are right now in the midst of an analysis as to whether it makes sense for us to really jump in on AIS. One of the things we are looking at is how much work it takes to really make sense to figure out that the nut came from a Fiat once we get data back.

We are in a little different position just because of the volume of data that we get in through our own sensors. So there is, you know, a lot of information we have already obtained on our own, so there may be less unique data than other organizations.

But we have reviewed in the past and are now revisiting again to see if it has evolved to a place where it is useful to us. So we are looking at the questions that you asked, right now. But the most important thing, though, is we now have a formal process as opposed something that is purely relationship-based.

Mr. GILLIS. So on the operational side, I would echo all of these statements, which is that AIS has the right foundation. It needs to be sharing more particularly on the context side. If you look at the Cyber Threat Alliance, the way that we are now sharing is not just a quantity of indicators of compromise, you have to actually share with context. So what phase of the attack is this in? Is it intelligence and reconnaissance? Is it command-and-control? Is it linked to a known campaign?

With that broader context, if AIS can incorporate some of those technological best practices, it will be far more valuable in what it does.

On the programmatic side, this seems simple, but I have talked to DHS about this, so as a DHS alum I wanted to stick with this. There are some challenges to just on-boarding. They are short-staffed and there is not a real customer service focus to outreach to the private sector and bring even willing participants on in a timely and effective manner.

So they recognize that. It is something that is very much correctable, but it would go a long way as you go out to companies and try and build trust, because AIS is only going to be more effective with more parties involved. Making that process as easy as possible is an administrative thing that I think can add real operational value.

Mr. RICHMOND. Let me thank you.

Mr. Montgomery, you must be a golfer because you used "muscle memory" as opposed to just saying habit or something. But just thought I would point that out. Thanks.

Mr. RATCLIFFE. The gentleman yields back.

The Chair now recognizes the gentleman from Wisconsin, Mr. Gallagher. The Chair also welcomes him and Mr. Fitzpatrick and Mr. Garrett and Mrs. Demings to our subcommittee. We are glad to have you all.

With that, the gentleman is recognized.

Mr. GALLAGHER. Thank you, Mr. Chairman.

Mr. Montgomery and Mr. Greene, at the end of the second quarter of 2016, I believe Amazon and Microsoft, IBM and Google combined for about 55 percent of the global cloud infrastructure market share. What more could we be doing as a committee to ensure security of that vital cloud computing system? Is there any more attention we need to be paying to the actual physical security of these systems as we talk about securing sort of cyber space?

Just easy questions today.

[Laughter.]

Mr. MONTGOMERY. Boy, that is a big-boy-pants question.

[Laughter.]

Mr. GALLAGHER. The only kind of pants we wear on this committee.

[Laughter.]

Mr. MONTGOMERY. All right. So let us start with hardware and physical security because I think it is foundational, whether it is cloud or whether it is brick-and-mortar.

One of the things that we recognize across the technical folks on the committee is that if you don't have a good foundation, the pyramid gets top-heavy very, very quickly. So underlying chip-level, firmware-level security is essential in the trust model.

Because what you are doing when you go to a—now, when we do go to the cloud, you are basically renting a data center from somebody else. So the physical controls and the physical security and the chip-level security have to be sacrosanct.

Intel has long led with respect to this with a series of freeware tools that are available in order to test the efficacy and tamper-proof or tamper state of the firmware and chips that the commonly-used cloud providers utilize.

I think that one of the things that is challenging about cloud is that, just like any other technology, it is not a panacea. It is a useful tool for solving a series of problems. But one of the things that I think Government can do is help establish, what problem are you trying to solve? Are you trying to buy CPU cycles very cheaply? The cloud is the best way for doing that. Are you trying to have highly regulated or Classified or Sensitive data housed at the same security as brick-and-mortar, but have someplace else or somebody else do it? Your mileage may vary on costs. You will get there, but your costs will wind up being different.

So what can we do? Homeland's role here in terms of communication is essential. What do we mean by cloud? If I asked all of the committee Members or subcommittee Members, you would all have your own idea on what cloud means.

So putting some definitions around what we mean, what the best uses are, what Government should be doing or potentially not doing, where brick-and-mortar is appropriate versus cloud is a great start to helping to identify not only what should we doing at home in our own data closet, but also which third-party partner that you mentioned should we be going to and why. I think that is a great start.

Mr. JEFFREY GREENE. So I would start by cloud is a different domain, a different environment, but a lot of the same risks and threats. So let us not overthink in the sense that we have to come up with something brand new. I would apply the same thing to this internet of things which is growing. Let us not forget the lessons we have learned and act like we have to start from scratch.

So a lot of the same traditional cyber hygiene is going to apply. I think you also need to distinguish between whether we are talking about securing the actual cloud provider or securing the user of the cloud.

Then you get get down to risk-based decisions. If I am using the cloud to host my kid's Minecraft site, probably not a high-level security needed. If a power generation plant or some critical infrastructure is using the cloud for some capacity, much higher need for security there. In that case, you have to think about what is the obligation for both the cloud provider and the organization that chooses to use the cloud, which is a fine decision.

Here, I think the NIST framework comes in well, both for the cloud provider and the user. Use the risk-based calculations in the framework to figure out what you are doing right, what you are doing wrong, where your gaps are, how you improve them. So I would encourage you to think about it from both ends.

Mr. GALLAGHER. Great. Quickly, Mr. Gillis, in the 30 seconds we have, one of your co-founders is Israeli. Every day I hear about a new Israeli company in this space. What are we doing with them now? What can we learn from the Israelis who seem to be a leader in this space?

Mr. GILLIS. Sure. So there are certainly some lessons learned from Israel. It is obviously a very different dynamic and not just the neighborhood that they are in, but the mandatory service. So there is a lot of institutional knowledge as well as Israel as a government has done a lot both to attract American company investment and to ensure that those that they have within country that have expertise are supported from a venture capital perspective as they transition to the private sector.

I would also echo on the cloud side of things, too, you know, fundamentally, we talked earlier, you have got to protect your customers wherever their data resides and transits. So as Jeff has said, you need to move effective technology geared to the specific how of defending a cloud and evolve that into that new area.

But the principle remains the same, which is that you need to be secure, whether it is in a data center, whether it is at a terminal, or on a mobile device.

Mr. GALLAGHER. Thank you.

Thank you, Mr. Chairman.

Mr. RATCLIFFE. The Chair recognizes the gentlelady from Florida, Mrs. Demings.

Mrs. DEMINGS. Thank you. Thank you to our witnesses for being with us today.

Ms. Greene, as we continue to assess the impact of cyber intrusions and begin to make adjustments to cyber policies based on what we know about these intrusions, what must we keep in mind on the privacy and the civil liberties front to make sure we balance security with the privacy concerns?

Ms. ROBYN GREENE. Thank you. I think ensuring that we maintain a civilian lead within the Federal Government on cybersecurity is going to be absolutely essential as we move forward in this space.

Additionally, always remembering that the more we are protecting privacy, the more we are increasing security. Well-curated information is going to be one of the best tools that we have and security experts are in nearly unanimous agreement that that almost never includes information like communications content or personally identifiable information.

So as we move forward, ensuring that whatever new undertakings, you know, lay ahead and whatever changes to the guidance that may be made for CISA, we always keep privacy and minimizing unnecessary information sharing at the forefront.

Mrs. DEMINGS. Also for Ms. Greene, in President Obama's cybersecurity Executive Order, there was a designated role for the Privacy and Civil Liberties Oversight Board. Should this board have a designated role in future Executive Orders and legislation? How important is it to have a fully functioning Privacy and Civil Liberties Oversight Board?

Ms. ROBYN GREENE. So in previous iterations of information-sharing legislation, there had also been a role for the Privacy and Civil Liberties Oversight Board contemplated. OTI supported the inclusion of the PCLOB as an entity to oversee the implementation of information-sharing programs.

Whether it is expanded into the cybersecurity space or not, the Privacy and Civil Liberties Oversight Board plays an incredibly important role in Americans' privacy. It not only conducts oversight of counterterrorism activities for the Federal Government and their implications on privacy and civil liberties, it also serves as a sounding board for the intelligence community to ensure that they are doing things in the best way for privacy possible.

Oftentimes, the PCLOB will actually raise concerns or make suggestions about how the intelligence community can be improving privacy that they simply hadn't thought of yet. So they do play a critical role in bolstering Americans' privacy and civil liberties.

Mrs. DEMINGS. Thank you.

This next question is, for the sake of time, for any witness who feels it is more appropriate for them.

For a long time, the information-sharing conversation has been stuck on gathering data, either making it easier to participate or offering incentives to share.

It is time to start shifting our attention to focus on what we should do with the cyber threat data that we collect?

Mr. JEFFREY GREENE. Real quick, I think I am very pleased to hear the idea of shifting away from incentives, not that companies or organizations are going to turn them down. But at the highest policy level, I have always had a little discomfort with this notion that we need to give incentives for people to improve their cybersecurity. It is not something that we should have to incent people to do.

We need to get to a world where securing your data, whether your personal, your corporation, your pizza shop, is the same as locking your door. In college I worked at a bicycle store, and when I left at night no one had to incent me to lock the door so someone wouldn't steal my bikes. I think we need to get to a place in cybersecurity where the mind-set is that this is just a reality of doing business.

I do have some concern that a continuing discussion of incentives perpetuates this idea that cybersecurity is some extra that we need to encourage people to do as opposed to just the reality of the world we live in today.

Mr. NUTKIS. Just to give you a perspective from industry, so we use the terms "consumption" and "actionability." I think the problem is, is that we work with Fortune Six organizations and we work with two-doc practices. So when we are talking about the shift, we also have to shift the approach.

I think we have piloted and we have seen methods of high-tech, low-touch where, you know, we hear from the smaller organizations that they just don't have the resources, they don't have the appetite. They are trying to screen patients for Zika virus or other things and that is what they are going to worry about. They are not worrying about information security. They expect that that will be an automated process that the vendors are going to have to figure out how to automate that process.

So it is not a one-size-fits-all, but the consumption and actionability is clearly an issue we have to shift to.

Mrs. DEMINGS. Great, thank you so much.

Mr. RATCLIFFE. The Chair now recognizes the gentleman from Pennsylvania, Mr. Fitzpatrick.

Mr. FITZPATRICK. Thank you, Mr. Chairman.

Thank you to the Ranking Member as well.

Thank you to the panel for being here today on a really critical issue.

I have said many times, of all the threats we face as a country, I am not aware of a larger threat than that of cyber threats, both from a National security standpoint and an economic security standpoint.

When the law enforcement folks appear before us, I am going to ask them about their relationship with each other. Generally, the

FBI and DHS have concurrent jurisdiction on the Federal level over cybersecurity-related issues.

But the question I want to ask this panel, given that you are representing the private sector, is your relationship with law enforcement, with both organizations, because in order to advance the ball in this arena it is critically important from both sides, not just from the private sector, but from law enforcement that there be a solid relationship, that there be information sharing, that there be established protocols as far as reporting incidents.

I can tell you, coming from that profession, we relied heavily in all areas, but particularly in this area, on the private sector and sharing information with us as law enforcement officials, educating us.

What I would like to know from the members of the panel is, how has that relationship been with both agencies when it comes to sharing information about threats, digital fingerprints, and the like? What is working? What is not working? What can be improved in that area?

Mr. GILLIS. Sure. Let me give you a little bit of historical perspective as well here, because I can tell you from while I was in government when the U.S. Government first started responding to victim notifications, sometimes one company would call several different agencies. As ridiculous as this sounds, we have seen instances where each agency would show up with a different nondisclosure agreement, the company would sign each one of those and then the agencies couldn't share amongst each other.

Absurd as that is, we have come a long way in just the basics along those lines. I think you have seen much better collaboration amongst the Secret Service and FBI. I think they are working well together.

To give you a personal anecdote from the private sector side as well, we have talked a little bit before about raising the cost of an attack. So first, that starts with preventing attacks, to weed out unsophisticated actors and also to make sophisticated actors up their game in a way that makes it more easily attributable.

Law enforcement is going to be an important component of that. Right now because the noise is so prolific, it is hard to go after malicious actors because there are so many people in the space. If the technology can weed out some of the unsophisticated actors, it can allow law enforcement to go after those criminals in a way that they will be forced to come out in the open more. It will be easier to identify who is acting because they are going to have to develop, not just use freely available tools, but develop their own tools that will make it easier to identify those entities.

We as security companies will sometimes be able to identify as those campaigns are coming in, this is the infrastructure they are using. So when that case occurs, we contact FBI, Secret Service, and others as appropriate to help say this is the playbook that is being run against us and that can help inform investigations.

So they do have a very important role and it is something that we focus on from a private-sector side.

Mr. JEFFREY GREENE. Yes. I would echo that. I would say that direct to DHS, as I mentioned earlier. Just last week, we had 10 analysts in to talk about a specific threat that they are looking at, to share our research on. At any point in time, we are active with several active FBI investigations, providing information about criminal infrastructure, indicators of compromise.

Not just us, but industry in general has developed a fairly good relationship with the large actors out there. It is something we can certainly provide you more details on some of the cases that we and others have worked on.

Mr. MONTGOMERY. So I would say I would agree with respect to collaboration. For instance, nomoreransom.org is a not only National law enforcement collaboration, but also cross-vendor where we have actually harvested and returned keys to victims in conjunction with law enforcement investigations.

So I would say with respect to collaboration, there is a lot of progress, there is a lot of great partnership and cooperation.

There is one instance where I think we can make improvement and it is when there is a data classification around a Government event. I will give you a functional example, the Iranian incursion into Navy SQL servers.

Basically by classifying the event, what we are doing is restricting the number of people who can lend assistance and also allowing the adversary to operate with impunity where, if we can release this information sooner, we are actually affecting not only Government, but private-sector organizations that have the same, very, very common, to Ryan's point, very low-hanging fruit attack.

So whereas I think the collaboration is good, when there is a Government instance requiring data classification, we are classifying too quickly sometimes and not allowing that information to be propagated both in public and private sector.

Mr. NUTKIS. So just for a slightly different perspective. So we end up working between DHS and FBI on almost, I would say, a weekly basis between some event that is going on in the industry. It is sometimes hard to understand the roles. It certainly, I think, recently has been much more clarified between the Bureau and Secret Service.

The term that I can't stand hearing is active law enforcement investigation which shuts down the sharing. That is really, so they will reach out, they will ask for a whole bunch of stuff or we will share a whole bunch of stuff with them, and then everything stops.

From our perspective, since we already are aware of it because we were sharing it across multiple organizations, in fact we are not sure why they can't share back as we are trying to work the same incident as they are.

So again, we understand the obstacles they are under. You know, we found that certainly it is a great, you know, relationship, but their hands are tied. So we end up spinning a lot of cycles.

Also, the part that has, I think, become much more efficient is now they reach out to us. They used to reach out to a hundred organizations individually. They reach out to us and then we will reach out as an outreach effort, which certainly makes it much more efficient.

Mr. FITZPATRICK. What do you think the solution is regarding obviously their hands are tied as far as disclosing law enforcement sensitive information regarding an on-going investigation?

Mr. Montgomery, regarding the classification issue, what are suggested improvements on how to deal with that?

Mr. NUTKIS. Well, I am not sure I have an answer specifically because unfortunately we are not aware of what they are not sharing. But it appears that they don't have to—from our perspective, the effort that we are trying to put in place is cyber resilience. We are trying to defend the public sector from additional loss. So there has to be a happy medium here where they can provide us with enough information to defend the sector without compromising a law enforcement investigation.

But right now, I don't think they are going through the analysis. It is a binary. It is yes, there is a law enforcement investigation, stop, versus what do we need to give the sector to protect itself? I think that varies based on the significance of the investigation and the significance of the threat.

Mr. MONTGOMERY. I can't agree more with Mr. Nutkis. This knee-jerk to classify an issue, for instance, a SQL server on an Unclassified network, having an issue for which there is a 7-year-old patch, this doesn't feel like a National security issue, this feels like an overreaction to what has occurred on an Unclassified DOD network.

That information could have been useful to a broad swath of practitioners, both in the private and public sector. But the knee-jerk classification makes that impossible. So I would agree, the context around the event makes it easy to decide what should be disseminated quickly and what should not.

Mr. JEFFREY GREENE. Mr. Gillis made a great point before, that a lot of times the information that law enforcement holds or is looking at exists and that private sector has developed that on their own. So we may have evidence of the compromise or know what needs to be done and there is a way and times to push that out without any connection back potentially to the fact that there is law enforcement if Palo Alto holds it, if McAfee, Intel, or Symantec. There are creative solutions that we can work toward.

Mr. FITZPATRICK. I am over my time, but we really would like to work with you on that because that is something that is really important, and it is something I think we could work to fix.

So I yield back, Mr. Chairman.

Mr. RATCLIFFE. Last but not least, the Chair recognizes my friend from Rhode Island, the Chairman of the Congressional Cyber Caucus, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Thanks for holding this hearing.

I want to thank our panel of witnesses here today for your testimony and the work that you are doing to help protect our Nation in cyber space.

So I wanted to follow up and just talk a little bit more about the information-sharing issue and build on some of the questions that Mr. Richmond had asked earlier.

I just wanted to start with Mr. Montgomery and then the panel members can chime in as well.

But, Mr. Montgomery, I just have a couple of clarifications I would like to make from your written testimony, if you don't mind.

First, you state, today, AIS does not provide a means for enriching the information it shares and it simply shares minimal IOC information. So do you mean that AIS and the STIX and CybOX expressions used under the program are not able to convey meaningful, contextual information or that as a matter of practice the information being shared currently lacks the rich, holistic content?

You know, I want to figure out, is this a logistics and capabilities part of the protocols with AIS? Or is it the information that they are receiving isn't robust enough?

Mr. MONTGOMERY. Yes. Unfortunately, it is both. The ability to extract information from a generic individual IOC, like a domain name or a URL or a fingerprint of a file, unless the IOC is so damning and points to such a condition, typically it is simply one of the needles in a pile of needles.

So two things are required. One, a greater degree of context around how a particular IOC was collected, under what context. How was it received? How was it transmitted? From whom, to whom? When was it received? Was it received during the course of the normal 9–5 business cycle? Was it sent wildly out of band?

These are the kinds of pieces of information that a practitioner would require in order to try and sort out what to do next. The ability to provide those levels of context as part of AIS is both—it is a technical limitation that we can't do that today. It is also sort-of it is base-table stakes in terms of what a practitioner would do next.

So if we were to make recommendations on change, it would be around sort-of that practitioner knowledge that comes with an individual IOC because then it becomes a force multiplier.

Mr. LANGEVIN. OK, very good. Thank you.

So another question, again following up on Mr. Richmond's question, relates to the free rider problem that you describe with information sharing.

So I have been impressed with CTA's work to address this problem, particularly as it moves away from volume-based measures of input to quality-based ones. So in your testimony, you state that DHS declassifying more information will help address the issue of free rider.

While I certainly fully support quicker declassification of threat indicators, it mystifies me how this is going to incentivize the private sector to share with Government. Can you help clarify that for me?

The rest of the panel, I welcome any comments that you might have, how we can deal with free riders in the broader ecosystem.

Mr. MONTGOMERY. Sure. So with respect to this has been the long-standing issue with the private-sector sharing. As Mr. Nutkis pointed out, we feel like we give information and we don't get the same yield back.

A declassification process would allow the Government to determine, particularly as it relates to homeland and its critical infrastructure mission, what is the implication of a particular piece of information as it relates to the physical critical infrastructure before giving it back?

But if that vetting process included even a Classified effort among vendors who were, as Mr. Greene pointed out, we sit at a lot of interesting nexuses. If we are able to complement that effort, collaborate in even the declassification effort, we all have our cleared elements. In order to get to that point to say, look, although the Government has classified a particular piece of information, it is in the wild or it is in the dark web. The value is only allowing adversaries to operate with impunity.

This would allow people to get real yield back from the program on a more timely basis.

Mr. GILLIS. Sure. Let me add also on a sector-by-sector basis within industry. One of the real values of the Cyber Threat Alliance is that everybody in there is a security vendor, has sophisticated capabilities, and our customer base is across all sectors of industry.

So by sharing information, No. 1, we wanted to ensure that the barrier to entry wasn't just a pay-for-play, but that you had to contribute significant, actionable intelligence on a regular basis. The benefit of that is that all of our customer set is better protected.

If you looked at ISACs, so financial sector, energy sector, health sector, for example, the less that those ISACs have to do for plugging in individual indicators of compromise or stopping individual playbooks, if they can rely on the security vendors to do that, then you can have more participation within those industry verticals on things that are specific to their sector. So there is a real force multiplier across different sectors of industry by coupling the CTA with the role of the Government and the role of these different ISACs on a sector-by-sector basis.

Mr. NUTKIS. Yes, I would agree with that. Although this has been an issue that we have had to deal with. I am not sure if people realize the only organization that doesn't benefit from information sharing is the one who shared.

So as we have gone through this and we did our original analysis, we found that 4.1 percent of the organizations that were in our information-sharing center were actually contributing. Of that, they were contributing in a relatively abysmal way, 7 weeks between identification to sharing and things like that.

We then went to what we called enhanced, which you had to share within 5 minutes and it had to have the metadata and you had to share complete indicators. What we did is we delayed the participation or the sharing of those indicators by 14 days to anyone else. That was the only carrot we could find which was, if you wanted better indicators you had to share better indicators. That was really the incentive.

Actually, it worked. We were able to get a lot of organizations to step up to the table, by the way recognizing that, and I think this is also important, that there is an underlying element here that gets lost, which is a lot of the issues with sharing has to do with the maturity of the organization or their ability to share in the first place.

So even though we are sharing, we also have this other issue, if you are not mature enough to share, are you mature enough to consume. I know that gets lost on a lot of this and this hearing is on sharing, but we need to make sure as we share, again, as the technology vendors look to improve the infrastructure and the security technology, is how do we consume them.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Is it your intention, Mr. Chairman, to do a second round or are we just doing a first round?

Mr. RATCLIFFE. Yes. Unfortunately, just one round today.

Mr. LANGEVIN. OK. So I have some additional questions I would like to submit for the record and hopefully our witnesses can respond in writing.

Mr. RATCLIFFE. Terrific.

Mr. LANGEVIN. Thank you.

Mr. RATCLIFFE. Thank the gentleman.

The Chair now recognizes my colleague from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you for the courtesy of the Chair and the Ranking Member.

Thank all the witnesses today.

Let me just begin and thank you for what I have gleaned in this hearing. I appreciate maybe global responses if you could quickly give.

A bill that I introduced, H.R. 940, Securing Communications of Utilities from Terrorist Threats, and an aspect of it is to seek voluntary participation on ways that DHS can best defend against and recover from terrorist acts that have an impact on National security. It involves working with the private sector.

Then H.R. 935, Cybersecurity and Federal Workforce Enhancement, is to seek a more trained work force that will be working for the Federal Government.

In the course of my questions, maybe someone would answer the importance of obtaining skills to address our Nation's deficit in the number of workers that are so crucial.

I also look forward to introducing soon Prevent Zero-Day Events which would help DHS in working with sector-specific entities to better understand the detection of undiscovered or unreported vulnerabilities in software and firmware. That one in particular I would like to have a comment on as I ask the question.

So I want to ask a specific question that deals with, in the wake of the Russian cyber campaign against our electoral system, about there has been discussion about the importance of attribution. Panel, could you speak to why it matters, particularly as interest grows in exacting retribution? That is the question of attribution as to, how did it happen?

Also, we are now hearing without details of the potential release of a number of tactics that are being used by the CIA. Again, news reports speculate that this may have come from individuals with access who work for private contractors.

You are from the private sector. I would be interested in your vetting processes regarding individuals that have access to governmental, confidential security data and information.

I would also like to put on the record, Mr. Chairman, the request for a briefing. It may be this committee, it may be another subcommittee, any one, or the full committee. That I believe that we should receive a Classified briefing as to what actually was released that impacts negatively on the intelligence community regarding the representation that Wikileaks has released through information they received, some very viable and important data. I think that this is a key responsibility that we have.

So could you begin? Who will take questions?

Mr. GILLIS. I will start with securing utilities, where you began there. So that is an essential area that we as a Nation need to be concerned about. It is an area where we collectively need to work, again public/private.

Let me give you an example of one instance in which we have done so. So last fall, our security intelligence team identified new strands, new iterations of what is called the Shamoon attack. Shamoon attack is what was levied against Saudi Aramco, an oil producer within Saudi Arabia, that had destroyed 35,000 hard drives in 2012.

We noticed in late fall that there were new evolutions of some of that old infrastructure with new techniques being used. As we identified that, we called up Department of Homeland Security, ensured that they had a predecisional copy of that report, ensured that they were able to help protect U.S. Government networks against it, ensured that they were able to distribute that across the broader USG community, ensured that they were able to help develop their own critical infrastructure bulletin so that U.S. industry in the electric sector and other utilities were able to prevent against those types of attacks.

So that is a place where, if you look from a National security and economic security perspective, utilities are obviously key. It is essential to look at the intersection of physical and cybersecurity, as this committee does here and an example of something that we highly value and DHS has a tremendous role toward.

Ms. JACKSON LEE. Mr. Nutkis and Mr. Montgomery, can you answer the question about the issue of, how do you vet your individuals that work with Government data? What do you think about attribution?

Mr. NUTKIS. With regards to vetting, we follow the Government's requirements for vetting. So DHS has a formal process which requires for vetting of anyone who has access to Classified information. That is the process that we follow.

With regards to attribution, we, again, there is—from cyber resilience and defending, that is a different, you know, that is not as relevant for us down in the private sector.

We want to know what the threat is, how real the threat is, what to do about it. It is really about either anticipating the threat so that we can have a defense posture.

Although it has always been interesting and as we go to various briefings to understand where the threats are coming from and, again, it helps us protect our networks and protect the environment, specific attribution to the individual threat actor, it has always been interesting, but we have never really determined how best to use it and certainly use it on a wide scale at an industry level.

Ms. JACKSON LEE. Mr. Montgomery.

Mr. MONTGOMERY. With respect to people having access to Government data, we use the same DSS and OPM clearance processes as everybody else does. We do some stove-piping of Government data away from other systems in order to meet the physical and data security requirements.

With respect to attribution, I think attribution, it is a step that I think people are prioritizing more heavily at the wrong times. Asking about attribution first in the wake of a breach or of a successful attack is much akin to trying to decide what color carpet to put in your house while it is still on fire.

There is a point at which you should decide what color carpet to put in the house, but put the fire out first.

There are hygiene and security elements that are far more important to take care of, particularly as it relates to utility and critical infrastructure, long before sorting out which foreign national, which we may or may not ever get jurisdiction over, is ultimately responsible.

So while I think that attribution is an important step in the life cycle of an event, putting it first is what we seem to do as a society and as a technical society. It should be far, far further down the track so that the events can't occur again rather than figuring out who to blame.

Ms. JACKSON LEE. Does anyone else?

Mr. Chairman, you have been very gracious. I know that the answers refer to the private sector and do not, in respect to attribution and retribution, I appreciate Mr. Montgomery, do not reflect on the importance of our Government finding out who this should be attributed to. Therefore, we have the opportunity to deal with what our response will be.

Certainly, as the house is on fire, I would like to say, in concluding, I would like to get it before the house is on fire, I would like it not to happen. That is what I hope as Members of the Homeland Security Committee and this committee that we can work in that preventative mode. That would make us all safer and securer and make the work with our partners in the private sector a smoother pathway.

I yield back, Mr. Chairman.

I thank you, Mr. Montgomery.

Mr. RATCLIFFE. Thank the gentlelady for her remarks.

That concludes our hearing. I had high expectations, as I said at the outset, and from my perspective those expectations have been met for this hearing.

I think the testimony and the responses to questions that we have had from the witnesses have been particularly insightful and instructive, certainly to the committee, and hopefully to the new administration.

So I thank you all for your testimony, and I thank the Members for their thoughtful questions today.

The Members of the committee, at a minimum Mr. Langevin, perhaps others, will have additional questions for some of the witnesses. We will ask you to respond to those in writing.

Pursuant to committee rule VII(D), this hearing record will be held open for a period of 10 days.

Without objection, the subcommittee will stand adjourned.

[Whereupon, at 11:41 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE JAMES LANGEVIN FOR DANIEL NUTKIS

Question 1a. AIS was one of the central accomplishments of the Cybersecurity Act of 2015, and I believe that real-time, machine-to-machine sharing can make a real difference in protecting our networks. I have, however, been concerned by the lack of participation in AIS, particularly because in order to function, it needs to take advantage of the network effects of a robust pool of participants. Why do you think participation numbers are so low, particularly since we heard from the private sector repeatedly while working on the bill that this sort of initiative was urgently needed?

What specific measures could DHS take to encourage private-sector participation?

Question 1b. Does your organization/company participate in AIS?

If yes: (a) When did you join the program? (b) What were your initial set-up costs to do so? (c) What factors motivated your decision to join AIS?

If no: (a) Have you considered joining AIS? If so, what factors caused you to decline to participate? (b) What would need to change about the program to make it worthwhile to participate?

Answer. Response was not received at the time of publication.

Question 2. One of my goals this Congress is to get a better handle on cybersecurity metrics: Namely, are the actions we are taking having measureable improvements on our security? Based on your experience, how can we better measure cybersecurity outcomes?

Answer. Response was not received at the time of publication.

Question 3a. On December 29, 2016, the Department of Homeland Security released a Joint Analysis Report (JAR) regarding Russian malicious cyber activity designated as GRIZZLY STEPPE. Included in the JAR were indicators that were released in STIX and CSV formats.

How did your organization/company utilize the JAR?

Question 3b. Did you find the technical indicators of malicious Russian cyber activity useful? Why or why not?

Question 3c. What proportion of the technical indicators was your organization/company aware of before the release of the JAR?

Question 3d. Do you believe the JAR helped improve the Nation's cybersecurity?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE JAMES LANGEVIN FOR SCOTT MONTGOMERY

Question 1a. AIS was one of the central accomplishments of the Cybersecurity Act of 2015, and I believe that real-time, machine-to-machine sharing can make a real difference in protecting our networks. I have, however, been concerned by the lack of participation in AIS, particularly because in order to function, it needs to take advantage of the network effects of a robust pool of participants. Why do you think participation numbers are so low, particularly since we heard from the private sector repeatedly while working on the bill that this sort of initiative was urgently needed?

Answer. The limited level of private-sector participation in the AIS system has many causes. These include:

- Most organizations have an inherent hesitation or fear to share cyber threat information. There is a concern that sharing may expose internal corporate information unnecessarily. General counsels have found it easier to have policies that restrict sharing to all but the most trusted partners.
- The sign-up process for AIS is a bit onerous. The process could be made much easier and more streamlined to incent participation.
- Currently, AIS only shares indicators and mitigations. While these pieces of information are large components of the cyber threat life cycle, there is currently

no way to enrich data that an organization receives from AIS. In other words, if an organization finds additional data sets that can be used to enrich the data received from DHS, it has no way to share these data sets with the AIS community.

- The limited legal liability protection established in the legislation and implemented in regulation has been and continues to be confusing.

Question 1b. What specific measures could OHS take to encourage private-sector participation?

Answer.

- Provide general counsels with more information that shows the value of participating in AIS.
- Clarify liability protection.
- Improve the sign-up process to make it is easier to understand and implement.
- Provide an organization's IT/security staff with materials they can use "to sell" the effort to their management and general counsel.

Question 1c. Does your organization/company participate in AIS?

Answer. McAfee recently spun-out as a separate, stand-alone company. As such, we are currently developing new internal processes and procedures. Currently, we do not participate in the AIS program.

Question 1d. Have you considered joining AIS? If so, what factors caused you to decline to participate?

Answer. McAfee is still deciding whether to join AIS.

Question 1e. What would need to change about the program to make it worthwhile to participate?

Answer. The program would be much more valuable if there was a means to enrich the data provided. It is our understanding that AIS does not provide a unique set of indicators to the private sector. This means that multiple indicators could come from different submitters that, practically speaking, are the same. This puts the burden of data clean-up on every participating organization. It would be better for all if AIS did this data clean-up as part of their redistribution process.

Question 2. One of my goals this Congress is to get a better handle on cybersecurity metrics: Namely, are the actions we are taking having measurable improvements on our security. Based on your experience, how can we better measure cybersecurity outcomes?

Answer. It is very difficult to accurately measure progress in the cybersecurity domain. Scope and scale are the main challenges.

There are organizational risk management tools that can be used to track and depict organizational cyber program improvements, such as the NIST Cybersecurity Framework, but they are not appropriate when comparing one organization to another.

Because cybersecurity impacts so many parts of our digital world today, appropriate metrics need to be developed for each of the specific areas being examined. For instance, with an organizational baseline, it is not hard to measure how fast patches are deployed each month within a given organization. Macro-level measurements, on the other hand, are much more complex and difficult to develop. For example, how would you measure the impact of delaying procurement of new cybersecurity capabilities? The cybersecurity landscape is very much an arms race between the defenders and the malicious actors. If the process to acquire new capabilities takes two or more years, what effect does that have on an organization's defensive capabilities?

Given the many difficulties associated with metrics, it would be useful for NIST to create a metrics research effort. Such an activity should not be tied to the NIST Cybersecurity Framework, but should be a stand-alone effort that considers the scope and scale of the various needs for measurement. Organizational internal measurements, sector-specific comparison metrics, and consumer-, industry-, and National-level improvement tracking could all be areas of study. A research effort of this magnitude and complexity would require NIST to work in close collaboration with industry to produce a successful outcome.

Question 3a. On December 29, 2016, the Department of Homeland Security released a Joint Analysis Report (JAR) regarding Russian malicious cyber activity designated as GRIZZLY STEPPE. Included in the JAR were indicators that were released in STIX and CSV formats.

How did your organization/company utilize the JAR?

Question 3b. Did you find the technical indicators of malicious Russian cyber activity useful? Why or why not?

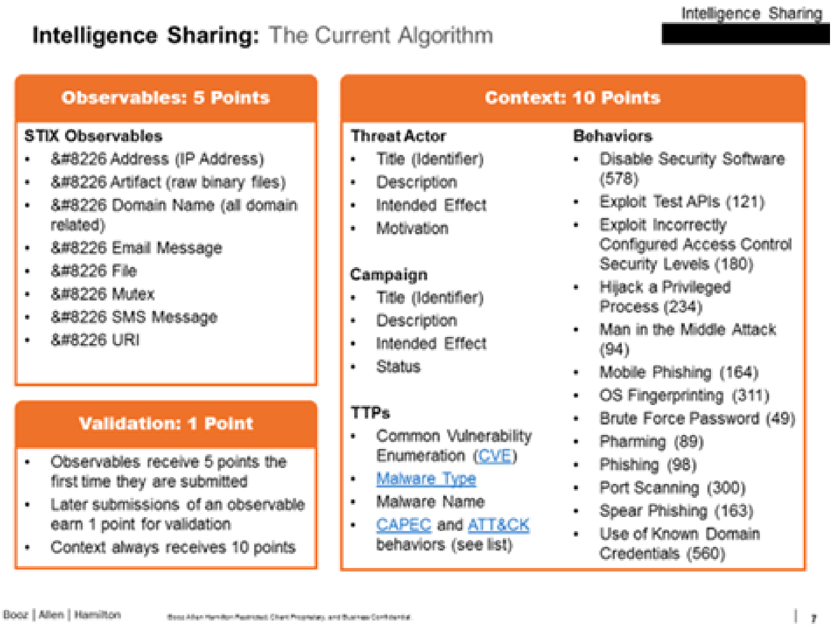
Question 3c. What proportion of the technical indicators was your organization/company aware of before the release of the JAR?

Question 3d. Do you believe the JAR helped improve the Nation's cybersecurity?

Answer. This event occurred prior to McAfee spinning-out from Intel and becoming an independent company. Since McAfee and Intel are two separate stand-alone companies, it would not be appropriate for McAfee to discuss Intel's use of the JAR. Intel's threat intelligence team should respond to this question.

Question 4a. Your company is involved in the Cyber Threat Alliance. What indicators does your company choose to share with CTA? By what process are they selected?

Answer. The slide below depicts the information shared between CTA members, which Members agreed to.



Intelligence Sharing

[redacted]

Intelligence Sharing: The Current Algorithm

Observables: 5 Points

STIX Observables

- &#8226 Address (IP Address)
- &#8226 Artifact (raw binary files)
- &#8226 Domain Name (all domain related)
- &#8226 Email Message
- &#8226 File
- &#8226 Mutex
- &#8226 SMS Message
- &#8226 URI

Validation: 1 Point

- Observables receive 5 points the first time they are submitted
- Later submissions of an observable earn 1 point for validation
- Context always receives 10 points

Context: 10 Points

Threat Actor

- Title (Identifier)
- Description
- Intended Effect
- Motivation

Campaign

- Title (Identifier)
- Description
- Intended Effect
- Status

TTPs

- Common Vulnerability Enumeration (CVE)
- Malware Type
- Malware Name
- CAPEC and ATT&CK behaviors (see list)

Behaviors

- Disable Security Software (578)
- Exploit Test APIs (121)
- Exploit Incorrectly Configured Access Control Security Levels (180)
- Hijack a Privileged Process (234)
- Man in the Middle Attack (94)
- Mobile Phishing (164)
- OS Fingerprinting (311)
- Brute Force Password (49)
- Pharming (89)
- Phishing (98)
- Port Scanning (300)
- Spear Phishing (163)
- Use of Known Domain Credentials (560)

Booz | Allen | Hamilton   Booz Allen Hamilton Restricted, Client Proprietary, and Business Confidential | 7

Question 4b. How does your company decide which indicators to share with the Government? To your knowledge, how does CTA decide which indicators (if any) to share with the Government?

What criteria/process is used to select indicators/threat intelligence to share with the Government?

What is the reason for not sharing more threat indicators with the Government?

Answer. The CTA does not currently allow direct Government membership. The Cyber Threat Alliance is a coalition of cybersecurity companies and is focused on expanding its private-sector membership. It should be noted, though, that the CTA has a history of sharing intelligence during events of National significance such as CryptoWall 3 and WannaCry with the appropriate Federal agencies. We expect to continue working with agencies on research/takedowns in those situations

Question 4c. What technical protocols does CTA use to share threat indicators?

Answer. The CTA members share information via STIX/TAXII.

Question 5. What suggestions do you have for DHS to enhance the Nation's cybersecurity workforce, in both the public and private sectors?

What actions can be taken by the Department acting alone, and what requires public/private collaboration?

Answer. DHS is an active participant in NSF's CyberCorps Scholarship for Service (SFS) program. DHS should support the expansion of this program.

The CyberCorps SFS program is designed to increase and strengthen the cadre of Federal information assurance specialists that protect Government systems and networks. Here's how it works: The National Science Foundation (NSF) provides grants to about 70 institutions across the country to offer scholarships to 10–12 full-time students. Students get free tuition for up to 2 years in addition to stipends—$22,500 for undergraduates and $34,000 for graduate students. They also get allowances for health insurance, textbooks, and professional development. Some universities also partner with DHS on these programs. Students generally have to be juniors or seniors and must qualify for the program by attaining a specific GPA, usually at least a 3.0 or higher. Upon completing their coursework and a required internship, students earn a degree, then go to work as security experts in a Government agency for at least the amount of time that they have been supported by the program. After that they can apply for jobs in the public or private sector.

With additional funding, the CyberCorps SFS program certainly could be expanded to more institutions and more students within each of those schools. To date, the Federal Government has made a solid commitment to supporting the SFS program, having spent $45 million in 2015, $50 million in 2016, and the most recent administration's budget requests $70 million. As a baseline, an investment of $40 million pays for roughly 1,560+ students to complete the scholarship program. Given the size and scale of the cyber skills deficit, policy makers should significantly increase the size of the program, possibly something in the range of $180 million. At this level of funding, the program could support roughly 6,400 scholarships. Such a level of investment would make a real dent in the Federal cyber skills deficit, estimated to be in the range of 10,000 per year. At the same time, this level of investment could help create a new generation of Federal cyber professionals that can serve as positive role models for a countless number of middle and high school students across the country to consider the benefits of a cyber career and Federal service. Indeed, this positive feedback loop of the SFS program might well be its biggest long-term contribution.

What should the private sector do to make an impact on the cyber skills deficit? The private sector must also be prepared to up-level its partnerships with the Government and others in industry to ensure a steady supply of worthwhile internships, co-ops, and training opportunities. In a recent report from McAfee and the Center for Strategic and International Studies (CSIS), a lack of quality training opportunities was cited as a significant reason why cyber practitioners seek alternative employment. For this reason, it is not only imperative that public-sector entities compensate their cyber professionals well, but also provide ample opportunities for employees to learn new skills and train on new technologies. With more robust public-private partnerships in this area, private companies in different industries can reach individuals at every stage in their career and engage them with new opportunities to learn about a wide variety of digital environments and next-generation technologies.

Questions From Honorable James Langevin for Jeffrey Greene

Question 1a. AIS was one of the central accomplishments of the Cybersecurity Act of 2015, and I believe that real-time, machine-to-machine sharing can make a real difference in protecting our networks. I have, however, been concerned by the lack of participation in AIS, particularly because in order to function, it needs to take advantage of the network effects of a robust pool of participants. Why do you think participation numbers are so low, particularly since we heard from the private sector repeatedly while working on the bill that this sort of initiative was urgently needed?

What specific measures could DHS take to encourage private-sector participation?

Question 1b. Does your organization/company participate in AIS?

If yes: (a) When did you join the program? (b) What were your initial set-up costs to do so? (c) What factors motivated your decision to join AIS?

If no: (a) Have you considered joining AIS? If so, what factors caused you to decline to participate? (b) What would need to change about the program to make it worthwhile to participate?

Answer. The roll-out of DHS's Automated Indicator Sharing (AIS) program was an important step in developing real-time information sharing. And while the program is still new, it shows great promise. Symantec is currently testing AIS to determine how the automated feed can contribute to our overall protection system and in the coming months will be conduct a pilot program to ingest some of the indicators and review them for accuracy and value.

The current participation rate in AIS no doubt reflects in part that it is still relatively new—it has only been functioning for less than 1 year. Some companies, especially smaller ones, are still establishing internal policies for sharing. Additionally, investing in the STIX/TAXI protocols could be a resource barrier for some smaller companies that might otherwise want to join. In larger companies, policy development can be a lengthy process as it typically includes input from operational, corporate, legal, and privacy functions. Last, while the fidelity of the indicators is improving, the quality in the early days was inconsistent and some would have caused false positives had they been fully deployed within a company or across a security vendor's customer base.

As a security vendor, Symantec is in a different position from many potential program partner. We are concerned with much more than our own systems; rather, we have to assess the impact on millions of customers around the world who rely on our near-real-time security updates. Each indicator of compromise needs to be carefully vetted to ensure we are pushing out quality indicators with a minimum of false positives. This vetting requires context, which at times has been insufficient. We recognize that DHS is in a difficult spot—industry is asking for both timely and rigorously-vetted information and this balance can be difficult to strike. DHS has made strides in the year AIS has been operational, and we hope that will continue.

Question 2. One of my goals this Congress is to get a better handle on cybersecurity metrics: Namely, are the actions we are taking having measureable improvements on our security? Based on your experience, how can we better measure cybersecurity outcomes?

Answer. Cybersecurity metrics is certainly a hotly-debated topic. At core, measuring success is often proving the negative—pointing to attacks that did not occur or did not succeed. Moreover, how do you show what might have happened if you do not have appropriate tools and procedures in place? One approach is to focus on cyber hygiene basics that provide a foundation for an effective cyber defense posture. These are relatively easy to measure and include activities such as:

- *Hardware and Software Asset Management*.—Identifying all hardware and software assets; it is often said that "you can't protect what you can't see."
- *Configuration Management*.—Properly configuring assets to eliminate known threat vectors.
- *Vulnerability Management*.—Scanning assets for known vulnerabilities and applying the appropriate patches.
- *Identity Credential and Access Management*.—Checking user privileges to ensure they are limited to only the rights they need and limiting any excessive privileges found.
- *Multi-Factor Authentication (MFA)*.—Implementing MFA and enforcing its use.

Consistent progress on these basic—but critical—foundational activities will lead to a reduction of some of the most commonly exploited cyber threat vectors.

Question 3a. On December 29, 2016, the Department of Homeland Security released a Joint Analysis Report (JAR) regarding Russian malicious cyber activity designated as GRIZZLY STEPPE. Included in the JAR were indicators that were released in STIX and CSV formats.

How did your organization/company utilize the JAR?

Question 3b. Did you find the technical indicators of malicious Russian cyber activity useful? Why or why not?

Question 3c. What proportion of the technical indicators was your organization/company aware of before the release of the JAR?

Question 3d. Do you believe the JAR helped improve the Nation's cybersecurity?

Answer. We received the December 29, 2016 Joint Analysis Report (JAR) regarding Russian malicious cyber activity designated GRIZZLY STEPPE and reviewed the indicators to ensure that our customers were properly protected. While most DHS reports include substantive analysis and some actionable information, on this occasion we believe the report fell short. Unfortunately, the indicators led to a high volume of false positives and in some cases the indicators proved to be unrelated to the threat itself. Finally, we were already aware of all indicators provided and those that we were not aware of were unrelated to the threat. However, to its credit, DHS issued an updated report that was higher in quality in terms of analysis and accuracy of indicators.

Question 4a. Your company is involved in the Cyber Threat Alliance.

What indicators does your company chose to share with CTA? By what process are they selected?

Question 4b. How does your company decide which indicators to share with the Government? To your knowledge, how does CTA decide which indicators (if any) to share with the Government?

- What criteria/process is used to select indicators/threat intelligence to share with the Government?
- What is the reason for not sharing more threat indicators with the Government?

Question 4c. What technical protocols does CTA use to share threat indicators?

Answer. The Cyber Threat Alliance (CTA) is an excellent example of the private sector banding together to improve the overall safety and security of the internet. In 2014, Symantec, Fortinet, Intel Security, and Palo Alto Networks formed the CTA to work together to share threat information. The goal was to distribute detailed information about advanced attacks and thereby raise the situational awareness of CTA members and improve overall protection for our customers.

Prior industry-sharing efforts were often limited to the exchange of malware samples, and the CTA sought to change that. Over the past 3 years the CTA has consistently shared more actionable threat intelligence such as information on "zero day" vulnerabilities, command-and-control server information, mobile threats, and indicators of compromise related to advanced threats. By raising the industry's collective intelligence through these new data exchanges, CTA members have delivered greater security for individual customers and organizations. In short, the CTA is not about one vendor trying to gain advantage—we are all contributing and sharing with the community.

Each member must share at least 1,000 samples of new Portable Executable (PE) malware per day that are not observed on VirusTotal over the preceding 48 hours at the time of sharing, and meet at least one of the following three criteria:

- *Mobile Malware.*—At least 50 samples of new mobile malware per day in the APK, DEX, or other popular mobile malware file formats that are not observed on VirusTotal over the last 48 hours at time of sharing.
- *Botnets C2 Servers.*—At least 100 botnet command-and-control servers (C2), and/or peer-to-peer nodes, per week beyond those listed on public forums such as ZeusTracker, must be different than the previous week's dump from the contributing member; and must be active upon sharing.
- *Vulnerabilities & Exploits Sites.*—At least 100 attack sites per week beyond those listed on public forums, must be different than the previous week's dump from the contributing member, and must be active upon sharing.

CTA is also committed to initiatives such as developing industry best practices that will improve cybersecurity for individuals and governments. As CTA moves forward with its mission, Government partnerships will be an important piece of the process.

Question 5a. What suggestions do you have for DHS to enhance the Nation's cybersecurity workforce, in both the public and private sectors?

Question 5b. What actions can be taken by the Department acting alone, and what requires public-private collaboration?

Answer. Today, there are an estimated 1 million cybersecurity jobs in the United States that supposedly cannot be filled. We believe that a new approach to IT professionals generally will help solve this problem. There are many general IT professionals in both Government agencies and in businesses around the world, and with in-house training they could become specialized security professionals. Their roles could in turn be filled by junior IT professionals or even recent graduates. Looking to existing IT staff to train for security roles has several benefits—these personnel will already know an organizations' systems, and providing another opportunity for career growth will improve retention and job satisfaction. Training the current IT workforce in cybersecurity is also fiscally smart, as it allows governments and enterprises to cut down their contract workforce and train from within, leading to a more secure IT environment.

We do this at Symantec, in part by conducting an annual "Cyber War Games" exercise. This exercise takes IT professionals from 10 regions around the world and creates scenarios to encourage innovative thinking and growth in cybersecurity skills. These types of activities allow us to find hidden expertise in current employees as well as new expertise to bolster our own workforce. In addition, Symantec created the Symantec Career Connection (SC3). SC3 is an innovative program designed to help close the cybersecurity workforce gap while creating meaningful career paths for underrepresented young adult and veterans. Through targeted classroom education combined with hands-on training, SC3 graduates are working amongst many of the world's largest and reputable companies.

Thank you again for the opportunity to testify and to provide these further responses.

QUESTIONS FROM HONORABLE JAMES LANGEVIN FOR RYAN M. GILLIS

Question 1a. AIS was one of the central accomplishments of the Cybersecurity Act of 2015, and I believe that real-time, machine-to-machine sharing can make a real difference in protecting our networks. I have, however, been concerned by the lack of participation in AIS, particularly because in order to function, it needs to take advantage of the network effects of a robust pool of participants. Why do you think participation numbers are so low, particularly since we heard from the private sector repeatedly while working on the bill that this sort of initiative was urgently needed?

What specific measures could DHS take to encourage private-sector participation?

Question 1b. Does your organization/company participate in AIS?

If yes: (a) When did you join the program? (b) What were your initial set-up costs to do so? (c) What factors motivated your decision to join AIS?

If no: (a) Have you considered joining AIS? If so, what factors caused you to decline to participate? (b) What would need to change about the program to make it worthwhile to participate?

Answer. Response was not received at the time of publication.

Question 2. One of my goals this Congress is to get a better handle on cybersecurity metrics: Namely, are the actions we are taking having measureable improvements on our security? Based on your experience, how can we better measure cybersecurity outcomes?

Answer. Response was not received at the time of publication.

Question 3a. On December 29, 2016, the Department of Homeland Security released a Joint Analysis Report (JAR) regarding Russian malicious cyber activity designated as GRIZZLY STEPPE. Included in the JAR were indicators that were released in STIX and CSV formats.

How did your organization/company utilize the JAR?

Question 3b. Did you find the technical indicators of malicious Russian cyber activity useful? Why or why not?

Question 3c. What proportion of the technical indicators was your organization/company aware of before the release of the JAR?

Question 3d. Do you believe the JAR helped improve the Nation's cybersecurity?

Answer. Response was not received at the time of publication.

Question 4a. Your company is involved in the Cyber Threat Alliance.

What indicators does your company chose to share with CTA? By what process are they selected?

Question 4b. How does your company decide which indicators to share with the Government? To your knowledge, how does CTA decide which indicators (if any) to share with the Government?

- What criteria/process is used to select indicators/threat intelligence to share with the Government?
- What is the reason for not sharing more threat indicators with the Government?

Question 4c. What technical protocols does CTA use to share threat indicators?

Answer. Response was not received at the time of publication.

Question 5a. What suggestions do you have for DHS to enhance the Nation's cybersecurity workforce, in both the public and private sectors?

Question 5b. What actions can be taken by the Department acting alone, and what requires public-private collaboration?

Answer. Response was not received at the time of publication.

Questions From Honorable Cedric Richmond for Robyn Greene

Question. Your organization, the Open Technology Institute, has taken a relatively hard line on two issues that are central to the current cybersecurity threat landscape—first, on the dangers of active cyber defense (i.e. allowing companies to "hack back"); and second, that the Government should adopt a more transparent, Congressionally-authorized process for when to disclose zero-day vulnerabilities in its possession. What are some of the key considerations policy makers should bear in mind on these issues?

Answer. New America's Open Technology Institute (OTI) opposes proposals to authorize active cyber defense (also known as "hacking-back") because they threaten to undermine cybersecurity rather than enhance it, and may result in harming innocent third parties. Hacking-back is a form of digital vigilantism. As vigilantism is illegal in the physical world, so too should it remain on-line. As Congress carefully weighs the risks and rewards that may result from hack-back proposals, it will likely find that the risks are unjustifiably high.

Hacking is dangerous whether you are a victim reacting to a cyber attack, a malicious actor, or a Government. Authorizing cyber attack victims to hack-back will almost certainly result in harms to innocent third parties. It is possible that a malicious actor could obtain malware used in a hack-back and turn it against innocent third parties. Further, attribution of the attack, though constantly improving, is still exceedingly difficult. When deploying an active cyber defense, it is difficult to guarantee that the device or network affected does not belong to an unrelated third party who has been misidentified as the malicious actor. Additionally, the hack-back could target a perceived malicious actor who is actually a person or entity that has been the victim of a cyber attack themselves, like a hospital or fire department whose network has been taken over by a botnet.

Finally, even if an attack has been successfully attributed to a particular malicious actor, identifying that attacker can still be difficult and time-consuming. Because of the rapid-response nature of hacking-back, it is possible that an entity will be retaliating against foreign actors, including nation-states. This could put entities that choose to engage in hacking-back in a conflict of law with the country where their target is located. It could also raise diplomatic concerns. For example, if hacking-back was legal in 2014, Sony could have chosen to retaliate against its attackers who turned out to be agents of the North Korean government, a hostile foreign power, instead of seeking assistance from law enforcement.

FBI Director Comey raised similar concerns at two speaking engagements this year. He was unequivocal in his opposition to allowing victims to hack-back. He cautioned that such an authorization was dangerous, and that it would interfere with the FBI's ability to conduct its investigations into cyber crimes.[1] OTI agrees with this assessment and would urge Members of Congress to oppose any proposal that legalizes hacking-back.

Unlike hacking-back, establishing a permanent process for disclosing previously unknown vulnerabilities (often called zero-days) in the Government's possession is essential to improving cybersecurity. As we have seen from the Shadow Brokers disclosures,[2] the arrest of an NSA contractor for hoarding zero-days at his home,[3] and the recent CIA leaks,[4] secrets get out. There is no way to guarantee that when the Government is in possession of zero-days and related exploits, that information will not eventually be leaked, posing significant and immediate risks of exploitation to Americans and internet users everywhere.

When the Government discovers or purchases vulnerabilities that put American internet users and companies at risk, it should disclose them as soon as possible so they may be patched. To ensure this happens, Congress should codify a interagency review and disclosure process. Any such process should be mandatory, such that no matter how the Government comes into possession of a zero-day vulnerability, it must submit it for review so that disclosure to the developer can be made in a timely manner.

The review of vulnerabilities should be undertaken with a presumption in favor of disclosure, and a requirement for recurring review of any vulnerability that is not disclosed. The reviews should be conducted by a set group of stakeholders representing the prevailing interests in favor of and opposing disclosure. Those stakeholders should represent the equities of the U.S. economy, including the digital economy; domestic cybersecurity and critical infrastructure owners and operators; the intelligence community; and the civil rights and civil liberties communities.

Finally, the process should include robust transparency mechanisms. The vulnerability review and disclosure process should be transparent about the points of inquiry it considers when making its assessments, and what agencies participate in the reviews. Congress should also require the review board to publish annual public reports that assess the efficacy of the process, and provide related metrics, such as the number of zero-days submitted for review, and the percentage of those zero-days that were disclosed to developers.

Questions From Honorable James Langevin for Robyn Greene

Question 1a. AIS was one of the central accomplishments of the Cybersecurity Act of 2015, and I believe that real-time, machine-to-machine sharing can make a real difference in protecting our networks. I have, however, been concerned by the lack of participation in AIS, particularly because in order to function, it needs to take advantage of the network effects of a robust pool of participants. Why do you think

[1] See James Comey, Dir. Fed. Bureau of Investigation, Speech at Boston Cybersecurity Summit 2017 (Mar. 8, 2017), *https://www.youtube.com/watch?v=VzhVYv7K4qc;* and James Comey, Dir. Fed. Bureau of Investigation, Speech at U. of Tex. Austin (Mar. 23, 2017), *https://www.youtube.com/watch?v=iR5EwIbUvA0.*

[2] See David E. Sanger, *"Shadow Brokers" Leak Raises Alarming Question: Was the NSA Hacked?,* NY Times (Aug. 16, 2016), *https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html;* Bruce Schneier, *Another Shadow Brokers Leak,* Schneier on Security (Nov. 1, 2016), *https://www.schneier.com/blog/archives/2016/11/another__shadow__.html;* and *Don't Forget Your Base,* Medium (Apr. 8, 2017), *https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1.*

[3] Ellen Nakashima, Matt Zapotosky, & John Woodrow Cox, *NSA Contractor Charged with Stealing Top Secret Data,* Wash. Post (Oct. 5, 2016), *https://www.washingtonpost.com/world/national-security/government-contractor-arrested-for-stealing-top-secret-data/2016/10/05/99eeb62a-8b19-11e6-875e-2c1bfe943b66__story.html.*

[4] Scott Shane, Matthew Rosenberg, & Andrew W. Lehren, *Wikileaks Releases Trove of Alleged C.I.A. Hacking Documents,* NY Times (Mar. 7, 2017), *https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.*

participation numbers are so low, particularly since we heard from the private sector repeatedly while working on the bill that this sort of initiative was urgently needed?

What specific measures could DHS take to encourage private-sector participation?

Question 1b. Does your organization/company participate in AIS?

If yes: (a) When did you join the program? (b) What were your initial set-up costs to do so? (c) What factors motivated your decision to join AIS?

If no: (a) Have you considered joining AIS? If so, what factors caused you to decline to participate? (b) What would need to change about the program to make it worthwhile to participate?

Answer. Though New America does not currently participate in the Department of Homeland Security's Automated Information Sharing (AIS) program, one of the concerns that we raised as CISA was being debated was that it would not address the need for two-way information sharing. Security experts and witnesses at the March 9, 2017 hearing were clear that for information sharing to be effective, the Government must be willing and able to increase its declassification and sharing of unique cyber threat indicators in a timely and actionable manner.[5]

Rather than focusing on persuading more companies and Information Sharing and Analysis Organizations and Centers to join AIS, DHS should focus on showing these entities why joining AIS would be beneficial by increasing information sharing by the Government to the private sector. DHS should also endeavor to be transparent about how much information it shares with the private sector, and what the quality of that sharing has been.

Additionally, many technology companies voiced opposition to CISA just before its passage citing to concerns, shared by the privacy community, about the civil liberties of their users.[6] Companies may feel more comfortable participating in information sharing under CISA if Congress amended the law to address those concerns. Specifically, Congress could amend CISA to strengthen the requirement to remove personal or identifiable information before sharing by clarifying that such information is not directly related to a cyber threat unless it is necessary to "detect, prevent, or mitigate" it.[7]

Congress should also consider amending CISA to narrow the law enforcement use authorizations so that information shared can only be used for cybersecurity purposes and investigations into related computer crimes. Finally, Congress can resolve the privacy community and technology industry's concerns by removing the authorization for the President to designate a second authorized information-sharing portal.

Question 2. One of my goals this Congress is to get a better handle on cybersecurity metrics: Namely, are the actions we are taking having measureable improvements on our security? Based on your experience, how can we better measure cybersecurity outcomes?

Answer. The annual Verizon Data Breach Investigations Report is one of the best-available resources for measuring the effectiveness of our actions to improve cybersecurity. The report provides a good 60,000-foot view of the state of cybersecurity threats and response. It can also help to provide guideposts for where to focus resources to yield the most improvement.

For example, year after year, these reports make clear that the vast majority of cyber threats target previously known vulnerabilities, so Americans fall victim to data breaches simply because they have failed to maintain updated software.

[5] "While DHS has made progress, it still needs to improve the quality and the quantity of the threat data it shares with the private sector to address this issue of the free rider. DHS should thus declassify larger categories of threat data and actively share them with the private sector. DHS should issue many more security clearances to qualified company representatives to enable access to the most sensitive, and potentially most valuable, pieces or classes of threat data." Current State of DHS Private Sector Engagement for Cybersecurity: Hearing Before the H. Homeland Sec. Subcomm. on Cybersecurity and Infrastructure Protection, 115th Cong. 7 (2017) (Written statement of Scott Montgomery, V. President and Chief Technical Analyst, Intel Security Group), *http://docs.house.gov/meetings/HM/HM08/20170309/105671/HHRG-115-HM08-Bio-MontgomeryS-20170309.pdf.* See also Sara Sorcher, *Security Pros: Cyberthreat Info-sharing Won't Be as Effective as Congress Thinks,* Christian Sci. Monitor, Jun. 12, 2015, *http://www.csmonitor.com/World/Passcode/2015/0612/Security-pros-Cyberthreat-info-sharing-won-t-be-as-effective-as-Congress-thinks.*

[6] Robyn Greene, *Tech Industry Leaders Oppose CISA as Dangerous to Privacy and Security,* The Hill, Oct. 21, 2015, *http://thehill.com/blogs/pundits-blog/technology/257601-tech-industry-leaders-oppose-cisa-as-dangerous-to-privacy-and.*

[7] Dep't of Homeland Security & Dep't of Justice, *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measure with Federal Entities under the Cybersecurity Information Sharing Act of 2015* 5, *https://www.us-cert.gov/sites/default/files/ais__files/Non-Federal__Entity__Sharing__Guidance__(Sec%20105(a)).pdf.*

Verizon's 2016 report concluded that 85 percent of successful exploits used the same 10 vulnerabilities, all of which have patches available.[8] This marks an improvement over the previous year, where Verizon found that "99 percent of the exploited vulnerabilities were compromised more than a year after the CVE was published," and 97 percent of those exploits targeted just 10 vulnerabilities.[9]

Thus, the reports show that one of the most meaningful ways to enhance cybersecurity would be to reduce the frequency of successful attacks that were preventable. Despite the improvements that are being made, Congress should place greater focus on identifying policy solutions that will encourage more and more regular vulnerability patching. Additionally, Congress should identify ways to incentivize companies to incorporate privacy by design as they build their products and services, such as by providing automatic security updates.

Though Verizon's annual report, and similar reports from other companies are helpful, they do not provide the granular data that may be necessary to respond to more advanced threats or to identify certain trends. For this, improving metrics is key. DHS is currently collaborating with the insurance industry through the Cyber Incident Data and Analysis Working Group to try to establish a repository for sharing of current and historical non-personally identifiable cyber incident data.

The goal of the repository would be to create a data-rich resource that can be analyzed to "promote greater understanding about the financial and operational impacts of cyber events, the effectiveness of existing cyber risk controls in addressing them, and the new kinds of products and services that cybersecurity solutions providers should develop to meet the evolving risk mitigation needs of their customers."[10] Thus, if effective, the repository would yield new metrics that can be used to improve risk mitigation strategies, and may also positively impact the cybersecurity insurance market. Congress should follow the progress of this working group to determine if such a repository is an effective way to obtain more and more actionable metrics on the effectiveness of our cybersecurity strategy.

Question 3a. On December 29, 2016, the Department of Homeland Security released a Joint Analysis Report (JAR) regarding Russian malicious cyber activity designated as GRIZZLY STEPPE. Included in the JAR were indicators that were released in STIX and CSV formats.

How did your organization/company utilize the JAR?

Question 3b. Did you find the technical indicators of malicious Russian cyber activity useful? Why or why not?

Question 3c. What proportion of the technical indicators was your organization/company aware of before the release of the JAR?

Question 3d. Do you believe the JAR helped improve the Nation's cybersecurity?

Answer. New America did not utilize the Joint Analysis Report (JAR) regarding Russian malicious cyber activity designated as GRIZZLY STEPPE.

[8] Verizon, *2016 Data Breach Investigations Report: Executive Summary* 10 (2016), *http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf.* Full Report available at *http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/*.

[9] Verizon, *2015 Data Breach Investigations Report 15–16* (2015), *https://msisac.cisecurity.org/whitepaper/documents/1.pdf.*

[10] Dep't of Homeland Sec., *Enhancing Resilience Through Cyber Incident Data Sharing and Analysis: The Value Proposition for a Cyber Incident Data Repository* 2 (2015), *https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf.* For more resources on the CIDAWG, see Cyber Incident Data and Analysis Working Group White Papers, Dep't of Homeland Sec, *https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers* (last accessed Apr. 13, 2017).