S. HRG. 115–756

# COMPLEX CYBERSECURITY VULNERABILITIES: LESSONS LEARNED FROM SPECTRE AND MELTDOWN

## HEARING

BEFORE THE

## COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 11, 2018

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
55–216 PDF WASHINGTON : 2024

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JOHN THUNE, South Dakota, *Chairman*

| | |
|---|---|
| ROGER WICKER, Mississippi | BILL NELSON, Florida, *Ranking* |
| ROY BLUNT, Missouri | MARIA CANTWELL, Washington |
| TED CRUZ, Texas | AMY KLOBUCHAR, Minnesota |
| DEB FISCHER, Nebraska | RICHARD BLUMENTHAL, Connecticut |
| JERRY MORAN, Kansas | BRIAN SCHATZ, Hawaii |
| DAN SULLIVAN, Alaska | EDWARD MARKEY, Massachusetts |
| DEAN HELLER, Nevada | TOM UDALL, New Mexico |
| JAMES INHOFE, Oklahoma | GARY PETERS, Michigan |
| MIKE LEE, Utah | TAMMY BALDWIN, Wisconsin |
| RON JOHNSON, Wisconsin | TAMMY DUCKWORTH, Illinois |
| SHELLEY MOORE CAPITO, West Virginia | MAGGIE HASSAN, New Hampshire |
| CORY GARDNER, Colorado | CATHERINE CORTEZ MASTO, Nevada |
| TODD YOUNG, Indiana | JON TESTER, Montana |

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
JASON VAN BEEK, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

# CONTENTS



WITNESSES



APPENDIX

# COMPLEX CYBERSECURITY VULNERABILITIES: LESSONS LEARNED FROM SPECTRE AND MELTDOWN

**WEDNESDAY, JULY 11, 2018**

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:05 a.m. in room SR–253, Russell Senate Office Building, Hon. John Thune, Chairman of the Committee, presiding.

Present: Senators Thune [presiding], Wicker, Fischer, Moran, Sullivan, Inhofe, Capito, Gardner, Young, Nelson, Cantwell, Blumenthal, Peters, Markey, Udall, Baldwin, Hassan, Cortez Masto, and Tester.

## OPENING STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

The CHAIRMAN. Good morning.

We know that cyber criminals and rogue states aim to steal vast amounts of personal and proprietary information and access our critical infrastructure networks.

Cybersecurity vulnerabilities found in computer hardware like the creatively named Spectre and Meltdown vulnerabilities present new pathways for bad actors to cause significant damage and exemplify the ever-changing landscape of cybersecurity risks that we face.

Fortunately, these hardware vulnerabilities were discovered by the good guys, the White Hat security researchers.

Of critical importance, however, these vulnerabilities, which existed unnoticed for decades, have an unprecedented scope and required a coordinated response across the chip manufacturers like Arm and AMD and Intel and the entire tech industry.

In February, Senator Nelson and I sent letters to 12 companies to discuss the steps taken in response to these vulnerabilities. We asked questions about the level of coordination with other companies and with the U.S. Government, efforts to patch the vulnerabilities, and recommendations for future steps to reduce risks stemming from hardware vulnerabilities.

Our oversight identified several issues.

First, although security researchers initially informed certain companies of the vulnerabilities in June 2017, the vulnerabilities were not widely disclosed until January 2018 in order to allow time

to remediate the vulnerabilities. Afterwards, other related vulnerabilities continued to be disclosed.

These processes raise questions about how a coordinated vulnerability disclosure process should be carried out to ensure that companies have enough time to test and implement patches. It is not enough just to develop patches. They also need to be tested and applied so that consumers do not have a false sense of security about whether solutions are really in place.

The other thing we confirmed is that some Chinese manufacturers, including Huawei, were informed of the vulnerability prior to public disclosure. Given their close ties to the Chinese Government, Huawei's involvement in the coordinated vulnerability disclosure, while perhaps necessary, raises additional questions about supply chain cybersecurity.

Finally, only one company, IBM, reported that it contacted the U.S. Government prior to the January 3, 2018 public disclosure. And no vendor engaged CERT-CC to assist in coordinating the vulnerability disclosure or response. Even the largest affected chip manufacturer, Intel, did not provide advance notice.

Some companies, including Intel, explained that notice to the U.S. Government was supposed to occur prior to public disclosure but these plans were frustrated by a premature leak. Nevertheless, this is truly disappointing since greater coordination earlier in the process would have reduced confusion and provided enhanced security. After additional conversations with this Committee, when newer variants were discovered, a few of the companies did provide significant notice, some up to 1 month, in advance of public disclosure.

The U.S. Government is responsible for the protection of Federal IT and critical infrastructure. It is also a significant customer in the supply chain.

Overall, this hearing is a reminder of the importance of public-private partnerships in cybersecurity. Cybersecurity standards should be industry-led and remain voluntary, but the cybersecurity risks that threaten our nation are too great to be handled solely by the government or by industry.

That is why this Committee has prioritized fostering public-private partnerships in cybersecurity risk management. We have enacted laws like the Cybersecurity Enhancement Act to provide for the development of the NIST Framework for Critical Infrastructure. Similarly, the Cybersecurity Information Sharing Act sought to incentivize greater cyber information sharing, and the Cybersecurity Scholarship Opportunities Act increased the government's role in workforce development.

We are also working to enact legislation to strengthen cybersecurity for self-driving vehicles, aircraft, and small businesses.

Some have privately expressed concern that this Committee should avoid public discussion of these vulnerabilities and the government's role. Now that the information on these vulnerabilities is publicly available, I believe we can have a responsible discussion of lessons learned to improve vulnerability disclosure and cyber resiliency, which are fundamental to cybersecurity.

With growing connectivity, the Internet of Things, and new risks posed by hardware vulnerabilities, examining and updating best practices now can help us avoid bigger problems down the road.

I want to thank all of our witnesses for being here today. It is especially good to see Dr. Griffiths, who traveled to be here today from South Dakota. She was an integral part of our cybersecurity roundtable last year, which highlighted the important role that South Dakota plays in cybersecurity research and education.

I will now turn to Senator Nelson for his opening remarks. Senator Nelson.

**STATEMENT OF HON. BILL NELSON,**
**U.S. SENATOR FROM FLORIDA**

Senator NELSON. Thank you, Mr. Chairman.

It is good that this Committee has this jurisdiction because we are embarking upon a realization of one of the greatest threats to our government, as well as our society. This jurisdiction is shared with the Armed Services Committee where this Senator has the privilege of being the Ranking Member on the Cyber Subcommittee. The jurisdiction is also shared with the Intel Committee. And the fact that we can do this in a bipartisan way, Mr. Chairman, I think is especially important because these threats are not Democrat or Republican. They are against our country and its wellbeing.

I think, and I have said this consistently, we are going to see further threats. We are going to see it in the business community, of which we have seen already quite a number. And unfortunately, I believe that we are going to see it in this coming election.

And remember, you do not have to have a threat that would actually go in and change the results of an election. All you have to do to instill total chaos is to go in and eliminate, say, every 10th voter on the rolls in a particular precinct that happens to be a critical precinct. And you can imagine when the voter arrives to vote or vote by mail and suddenly she is told she is not registered. You can imagine the chaos and the confusion that that would cause as well as the harm to our country. You can imagine if that occurred on election day. Ms. Jones arrives. "I am sorry, Ms. Jones, you are not registered." "Well, here is my registration card." "Our records show that you are not registered." So if you have a provisional ballot, that is one thing, but you can imagine how the lines stack up and the longer and longer wait times. This is just one of the realistic threats that we are facing today.

And now, as the Chairman has just said, the Spectre and Meltdown vulnerabilities discovered inside virtually every computer should be a wakeup call for all of us. These hardware vulnerabilities pose a grave threat to our economy, our way of life, and our national security.

And still, this Nation is not prepared to deal with this threat. Obviously, this includes the private sector as well. We continue to play defense. We patch vulnerabilities once they are discovered and exploited, and we simply do not have a sufficiently large, trained cybersecurity workforce to protect our country.

And of course, it is not just criminals. It is foreign actors as well. We know, as the Chairman has stated, that China has used cyber

attacks to steal both corporate and military secrets. Russia interfered with the election and launched attacks on computer networks around the world, including a crippling cyber attack on Ukraine's power grid, which is part of the Russians' MO now. There is no doubt that Russia and China will continue to exploit these and future vulnerabilities to advance their interests.

And so what brings us here to the table is that we are troubled by reports that chip makers failed to notify the U.S. Government in a timely manner of the Spectre and Meltdown vulnerabilities. According to the "Wall Street Journal," a handful of companies, including two Chinese companies, were notified before anyone at US-CERT, NSA, or DHS. And given the Chinese Government's history of exploiting cyber vulnerabilities, the lack of this disclosure is baffling and inexcusable.

While these vulnerabilities seemed to have been patched reasonably well, what about the next one? And we might not know about it until it is too late. So what are we doing about it?

I want to work with you, Mr. Chairman, and the other committees in the Senate to more proactively tackle this threat.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Nelson.

As I mentioned, we have got a great panel of witnesses in front of us today. And so we want to welcome you here and look forward to hearing from you. I am going to ask, as you give your oral remarks, if you could confine them as closely to 5 minutes as possible. We will make sure that your entire testimonies are included as part of the permanent written record of the hearing.

But we have Ms. Donna Dodson, who is Chief Security Advisor and Director of the National Cybersecurity Center of Excellence, National Institute of Standards and Technology at the U.S. Department of Commerce. We have Ms. Joyce Kim, who is Chief Marketing Officer for Arm. We have Mr. Art Manion, who is Senior Vulnerability Analyst, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University. As I said, Dr. José-Marie Griffiths, President, South Dakota, or I should say Dakota State University in South Dakota. And Mr. Sri Sridharan, who is Managing Director, Florida Center for Cybersecurity, University of South Florida.

So thank you all for being here.

Yes, sir?

Senator NELSON. Mr. Chairman, may I say we have got quite a cybersecurity center at the University of South Florida, and Mr. Sridharan's expertise on cybersecurity and his stewardship of the Florida center is a considerable asset to our country.

[The prepared statement of Senator Nelson follows:]

PREPARED STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Thank you, Mr. Chairman, for holding this hearing and working over the years on a bipartisan basis to address the growing cyber threat to our country.

The Spectre and Meltdown vulnerabilities—discovered inside virtually every computer in the world—should be a wake-up call to us all. These hardware vulnerabilities pose a grave threat to our economy, our way of life and our national security.

Still, the Nation is not prepared to deal with this threat and that includes the private sector. We continue to play defense, patching vulnerabilities once they are

discovered and exploited. And, we simply don't have a sufficiently large, trained cybersecurity workforce to protect the American people from cyberattacks.

And, of course it's not just criminals who seek to exploit cyber vulnerabilities, but hostile foreign powers too. We know that China has used cyberattacks to steal both corporate and military secrets. Russia interfered in our election and launched attacks on computer networks around the world, including a crippling cyberattack on Ukraine's power system.

There's no doubt that Russia and China will continue to exploit these and future vulnerabilities to advance their own interests and hold our economy and critical infrastructure at risk.

In this context, I am troubled by reports that chip makers failed to notify the United States Government in a timely manner of the Spectre and Meltdown vulnerabilities. According to the *Wall Street Journal,* a handful of companies, including two Chinese companies, were notified before anyone at U.S.-CERT, NSA or DHS. Given the history of the Chinese government to exploit cyber vulnerabilities, I find this lack of disclosure to the American government to be unacceptable.

While these vulnerabilities seem to have been patched reasonably well, the next one might not go so well. And we might not know about it until it's too late.

The question is: what are we doing about it?

I want to work with you and other committees in the Senate to more proactively tackle this threat. The Federal Government must work in an active partnership with the private sector to protect American citizens from the looming threat posed by hostile nation-state actors and those who seek to do us harm.

I look forward to hearing testimony from our witnesses today, and I especially want to welcome the Director of the Florida Center for Cybersecurity with the University of South Florida. Mr. Sridharan's expertise on cybersecurity and his stewardship of the Florida Center is a considerable asset to my state and to the Nation as a whole.

The CHAIRMAN. Thank you.

So we will start on my left and your right with Ms. Dodson, and please proceed. And then we will just move across the panel from there. Thank you.

## STATEMENT OF DONNA DODSON, CHIEF CYBERSECURITY ADVISOR AND DIRECTOR, NATIONAL CYBERSECURITY CENTER OF EXCELLENCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

Ms. DODSON. Chairman Thune, Ranking Member Nelson, and members of the Committee, I am Donna Dodson, Director of the National Cybersecurity Center of Excellence and Chief Cybersecurity Advisor at the National Institute of Standards and Technology known as NIST. Thank you for the opportunity appear before you today to discuss some of NIST's key projects in cybersecurity related to the Spectre and Meltdown vulnerabilities.

Cybersecurity has been part of NIST's mission since 1972, and NIST's role has been expanded since then to research, develop, and deploy cybersecurity standards and technologies to protect the Federal Government's systems against threats and to facilitate the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

Spectre and Meltdown are but two examples of hardware vulnerabilities. Vulnerabilities are weaknesses found in software, firmware, and hardware that, if exploited, can impact the confidentiality, integrity, or availability of information or information systems. NIST works to define vulnerabilities, understand their prevalence, and measure the efficacy of detection and mitigation techniques. NIST uses multiple strategies, including stopping vulnera-

bilities before they occur, detecting vulnerabilities and reducing their impact.

In 2017, a class of hardware vulnerabilities in microprocessors found in computers, servers, tablets, and phones were detected. These vulnerabilities, which became known as Spectre and Meltdown, took advantage of vulnerabilities in microprocessors to allow protected data stored in computers to be accessed. Mitigating the risk of these vulnerabilities requires efforts at multiple levels. NIST's programs addressed the concerns raised by Spectre and Meltdown in multiple ways: through resilient system design by managing vulnerabilities and complexity in systems and by looking at systematic cybersecurity challenges.

On the design front, NIST is developing guidelines on how to apply system security engineering and cyber resiliency principles, concepts, and activities into development processes. One objective of our work is to ensure that hardware and firmware provide integrity of computer systems. NIST has accomplished this objective by working with our industry partners to identify security capabilities that, when implemented, make computer systems more resilient to attacks.

NIST's work has already led to improvements in commercially available systems. Our guidelines are used by manufacturers of computers and servers around the world to create more trustworthy systems and are reflected in corresponding standards and international standards bodies.

This year NIST added additional guidelines to expand the breadth and scope of earlier work to provide detailed security guidelines for all components in a platform.

NIST also maintains the repository of publicly reported information technology vulnerabilities. This repository called the National Vulnerability Data base, or NVD, tracks vulnerabilities over time and allows users to assess changes in vulnerability discovery rates within specific products or specific types of vulnerabilities.

Examining vulnerabilities also reminds us that our technologies rely on a supply chain ecosystem that is long, complex, variable, interconnected, globally distributed, and geographically diverse. NIST's Supply Chain Risk Management Program helps organizations examine the supply chain risk through the entire lifecycle of system, products, and services. NIST is currently working to describe a method of prioritizing systems and components based on their relationship to the organization's mission.

The number of vulnerabilities being discovered also reminds us of the importance of effective planning to an organization's preparedness for cyber event recovery. NIST provides guidance to help organizations plan and prepare for the recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plans.

And one final point. NIST's Framework for Improving Critical Infrastructure Cybersecurity, which many organizations, including many State governments, use to manage their cybersecurity risk can also be used to manage risks to supply chains. An updated version released in April 2018 includes an expanded supply chain guidance section to assist organizations in implementing this capability.

NIST's work to provide and improve technical and policy solutions to an ever-growing set of cybersecurity challenges continues to build on our past efforts to address cybersecurity challenges of today.

Thank you for the opportunity to testify on this work in cybersecurity, and I am happy to answer any questions you may have.

[The prepared statement of Ms. Dodson follows:]

PREPARED STATEMENT OF DONNA DODSON, CHIEF CYBERSECURITY ADVISOR, AND DIRECTOR, NATIONAL CYBERSECURITY CENTER OF EXCELLENCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, UNITED STATES DEPARTMENT OF COMMERCE

**Introduction**

Chairman Thune, Ranking Member Nelson, and members of the Committee, I am Donna Dodson, Director of the National Cybersecurity Center of Excellence and Chief Cybersecurity Advisor at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss some of NIST's key projects in cybersecurity related to the Spectre and Meltdown vulnerabilities.

**The Role of NIST in Cybersecurity**

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with Federal agencies, industry, and academia since 1972, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. NIST's role, to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100–235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107–347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113–283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113–274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST also coordinates with numerous other Federal agencies, as well as its sister bureaus within the Department of Commerce. For example, as the Executive Branch agency principally responsible for advising the President on telecommunications and information policies, the Commerce Department's National Telecommunications and Information Administration, collaborates with NIST to ensure that the equities of innovation, economic growth, and an open Internet are factored into cybersecurity policy decisions within both domestic and international fora.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by Federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art, and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

**Managing Vulnerabilities and Building Secure Systems**

*Overview*

There are many different definitions of the term "vulnerability" that cover concepts such as knowledge, attacks, exploitability, risk, intention, threat, scope, and time of introduction. These vulnerabilities catalogued in NIST's National Vulnerability Database—a repository of vulnerability management data that enables auto-

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

mation of vulnerability management, security measurement, and compliance—are weaknesses found in software, firmware, and hardware that, if exploited, can impact the confidentiality, integrity, or availability of information or information systems. These vulnerabilities can include: manual configuration and operational mistakes (including bad passwords); insider malfeasance; functional bugs; purposefully introduced malware; or general weaknesses in code. Different types of vulnerabilities—and depending on where the affected products are being used—will require different types of responses.

Given the complexities and broad use of these technologies, fundamental to NIST's approach towards vulnerabilities is the idea that—like risk—an organization can never fully eliminate vulnerabilities. NIST works to define vulnerabilities, understand their prevalence, and measure the efficacy of detection and mitigation techniques. NIST uses multiple strategies including:

- Stopping vulnerabilities before they occur, including improved methods for specifying and building products;
- Finding vulnerabilities, including better testing techniques and more efficient use of multiple testing methods; and
- Reducing the impact of vulnerabilities by building architectures that are more resilient, so that vulnerabilities cannot be meaningfully exploited.

**Spectre and Meltdown**

In 2017, multiple teams of security researchers independently discovered a new class of hardware vulnerabilities in a broad set of microprocessors found in personal computers, servers, tablets, and phones. These vulnerabilities, which became known as Spectre and Meltdown, took advantage of a performance optimization technique found in these microprocessors to allow an attacker to bypass security mechanisms protecting data stored in computer systems. The implications of this vulnerability were severe: it could allow theft of credentials and cryptographic keys, or exfiltration of sensitive data. Mitigating the risk of these vulnerabilities required efforts at multiple levels, including patches in firmware and microcode, updates to operating systems, and modifications in applications. The necessity of a multi-level approach was due to the difficult nature of hardware-based vulnerabilities. Companies responsible for these components worked for several months before the vulnerabilities were publicly disclosed in January of 2018. At that point, security patches were released from these vendors, each addressing a different aspect of the vulnerabilities.

Spectre and Meltdown were not the first vulnerabilities in hardware. There has been an increasing risk of attacks on hardware due to their potential to be highly persistent, stealthy and powerful. The potential impact of a successful attack on hardware emphasizes the importance of ensuring that the hardware in computer system platforms is resilient. Such resilience includes strong security engineering practices when designing hardware, actively managing risks as these components move through the supply chain, and implementing foundational security capabilities in computer platforms.

I would like to take the opportunity of this hearing to highlight just a few of the efforts that relate to the Spectre and Meltdown vulnerabilities that NIST has undertaken across its Computer Security and Applied Cybersecurity Divisions. Our programs address the concerns raised by Spectre and Meltdown in multiple ways: some focus on making systems more resilient when they are designed; some assist in managing vulnerabilities and complexity after systems are operational; and many of our programs are much broader efforts looking at systemic cybersecurity challenges.

**Building Security in and Improving Hardware Security**

Through standards, guidelines, and best practices, NIST is working to improve the resiliency of systems. The hardware and firmware components that make up computer platforms are critical parts of these systems, and their secure and reliable operation is necessary for defensible, resilient systems. These components are the platform on which the rest of the system will be built.

Improving the security of these systems must start with their design. Security and resiliency should be integrated into architecture, design, and development of systems to reduce the risks of vulnerabilities and mitigate the impact of incidents that occur. NIST is developing guidelines on how to apply system security engineering and cyber resiliency principles, concepts, and activities into development processes.

One objective of our work is to ensure that hardware and firmware can provide a foundation on which we can establish greater trust in the integrity of computer systems. We have accomplished this objective by working with our industry partners

to identify security capabilities that, when implemented, make computer systems more resilient to attacks. These capabilities are based on the concepts of protection, detection, and recovery. They include mechanisms to protect the platform from malicious attacks through authenticated updates, mechanisms to detect problems if and when they occur, and mechanisms to securely recover these systems back to a trustworthy state when necessary.

Our work has already led to improvements in commercially available systems. Our guidelines are used by manufacturers of personal computers and servers around the world to create more trustworthy systems, and are reflected in corresponding standards in international standards bodies. This year, NIST added additional guidelines to expand the breadth and scope of earlier work to provide detailed security guidelines for all components in a platform. We are currently working to encourage broader adoption of the principles of firmware protection, detection, and recovery through our engagement with industry partners and consortia.

**The National Vulnerability Database**

Spectre and Meltdown, while notable, are but two examples of numerous new and pervasive vulnerabilities that have been discovered in recent years. NIST maintains the repository of publicly reported information technology vulnerabilities, called the National Vulnerability Database (NVD). The NVD is an authoritative source for standardized information on security vulnerabilities that NIST updates regularly.

The NVD tracks vulnerabilities over time and allows users to assess changes in vulnerability discovery rates within specific products or specific types of vulnerabilities. NVD uses the Common Vulnerabilities and Exposures vulnerability identification scheme, which is widely used by the security industry to provide a dictionary of common identifiers for publicly known hardware and software vulnerabilities.

As part of maintaining the NVD, NIST enables an organization to publicly disclose a vulnerability with an identifier that NIST has assigned it. NIST is working with the security community to expand the number of organizations that can disclose with a previously-allocated identifier, and to increase the degree of automation used to assign these identifiers and to publish these vulnerabilities. Health care and Internet of Things devices are specific areas of focus for this expansion, as identification of vulnerabilities in these types of devices is a growing concern for the security community.

While disclosed vulnerabilities assigned with an identifier are posted immediately, NIST also takes additional steps to analyze and provide a severity metric to assist practitioners in responding to each vulnerability. Both the number of vulnerabilities in the NVD and use of the NVD continues to grow. For example, since January 2017, each month we have seen an average of 10 percent growth in the amount of data downloaded. NIST is working aggressively to ensure the NVD can continue to provide this important information in a timely fashion.

**Supply Chain Risk Management**

These vulnerabilities also remind us that our technologies rely on a supply chain ecosystem that is long, complex, variable, interconnected, globally distributed, and geographically diverse. The same factors that decrease cost, enable interoperability, foster rapid innovation, and provide other benefits, also increase cyber supply chain risks. Managing supply chain risk requires that an organization ensure the integrity, security, and resilience of its supply chain.

NIST developed its Supply Chain Risk Management Program to work with industry, academia, and government to identify and evaluate effective technologies, tools, techniques, practices, and standards that help secure an organization's supply chain. This program examines the supply-chain risk throughout the entire lifecycle of systems, products, and services. NIST is currently working to describe a structured method of prioritizing systems and components based on their relationship to an organization's mission, thereby enabling organizations to most efficiently deploy their resources. This work will help organizations dramatically improve their cyber supply chain risk management.

**Cybersecurity Event Recovery**

The number of vulnerabilities being discovered also reminds us of the importance of effective planning to an organization's preparedness for cyber event recovery. As part of an organization's ongoing information security program, recovery planning enables participants to understand system dependencies; critical roles such as crisis management and incident management; arrangements for alternate communication channels, services and facilities; and many other elements of business continuity.

NIST provides guidance to help organizations plan and prepare for recovery from a cyber event and integrate the processes and procedures into their enterprise risk management plan. NIST's guidance presents hypothetical cyberattack scenarios and

the steps taken to recover. It provides a detailed description of the preconditions required for effective recovery, the activities of the recovery team in the tactical recovery phase, and, after the cyberattack has been eradicated, the activities performed during the strategic recovery phase.

NIST guidance assists organizations in developing an actionable set of steps, or a playbook, that organizations can follow to successfully recover from a cyber event. A playbook can focus on a unique type of cyber event and can be organization-specific, tailored to fit the dependencies of its people, processes, and technologies.

**Cybersecurity Framework**

I would like to highlight some changes to a document that the Committee maybe familiar with: the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"), which many organizations—including many state governments—use to manage their cybersecurity risk. Beginning in 2013, NIST created, promoted, and continues to enhance the Framework in collaboration with industry, academia, and other government agencies. The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework's voluntary, risk-based, flexible, repeatable, and cost-effective approach helps users manage their cybersecurity risk. The Framework was originally designed for owners and operators of critical infrastructure, but organizations of all sizes and from many economic sectors now use the Framework to manage their cybersecurity risks, including risks to their supply chains. While use is both voluntary and widespread in the private sector, the Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," formally requires Federal agencies to use the Framework to manage their cybersecurity risk—something many agencies did prior to its issuance.

In response to stakeholder requests, NIST began the public engagement process to update the Framework. This process included NIST examining lessons learned from use of the Framework, collecting written comments, hosting multiple workshops, incorporating comments and feedback, and issuing multiple drafts before publishing the final updated version 1.1 in April 2018. The Framework continues to be a living document which draws strength from active and voluntary private-sector contributors.

Due to this stakeholder engagement, NIST expanded supply chain guidance in the Framework and included a new subcategory under the "response" function that states: "Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (*e.g.,* internal testing, security bulletins, or security researchers)." While this work is an important step, it is only an initial one, and we hope to use its inclusion to further advocate for coordinated vulnerability disclosure and assist organizations in implementing this capability.

**Conclusion**

The programs that I have mentioned here are only a portion of NIST's portfolio in cybersecurity, which is only a portion of what NIST does more broadly. NIST's work to provide and improve technical and policy solutions to an ever-growing set of cybersecurity challenges continues to grow. Thank you for the opportunity to testify today on NIST's work in cybersecurity. I am happy to answer any questions you may have.

---

DONNA F. DODSON, NIST ASSOCIATE DIRECTOR AND CHIEF CYBER SECURITY ADVISOR

Donna F. Dodson is a Fellow at the National Institute of Standards and Technology (NIST). She holds the position of the Chief Cybersecurity Advisor for NIST and is the Associate Director for the Information Technology Lab (ITL). Donna also serves as the Director of NIST's National Cybersecurity Center of Excellence (NCCoE).

Donna oversees ITL's cyber security program to conduct research, development and outreach necessary to provide standards, guidelines, tools, metrics and practices to protect the information and communication infrastructure. Under her leadership, ITL collaborations with industry, academia and other government agencies in research areas such as security management and assurance, cryptography and systems security, identity management, security automation, secure system and component configuration, test validation and measurement of security properties of products and systems, security awareness and outreach and emerging security technologies. In addition, Donna guides ITL programs to support both national and international security standards activities. She led the establishment of the NIST NCCoE. Through partnerships with state, local and industry, the NCCoE collabo-

rates with industry sectors to accelerate the widespread adoption of standards-based cyber security tools and technologies.

Donna's research interests include applied cryptography, key management, authentication and security testing. She has led technical teams to produce standards, guidelines and tools in each of these areas.

Donna received two Department of Commerce Gold Medals and three NIST Bronze Medals. She received her second Fed 100 Award in 2018, for her innovations in cybersecurity and in 2011 was included in the top 10 influential people in government information security. She has also received two FedScoop awards recognizing her as one of DC's Top 50 Women in Tech.

The CHAIRMAN. Thank you, Ms. Dodson.

Ms. Kim.

**STATEMENT OF JOYCE KIM,**
**CHIEF MARKETING OFFICER, ARM**

Ms. KIM. Good morning, Chairman Thune, Ranking Member Nelson, and members of the Committee. I would like to thank you for holding this hearing and inviting Arm to participate. My name is Joyce Kim and I am the Chief Marketing Officer for Arm. Arm is the leading global provider of processor designs for the mobile industry, including Internet of Things and other advanced computing.

I have been in the tech sector for almost 25 years, and I am here to talk about Arm's handling of Spectre and Meltdown. I am pleased to be testifying here today and share Arm's perspective and the effectiveness by which we worked with our customers and the industry to respond to these vulnerabilities.

With respect to our business, Arm designs processors, and those designs are licensed to chip manufacturers. But we do not sell directly to end users, nor do we manufacture chips ourselves. We also do not have direct business relationships with supply chain vendors.

Spectre and Meltdown were an unprecedented challenge for the semiconductor industry. Arm responded to those vulnerabilities with the utmost urgency and seriousness. We quickly verified the issues immediately following notification in June 2017. Within 10 days of learning of the potential vulnerabilities, we began discussions with our architecture customers so that they could identify and evaluate the vulnerabilities with respect to their own customizations from the Arm processor designs. We worked with each of them to help them determine whether their products could be affected by these vulnerabilities, determine the full scope, and develop mitigations.

We informed our implementation customers and provided appropriate mitigations when the vulnerabilities were made public on January 3, 2018. We publicly released a detailed technical white paper and created a dedicated website to disseminate the information.

Later in 2018, another variant of Spectre and Meltdown emerged, which Arm aggressively addressed. We again notified our architecture customers early in the process, and this time we notified all potentially impacted customers 4 weeks prior to public disclosure. We also notified the U.S. Government in advance of the public disclosure.

We have treated information regarding Meltdown and Spectre with discretion due to the potential for exploitation by bad actors. Generally, when vulnerabilities are discovered by security researchers, they notify the affected parties and provide time to develop mitigations before public disclosure. That length of time depends on several factors, including severity, availability, complexity, as well as the potential impact of early disclosure.

I can attest that addressing these vulnerabilities was our top priority for Arm's senior leadership, as well as senior technical staff. We believe Arm's response contributed to the security of the ecosystem. Arm is pleased to have been able to build a productive relationship with the Department of Homeland Security, in which we look forward to partnering with security issues in the future. We plan further engagement to share information and best practices, and we look forward to a productive and mutually beneficial relationship regarding overall security of processors.

Cybersecurity risk management is a process. In addition to working with the government, Arm has taken several steps to refine its approach to vulnerability management. We created a dedicated website that is ongoing with more details on how researchers can contact the company. And additionally, we put in place internal vulnerability handling and disclosure policies based on the work that is done by the International Organization of Standards.

Thank you for your time.

[The prepared statement of Ms. Kim follows:]

PREPARED STATEMENT OF JOYCE KIM, CHIEF MARKETING OFFICER, ARM

Good morning. Chairman Thune, Ranking Member Nelson, and members of the Committee I would like to thank you for holding this hearing and for inviting Arm to participate. My name is Joyce Kim and I am the Chief Marketing Officer for Arm. Arm is the leading global provider of processor designs for mobile devices, the Internet of Things, and advanced computing. It is highly likely you are in possession of several Arm designed processors right now. If you have a mobile phone, smart watch, or tablet with you, you are utilizing Arm technology. As is well known, some of the products designed by Arm, were found to be subject to vulnerabilities known as Spectre and Meltdown. Other manufacturers' processors were also affected, reportedly far more substantially that Arm's. The Spectre and Meltdown vulnerabilities were made public on January 3, 2018. Given the prevalence of the affected technologies, we understand this Committee's and the government's interest in these vulnerabilities and the process followed to address them. I look forward to providing the Committee with information about Arms' response and our approach to addressing vulnerabilities in the highly interconnected global mobile supply chain.

As Arm's Chief Marketing Officer, it may not be readily apparent why I would be testifying today. I have more than 25 years in the tech sector, and I was heavily involved in Arm's response to the Spectre and Meltdown vulnerabilities on behalf of the executive team. This included interacting with Google Project Zero, after it found the vulnerabilities, coordinating with other industry companies that were addressing the vulnerabilities, as well as Arm's customers and partners to put mitigations and supporting documentations in place.

Arm treated and responded to these vulnerabilities with the utmost urgency and seriousness. We responsibly verified the issues within days of notification and successfully worked to mitigate the issues over several months. Despite these efforts, I believe many press stories on these vulnerabilities sensationalized the issue. This is not unusual when it comes to security vulnerabilities. Nonetheless, information about the Meltdown and Spectre vulnerabilities was handled with discretion and care by Arm due to the potential malicious exploitation of this vulnerability. As a general matter, Arm believes that vulnerability information is sensitive and should be treated with caution. Often, when vulnerabilities are discovered by security researchers, they will notify affected parties and provide time to develop solutions and mitigations before broader public disclosure. The length of time depends on the se-

verity of a vulnerability, availability of a solution or mitigation, the complexity of developing such solutions, and potential impact of early disclosure. Having been involved in coordinating Arm's response to these vulnerabilities from days after the discovery in June 2017, I can attest that addressing these vulnerabilities was a top priority for Arm's senior leadership and senior technical staff. I am pleased to be testifying today to share Arm's perspective on the efficiency and effectiveness by which we worked with our partners to respond to these vulnerabilities.

**Arm's business is to design processors that are used in a variety of devices and equipment**

To understand Arm's role in responding to the Spectre and Meltdown vulnerabilities, it may be helpful to start with a brief overview of Arm's business. Arm creates processor architectures that are primarily licensed to semiconductor manufacturers. Arm has two distinct types of commercial relationships with its direct customers for processor technology:

- *"Implementation partners"* license processors that have been fully designed, developed, and implemented by Arm itself. These partners then manufacture their own resulting chips.
- *"Architecture partners"* license Arm's processor architecture, but they design, develop, and implement their own processors based upon Arm's architectures. The architecture partners develop processors that, while software compatible, are proprietary in their implementation, and the specific detailed knowledge of the processors is not within Arm's knowledge or control. These partners then manufacture their own resulting chips.

Arm does not sell a physical product that is utilized by end users, nor do we have direct business relationships with end users or most of the software providers and supply chain. We license intellectual property in the form of processor designs to our customers who may or may not have a direct relationship with end users. Therefore, our response and mitigation plans to the Spectre and Meltdown vulnerabilities required a collaborative approach, including not only our architecture and implementation partners, but other software providers and industry.

**Arm's exposure to the Spectre and Meltdown vulnerabilities was relatively limited**

Spectre and Meltdown are vulnerabilities that take advantage of a design feature intended to improve the performance of processors. The vulnerabilities were discovered in a new area of research exploring the theoretical possibility of utilizing that performance feature, known as speculative execution, as a mechanism to extract pieces of sensitive data through a side-channel attack.

It should be noted that possible exploitations would be difficult, insofar as they appear to be dependent on malware running locally, which would have to be deployed on the target device. This means a device must already be compromised to execute this type of attack. It is therefore imperative for users to practice good security hygiene by keeping their software up-to-date and avoiding suspicious links or downloads. Arm has emphasized this in the process of developing and promoting mitigations for Meltdown and Spectre. I would also note, the vast majority of chips based on Arm processors are not impacted by Meltdown or Spectre.[1] Nonetheless, Arm and all of our industry and business partners have taken this very seriously.

Moreover, to date, Arm has been unable to create by itself (or identify from third-parties) any proof of concept code that creates the conditions necessary to improperly extract data from a mobile system using the Spectre vulnerability on any Arm processor. Arm is not able to detect if these vulnerabilities have been exploited, but, as mentioned previously, exploitation of the vulnerability requires malicious code to be installed on the user device. Industry researchers have only seen a rise in such malicious code following the public disclosure of such vulnerabilities.[2] Because mitigations were made available by Arm prior to the public disclosure through collaboration with our customers and others in industry, Arm believes that the ability for bad actors to use such vulnerabilities will be reduced by that collaboration.

**Arm responded thoroughly to the Specter and Meltdown vulnerabilities**

Upon learning of the first variants of Spectre and Meltdown on June 1, 2017, Arm acted expeditiously to validate the issues and help its partners develop mitigations. That work entailed placing a priority on evaluating the vulnerability, its potential

[1] See *http://www.arm.com/security-update*

[2] See *Malware Exploiting Spectre, Meltdown Flaws Emerges, https://www.securityweek.com/malware-exploiting-spectre-meltdown-flaws-emerges*

impact on processors implemented by Arm, and developing mitigations and software that its architecture and implementation partners could use and deploy to secure their devices and operating systems. In determining how to disseminate information about vulnerabilities and mitigations, Arm prioritized rapid development of technical solutions that could mitigate vulnerabilities and be used by its customers throughout the industry.

Within 10 days of learning of the potential exploits in June 2017, Arm informed architecture partners to provide them knowledge so they could evaluate the vulnerabilities with respect to their own implementations of the Arm architecture. This is due to the points mentioned above about Arm's business relationship with these customers. Arm's architecture partners create custom designs compliant with the Arm architecture licensed to them, so we are unaware how, or if, the end product these customers create may be affected by these vulnerabilities. We informed our implementation partners and provided appropriate mitigations in January 2018. Arm notified this set of partners later because the company knew that implementation partners would be affected and would not need to create their own mitigations because they receive processors designed by Arm, rather than a license to create their own.

After the public disclosure, Arm communicated recommended mitigation measures to all affected customers. Arm publicly released a detailed technical white paper that identified the issues and mitigations. Arm has updated that white paper as appropriate. The impact of this outreach and coordination was broad, covering companies, developers, and users of Arm processors across a wide variety of business sectors and industries.

Arm's response to the variants disclosed in January 2018 was praised publicly by ArsTechnica, an online publication read widely by technologists and IT professionals. In particular, the publication stated "Arm's response was the gold standard. Lots of technical detail in a whitepaper. . ."[3]

Later in 2018, a fourth variant to the Specter and Meltdown vulnerabilities emerged which Arm again aggressively addressed. We again chose to notify architecture partners early in the process for the reasons discussed above. Arm was able to determine which implementation partners were affected and which were not; Arm notified affected implementation partners approximately one month before public disclosure to afford the more time to put the mitigations in place prior to public disclosure. Arm also notified the U.S. Government of Variant 4 in advance of public disclosure.

**Arm has engaged the United States Government**

As Arm previously stated to the Committee in our written response to Chairman Thune and Ranking Member Nelson on March 1, 2018, we did not communicate with the U.S. Government prior to the initial Spectre and Meltdown variants being disclosed by Google Project Zero in January 2018. After considering emerging practices across industry, and after discussions with this Committee and your colleagues in the House of Representatives, Arm recognized and has pursued several process refinements to improve its handling of vulnerabilities. Among those, we have recognized the importance of working with government stakeholders that may be able to share information and help minimize the impact on end users. As such, Arm did notify the U.S. Government and brought our chief architect to DC from Arm's headquarters in Cambridge, United Kingdom to brief government stakeholders at the Department of Homeland Security (DHS) on Variant 4 in advance of the public disclosure of that vulnerability. We have remained in contact with DHS and plan further engagements to share information and best practices. We look forward to a productive and mutually beneficial relationship that can contribute to security in the mobile ecosystem.

**Arm has refined its vulnerability handling process**

Again, I believe Arm handled the response to these vulnerabilities extremely well. However, there is always room for improvement, because cybersecurity risk management is a process that evolves over time. As a result, Arm has taken several steps to refine its approach to vulnerability identification and management. First, Arm has created a dedicated, externally facing website with details on how researches may contact us with potential product vulnerabilities.[4] Second, Arm has put in place an internal vulnerability handling and disclosure policy based on the International

---

[3] See *Meltdown and Spectre: Here's want Intel, Apple, Microsoft, others are doing about it, https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/*

[4] See *https://www.arm.com/security*

Organization for Standards (ISO) standard numbers 30111[5] and 29147,[6] respectively. Lastly, as noted, Arm has engaged the U.S. Government to work collaboratively to minimize the impact of vulnerabilities on end users in advance of public disclosure of vulnerabilities.

**Conclusion**

Thank you again for the invitation to testify today. I look forward to your questions.

The CHAIRMAN. Thank you, Ms. Kim.

Mr. Manion.

**STATEMENT OF ART MANION, VULNERABILITY ANALYSIS TECHNICAL MANAGER, CERT COORDINATION CENTER, CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE**

Mr. MANION. Chairman Thune, Ranking Member Nelson, and members of the Committee, thank you for the opportunity to appear here today to discuss complex cybersecurity vulnerabilities and specifically some of the challenges and lessons from the Spectre and Meltdown disclosures.

My name is Art Manion. I am the Vulnerability Analysis Technical Manager at the CERT Coordination Center, and the CERT Coordination Center is part of Carnegie Mellon University's Software Engineering Institute.

Much of the vulnerability analysis work we have performed over the past 30 years has focused on coordinated vulnerability disclosure or, as I will abbreviate it, CVD. We are both practitioners. We offer a free public facing coordination service and facilitators. As part of the FFRDC mission, we transition CVD best practices to others. Some of that transition takes the form of guidelines and standards that we either author directly, such as the CERT Guide to Coordinated Vulnerability Disclosure, and also to ISO standards, and we have even contributed to the NIST Cybersecurity Framework.

We also work closely with the Department of Homeland Security, National Cybersecurity and Communications Integration Center, or NCCIC as they call themselves. There are elements there known as US-CERT and ICS-CERT, who are helpful for defending control system, safety critical systems and public safety in the U.S.

We also work with other CVD stakeholder communities such as security researchers, hardware and software vendors, and more recently policymakers and regulatory agencies.

I plan to use my time to explain coordinated vulnerability disclosure processes using Spectre and Meltdown as a leading example. I will be briefly referring to two figures in my written testimony. It is not necessary to have them in front of you, but just as a note, I will be talking about those things.

Also what is interesting to note is there was a new Spectre variant released yesterday. So we are not done with this line of disclosures.

So there were more than 20,000 publicly disclosed vulnerabilities in 2017—20,000—more than that. Essentially all the software and some of the hardware that we use and rely on has vulnerabilities

[5] See *https://www.iso.org/standard/53231.html*
[6] See *https://www.iso.org/standard/45170.html*

of some sort. Some are publicly known. Some are privately known. Some have not been discovered yet. There are entire fields dedicated to trying to reduce vulnerabilities, and yet here we are.

So to deal with these vulnerabilities in the systems we are all currently using and depending on, we turn to CVD. Figure 1 in my written testimony outlines the general phases of CVD. So a vulnerability must be discovered in the first place. Someone must find it. Ideally that person or organization chooses to report to a vendor or to a coordination center. There must be an assessment of that vulnerability, prioritization, triage, verification of it. Assuming it is a valid vulnerability, there is work to be done developing and testing fixes and working on a disclosure plan and eventually disclosing the vulnerability and fixes for it.

The primary risk posed by these vulnerabilities is that they could be exploited, as we have seen in things like the WannaCry and Petya malware. So to this end, during this coordinated disclosure process, the steps are kept secret. The activity is kept under embargo until the public disclosure. This secrecy and embargo period adds a lot of complexity to the process.

Bilateral disclosure is a relatively soft problem. One researcher and one vendor can easily communicate and follow the protocol and reach a generally agreeable consensus and end state.

Multi-party or multi-vendor coordination disclosure, as illustrated by Spectre and Meltdown, remains unsolved. Instead of one vendor, there can be dozens or hundreds. Each vendor has to go through all of the phases in secrecy, and somehow the public disclosure is coordinated so as many of the vendors as possible release updates all at the same time. Vulnerabilities that affect multiple vendors usually do so because of shared supply chain connections, and due to the way modern software and devices are built with increasing connected supply chains, we anticipate more vulnerabilities of this Spectre and Meltdown style with multiple vendors involved.

From the CVD process point of view, the difficult questions become how much information should be released, to whom, and when.

So the first phase of disclosure in Spectre and Meltdown involved chip manufacturers. They were told initially. They have the power to effect change that fixes the actual vulnerabilities. Very closely a second tier would be operating system vendors who have to make changes as well, who depend on the first tier vendors to have made their changes first. Later notifications could include Internet infrastructure providers, cloud service providers, and those responsible for defending networks and also groups like ICS-CERT and US-CERT who are responsible for public safety.

So just to close out, the Meltdown and Spectre disclosure process was reasonably successful. CVD processes were followed. Without any changes to existing practices, the process could have been tuned differently to include more vendors sooner and also to notify more stakeholders, including U.S. Government stakeholders, before the disclosure took place. We hope ongoing that we can adjust this process to not have a situation like Meltdown and Spectre occur again.

I thank you for the opportunity to be here today and welcome your questions.

[The prepared statement of Mr. Manion follows:]

PREPARED STATEMENT OF ART MANION, VULNERABILITY ANALYSIS TECHNICAL MANAGER, CERT/CC, CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

**Introduction**

Chairman Thune and Ranking Member Nelson, thank you for the opportunity to appear before the Senate Committee on Commerce, Science, and Transportation to discuss Complex Cybersecurity Vulnerabilities, specifically some of the challenges and lessons from the Meltdown and Spectre disclosures. I am currently the Vulnerability Analysis Technical Manager at the CERT Coordination Center (CERT/CC), part of Carnegie Mellon University's Software Engineering Institute (SEI).[1] The SEI is a Department of Defense Federally Funded Research and Development Center (FFRDC). The SEI conducts research and development in software engineering, systems engineering, cybersecurity, and many other areas of computing, working to transition new and emerging innovations into government and industry. The SEI holds a unique role as the only FFRDC sponsored by the DoD that is also authorized to work with organizations outside of the DoD. We work with partners throughout the U.S. Government, the private sector, and academia.

Much of the vulnerability analysis work at the CERT/CC over the past 30 years has focused on Coordinated Vulnerability Disclosure (CVD). This is the practice of reporting newly discovered vulnerabilities to vendors (and/or third-party coordinators, like ourselves), working cooperatively to develop fixes and mitigations, and eventually publicly disclosing information for defensive purposes. The results of many coordinated disclosure cases we work on are published as Vulnerability Notes.[2] We work closely with the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) elements commonly known as US–CERT and ICS–CERT as well as other stakeholder communities including security researchers, vendors and other software development organizations, and more recently, policy makers and regulatory agencies.

In August 2017 my team published *The CERT Guide to Coordinated Vulnerability Disclosure,*[3] capturing decades of experience, observation, and advice. This testimony draws heavily on the *Guide* and the collective experience of my current team and past members.

The CERT/CC is a founding member of the Forum of Incident Response and Security Teams (FIRST), and I co-chair two special interest groups within FIRST that deal with CVD. The Vulnerability Coordination SIG, collaborating with a National Telecommunications and Information Administration (NTIA) multistakeholder process,[4] published guidelines for multiparty CVD in June 2017.[5] My team provides advice to transportation (including the Department of Transportation) and medical device (including the Food and Drug Administration) sectors. We participate in other policy and community efforts to improve and advocate CVD processes, and we directly assist departments and agencies, helping to design and support the DoD Vulnerability Disclosure Program.[6] I also work in the International Standards Organization (ISO) where I am co-editor of ISO 29147 *Vulnerability disclosure* [7] and 30111 *Vulnerability handling processes.*[8]

**Coordinated Vulnerability Disclosure (CVD)**

We all depend on software and software-based systems. The devices we use to communicate and coordinate our lives, transport us from place to place, and keep us healthy include computers, network connections, and software. As a result, society has increased its dependence on software-based products and services that communicate both to each other and to the world at large.

One drawback: our modern and connected products and services have vulnerabilities—weaknesses that can compromise the security of the system in unexpected and

---

[1] *https://www.sei.cmu.edu/*
[2] *https://www.kb.cert.org/vuls*
[3] *https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330*
[4] *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities*
[5] *https://www.first.org/global/sigs/vulnerability-coordination/multiparty/*
[6] *https://hackerone.com/deptofdefense*
[7] ISO/IEC 29147 *https://www.iso.org/standard/45170.html*
[8] ISO/IEC 30111 *https://www.iso.org/standard/53231.html*

undesirable ways. Vulnerabilities leave our devices and systems susceptible to attacks. Smart phones, ATMs, MRI machines, security cameras, cars, airplanes, and the like have become network-enabled software-dependent systems, making it nearly impossible to avoid participating in the world without the potential to be affected by cybersecurity vulnerabilities.

Essentially unavoidable, vulnerabilities have numerous origins. Implementation defects, unexpected interactions between systems, configuration or design decisions, and other factors all contribute to what is effectively an unlimited supply.[9] In order to maintain assurance in the systems and devices we use daily, we need clear public policy and socio-technical norms encouraging the discovery of vulnerabilities, notification of their existence, and cooperative defense in the form of repair or mitigation. Otherwise, adversaries can take advantage of vulnerabilities to achieve goals at odds with the creators and users of the systems we depend on.

Notifying the public that a problem exists without simultaneously providing defense leads to increased adversarial advantage. Because there is rarely one optimal formula for minimizing risk and harm—short of avoiding the introduction of vulnerabilities in the first place—the current best practice is a process called Coordinated Vulnerability Disclosure (CVD).

CVD is the process of gathering information from security researchers, coordinating the sharing of that information to vendors and other relevant parties, and disclosing the existence of software vulnerabilities along with updates or mitigations to various stakeholders—including the public. The CVD process concludes when updates and mitigations have been widely deployed.

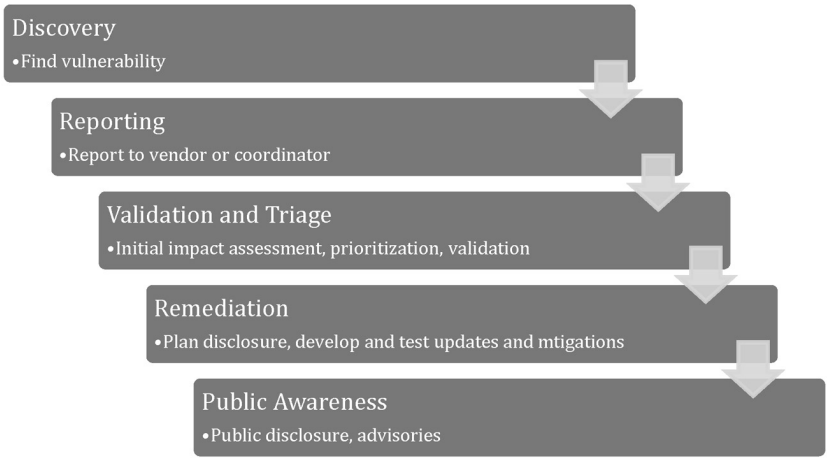



*Figure 1: CVD phases*

Figure 1 outlines a generally accepted set of basic CVD phases. As noted in the *Guide,* the more difficult questions are: "How much information should be released? To whom? And when?"

Bilateral CVD—between one researcher and one vendor—is largely a solved problem. That is to say, there exist established CVD processes that both parties can follow to a generally agreeable and optimal outcome.

Multiparty or multivendor CVD, as illustrated by Meltdown and Spectre, remains unsolved. The CERT/CC focuses our efforts on multiparty CVD, both directly handling cases and researching ways to make lasting improvements. As described in the *Guide,* CVD is a wicked problem,[10] and multiparty CVD even more so.

---

[9] Risk Based Security recorded ". . . over 20,000 vulnerabilities disclosed in 2017." The NIST National Vulnerability Database (NVD), based on the Common Vulnerabilities and Exposures (CVE) project, reports 14,650.

[10] H. W. Rittel and M. M. Webber, "Dilemmas in a General Theory of Planning," Policy Sciences, vol. 4, no. 1973, pp. 155–169, June 1973.

**Meltdown and Spectre**

Meltdown and Spectre are the widely used names for the first three instances of a class of vulnerabilities that arise from speculative execution[11] and shared caches,[12] features designed into modern CPU hardware for improved performance. These side-channel vulnerabilities allow attackers to infer the contents of memory without having direct access to the memory. Meltdown and Spectre were initially reported in June 2017 and three variants were publicly disclosed on January 3, 2018. Since then, three additional variants have been published, and further public disclosures are expected. It is interesting to note that these security issues were previously discussed in 1995.[13]

Meltdown and Spectre allow attackers to read memory that they shouldn't have access to, memory that could contain users' passwords, trade secrets, encryption keys, or the contents of private documents. Users of shared cloud infrastructure are particularly at risk. Attacks can also be performed against web browsers that visit malicious sites.

Such access to another's data is remarkable. Modern CPU hardware and operating system software separate running programs from each other and from the operating system, for stability and security reasons. This separation was meant to ensure that one user of the computer cannot read memory in use by another user or the privileged operating system, which could contain sensitive or secret information.

Because Meltdown and Spectre are intrinsic to CPU hardware, they are different from much more common software vulnerabilities. Consequently, while some of the Meltdown and Spectre variants can be mitigated with operating system and CPU microcode updates, newly designed CPU hardware will be required to fully resolve the majority of the vulnerabilities.[14]

**Challenges and Lessons Learned**

Overall, the vendor-led CVD process followed for Meltdown and Spectre was reasonably successful. Major vendors (including competitors Intel, AMD, and Arm) cooperated on security, and major software and service providers applied updates that protected many users en masse. The vendors involved followed current CVD practices, arguably tuned too far in favor of attempting to prevent premature public disclosure. This tuning introduced challenges, particularly for those tasked with defending critical infrastructure and public safety. Due to a number of factors, including the vendor-led CVD process and the novelty and complexity of the technology involved, Meltdown and Spectre garnered public attention that arguably exceeded the "actual" risk of the vulnerabilities.

The following are a set of challenges and lessons brought to light by the Meltdown and Spectre disclosures.

*CVD should follow the supply chain*

At its most effective, CVD follows the supply chain affected by the vulnerability. Many products today are not developed by a single vendor. Instead, they are assembled from components sourced from other vendors. For example, software libraries are often licensed for inclusion into other products. When a vulnerability is discovered in a library component, it is very likely that not only does the originating vendor of the library component need to take action, but all the downstream vendors whose products use it need to take action as well. Complex supply chains can increase confusion regarding who is responsible for coordinating, communicating, and ultimately fixing vulnerabilities, leading to delays and systems exposed to unnecessary risk. Because of the underlying nature of the vulnerabilities, Meltdown and Spectre exacerbated these concerns.

---

[11] occurs when the CPU, which would otherwise be sitting idle, instead makes an informed guess as to what instructions a running program will take next

[12] areas of memory with quick access

[13] *https://pdfs.semanticscholar.org/2209/42809262c17b6631c0f6536c91aaf7756857.pdf*

[14] *https://energycommerce.house.gov/wp-content/uploads/2018/02/Intel-Corp-response-HEC-FINAL.pdf*

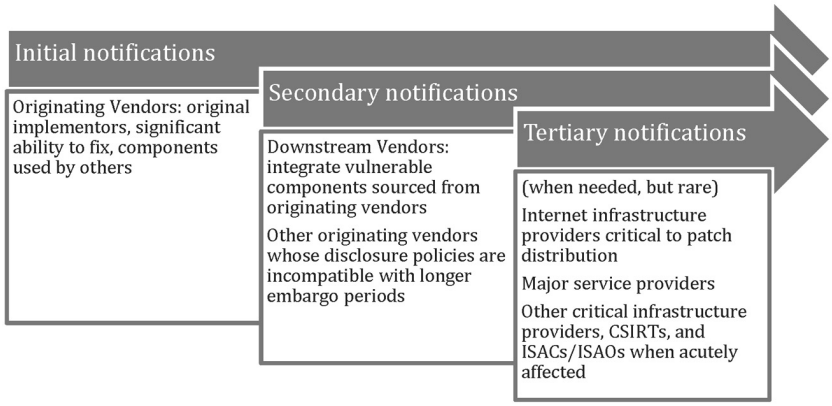



*Figure 2: Notional multiparty CVD process*

*Initial notifications*

When considering private notification and embargo, there is general agreement that those who have the ability to make changes that remove or substantially mitigate vulnerabilities need to be informed. This usually means vendors who produce original implementations. For Meltdown and Spectre, these vendors were CPU manufacturers: Intel, AMD, and Arm.

*Secondary notifications*

Operating system and virtualization software is tightly bound to CPU hardware, and mitigations for Meltdown and Spectre generally require both CPU microcode and software updates. Thus, another set of vendors with the ability to fix included Microsoft, Google, and Apple. For vendors who advertise short embargo periods, it is possible to delay notification until shortly before public disclosure.

*Tertiary notifications*

Depending on the nature, scope, and potential impact of the vulnerability, it may make sense to notify major service providers, in this case, the cloud computing elements of Amazon, Microsoft, and Google. Consideration should also be given to notifying critical infrastructure protection stakeholders, at least to reduce the harm associated with surprise disclosure.

Conceptually, it can be useful to think of the supply chain as horizontal or vertical. A horizontal supply chain implies that many vendors need to independently make changes to their products in order to fix a vulnerability. A vertical supply chain implies that one vendor might originate the fix, but many other vendors may need to update their products after the original fix is available. In these terms, Meltdown and Spectre exhibit aspects of both horizontal and vertical supply chains, making the coordination process even more complex.

*Fairness in CVD is desirable but difficult to achieve*

From a coordinator's perspective, it can be difficult to be fair when coordinating a multiparty CVD case, because it's almost inevitable to either miss some downstream vendor or wind up with one or more vendors ready to release while everyone is waiting for the other vendors to catch up. The CERT/CC's practice is to notify a wider selection of vendors and other stakeholders than those included in the Meltdown and Spectre CVD process, acknowledging that this increases the risk of premature public disclosure.

*Broader CVD cases require shorter embargo periods*

The CVD process for Meltdown and Spectre was complicated by the nature of the supply chain and the premature public disclosure which caught many by surprise. Our experience shows that problems can arise when the multiple parties involved in CVD function at different operational tempos. In both the vertical and horizontal supply chain cases discussed above, synchronized timing of disclosure to the public can be difficult to coordinate. The originating vendor(s) will usually want to release a patch announcement to the public as soon as it is ready. This can, however, put users of downstream products at increased risk. As a result, coordinators sometimes

find it necessary to make the difficult choice to withhold notification from a vendor in a complicated multiparty disclosure case if that vendor's disclosure policy is incompatible with the embargo or otherwise cannot be trusted to cooperate with the coordination effort. This may have been a factor for Meltdown and Spectre and was illustrated by the CVD process for the KRACK Wi-Fi vulnerabilities.[15]

*Vendors are not the only stakeholders with a role to play prior to public disclosure*

In situations where a vulnerability has the potential for major impact to critical infrastructure, it may be necessary to coordinate not only with vendors to fix the vulnerable products, but also with major deployers—those responsible for applying updates and other mitigations that affect large populations of users. One important concern in these cases is to ensure that Internet and other critical infrastructure remains available so that deployers and other network defenders can acquire and deploy the necessary information and patches. Another important concern is that critical infrastructure protection stakeholders are prepared to provide accurate and actionable information before public disclosure.

Luckily this scenario is rare, but vulnerabilities like Meltdown and Spectre, or those that affect basic Internet services such as the domain name system (DNS), can affect a large number of vendors. In these cases, the involvement of a coordinator such as the CERT/CC can often help contact and disseminate information to vendors, service providers, and other key stakeholders. Note that the CERT/CC was not engaged in the coordination of Meltdown and Spectre prior to their public disclosure.

*Rushed solutions can increase risk*

The Meltdown and Spectre disclosures generated a lot of public attention. They were the results of cutting-edge research from multiple sources; a lengthy embargo period (roughly 6 months) and closely held CVD process among major vendors; and in the end, the public disclosure happened one week earlier than planned. Many organizations were surprised by the public disclosure and spent considerable effort trying to understand the nature of the vulnerabilities and their impact.

Due to the fundamental technical nature of the vulnerabilities, the complexity of CPU and operating system interaction, and in some cases the lack of lead time, many of the updates and mitigations caused significant negative side effects. A partial list follows.

- Intel microcode updates caused instability.[16]
- Initial Meltdown updates for Microsoft Windows 7 and Server 2008 mistakenly allowed any user to read kernel memory and gain complete control of a computer.[17]
- Microsoft Windows updates caused some AMD systems not to boot.[18]
- Architectural changes caused some antivirus software running on Microsoft Windows to not work. The changes also had serious implications for receiving future security updates.[19]
- Lenovo systems running SUSE can become inoperable.[20]
- Pulse VPN client on Microsoft Windows would not connect.[21]
- Dell systems experienced unpredictable behavior.[22]

Independent of the unintentional side effects, the updates decrease performance, because the CPU and operating system have to spend more time clearing out the remnants of speculative execution left in the cache. While an individual user may not notice, busy server systems are significantly impacted by the performance decrease.[23] This may require the purchase of additional server capacity to maintain performance equivalent to pre-update levels.

---

[15] *https://www.krackattacks.com/#openbsd*
[16] *https://newsroom.intel.com/news/intel-security-issue-update-addressing-reboot-issues/*
[17] *https://www.kb.cert.org/vuls/id/277400*
[18] *https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892*
[19] *https://support.microsoft.com/en-us/help/4072699/windows-security-updates-and-antivirus-software*
[20] *https://support.lenovo.com/us/en/solutions/len-18282*
[21] *https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB43600*
[22] *https://www.dell.com/support/article/us/en/04/sln308588/microprocessor-side-channel-vulnerabilities-cve-2017-5715-cve-2017-5753-cve-2017-5754-impact-on-dell-emc-products-dell-enterprise-servers-storage-and-networking-?lang=en*
[23] *https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/*

Given the side effects and performance penalties, users should carefully consider the need to install Meltdown and Spectre updates. The vulnerabilities pose the greatest risk to systems that allow multiple users to run code, for example, cloud-based shared or multi-tenant hosting providers. Individual users may not substantially improve their security by installing updates. Systems that require high availability and reliability, such as industrial control and other safety critical systems, should not install updates or make other changes without significant testing.

*Surprise leads to misplaced effort and opportunity cost*

As with most situations in which multiple parties are engaged in a potentially stressful and contentious negotiation, surprise in CVD tends to increase the risk of a negative outcome. For technically complex vulnerabilities like Meltdown and Spectre, there is a need for stakeholders to understand the problem before it is possible to make good decisions about the appropriate response. Because so many vendors, deployers, and other stakeholders were caught off guard with the public disclosure of the Meltdown and Spectre vulnerabilities, much attention was diverted from potentially more pressing and immediate cybersecurity issues.

**CVD Improvements**

As previously stated, the Meltdown and Spectre CVD process was reasonably successful. Without any changes to existing practices, the process could have been tuned to include more vendors and to notify more stakeholder organizations before public disclosure. This recommendation comes with the understanding that the chance of premature disclosure increases with the number of people and organizations brought into the circle. I am aware of zero premature disclosures or other leaks caused by the NCCIC, US–CERT, or ICS–CERT. I am aware of a few leaks caused by organizations privately notified by the CERT/CC, but over 30 years and tens of thousands of CVD cases, I am comfortable with the balance we have chosen. Public information about Meltdown and Spectre started appearing in November 2017. In my experience, a case of this magnitude was unlikely to survive a lengthy embargo period.

Meltdown and Spectre set an inflection point in the history of CVD and Internet security. The researchers, and more importantly the coordinating vendors, could have recognized the need to at least reduce surprise by informing the U.S. Government (and possibly other governments) sooner. Such a decision is already accounted for in existing CVD guidance; implementing it is a matter of tuning known parameters.

Aside from the increased risk of premature disclosure, vendors have cited the need to act fairly as another reason not to notify governments in advance. Governments can be both customers and regulators, wielding purchasing and legal power. Which government(s) should a CVD process include before public disclosure?

There are options. Vendors could choose to inform governments based on confidence that the government will maintain the embargo and only use the information for defensive purposes. Microsoft, for example, offers a Government Security Program[24] to qualified governments that includes advanced notice of vulnerability disclosures. It is not clear, however, how conflicting sharing agreements are resolved. Also, the program notifies governments five days before public disclosure, Meltdown and Spectre leaked six days early.

Despite, or because of, our long history of handling multiparty CVD cases, we do not believe that a single global coordinator designed to handle nearly every multiparty case will scale. The CERT/CC is part of a loosely-affiliated multinational network of coordinators, with whom we share common CVD practices. This network sometimes shares vulnerability information in order to reach a wider global selection of vendors. These coordinators are related to their respective national governments: Japan, Finland, and the Netherlands.[25] One solution to scalable, multiparty CVD may be a more formal network of coordinators. Another option could be a more formal collection of national government computer security incident response teams (CSIRTs)[26] that agree to follow suitable embargo and information sharing restrictions. However, as mentioned above, government involvement in CVD may be a concern for vendors and inhibit their willingness to participate. Other ideas include non-governmental organizations (NGOs) or commercial businesses that are sufficiently independent of any one government.

---

[24] *https://enterprise.microsoft.com/en-us/trends/government-security-program-available-to-qualified-governments/*

[25] JPCERT/CC, NCSC–FI, and NCSC–NL

[26] *https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/index.cfm*

**Conclusion**

CVD is a process of coordinating human behaviors. Success at multiparty Coordinated Vulnerability Disclosure has more to do with understanding human communication and organization phenomena than with the technical details of the vulnerability. The hard parts are nearly always about coordinating the behavior of individuals and organizations with diverse values, motives, constraints, beliefs, feelings, and available energy and time. Technical vulnerability details may dictate the "what" of the response, but to a large degree, human organizational and social behaviors decide the "how." Optimal CVD operation requires carefully balancing "How much information should be released? To whom? And when?"

Thank you again for the opportunity to appear today before the Committee.

The CHAIRMAN. Thank you, Mr. Manion.

Dr. José-Marie Griffiths.

## STATEMENT OF JOSÉ-MARIE GRIFFITHS, PRESIDENT, DAKOTA STATE UNIVERSITY

Dr. GRIFFITHS. Chairman Thune, Ranking Member Nelson, and members of the Committee, I am José-Marie Griffiths, President of the Dakota State University in Madison, South Dakota. I like to think of us as the little university on the prairie. We are at once unexpected and different.

But I thank you for the opportunity to testify here today on this important topic.

In my written testimony, I try to identify the growing complexity of both our rapidly evolving technology environment and its increasingly global supply chain.

Within this grim problem context, what is the potential for addressing those problems?

Well, I believe that in the U.S. we have the people and organizations who can design and implement protective strategies and tactics to keep us safe. I have identified 10 strategies to move forward.

We need articulated standards, guidelines, and best practices, but these are a floor and not a ceiling, but they are a great start. The collaboratively developed and public NIST guidelines are far more effective than what we saw when Spectre and Meltdown were discovered. And the cybersecurity unit of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice has recently published a framework for a vulnerability disclosure program for online systems. This provides another excellent starting point for organizations to develop their own programs.

Coordinated vulnerability disclosure is most likely to minimize risk to technology users. Vulnerabilities privately disclosed and fixed through coordinated disclosure practices by all software vendors appear to work best. They do not create panic by early disclosure without solutions and do not alert criminal elements to current vulnerabilities. The balance between early public disclosure and tested solutions is tenuous at best. However, coupled with clear and consistent messaging, the potential damage can be minimized.

Two, the country needs to identify strong leadership to take control of planning and response, coordinate with others, and avoid the almost universal aversion to admitting weakness. Clarity and consistency in messaging are important but must be tailored to different audiences.

We need best practices for building secure products. A necessary but long overdue first step is a new and improved hardware/software contract. Both sides need to work to an interface, and that must be adequately specified for security purposes.

Four, we need a far more comprehensive and robust cyber education system in this country, both to develop professionals and to increase cyber knowledge of the general population.

We also need much better publicly required and shared cyber knowledge. We must leverage this country's intellectual assets, especially the human capital in U.S. universities.

Dakota State University in Madison, South Dakota was founded in 1881 and is a public university in the State university system. In 1984, a remarkably prescient South Dakota Governor and State legislature decided that South Dakota needed to dive into the technology revolution, and that DSU was the educational institution to lead the way.

DSU has developed into a powerhouse school of technology-intensive and technology-infused undergraduate through doctoral degree programs. The strength of our programs lies in the tight integration of computer science and cybersecurity principles and best practices, along with numerous experiential learning modules reflecting real world situations. Our students are also exposed to the ethical and social issues of technology development and use.

DSU's Beacom College of Computer and Cyber Sciences, one of its four colleges, has more than 1,000 students studying cyber operations and cyber defense, network administration, secure software engineering and development. We have recently developed the Madison Cyber Labs, what we call the MadLabs, a cyber research hub of research clusters that leverages the mad skills of our faculty staff and students in collaborations with government and corporate partners from local area partners all the way through to Federal agencies. The MadLabs is a reproducible model of using the intellectual resources of the university to engage in product and penetration testing, vulnerability assessments, and detection, remediation, and mitigation tool development. Eleven clusters across multiple disciplines, and more planned, combine disciplinary and cyber experts for targeted innovation.

Across U.S. universities, we have the potential to develop a nationwide distributed force that could be mobilized on short notice to address initial vulnerabilities and test solutions through multiple disciplines. And I should indicate that at the moment we have about 25 to 30 of our students and a number of faculty who have security clearances. We could easily build that up, but the security process takes time. But I just want you to know that we have that.

We must increase conservation of the cyber workforce. The shortage of skilled cyber professionals is seriously impacting the ability of organizations, including Federal and State governments, to protect our cyber resources. However, we cannot solve the workforce numbers problem until we are able to produce, recruit, and retain more cyber Ph.D.s to educate the next generation of cyber students.

We must encourage and attract more women and minorities into cyber careers.

And last but certainly by no means least, we must put into place expected cybersecurity protections and engagement across every in-

frastructure sector, power, water, communications, finance, agriculture, manufacturing, health care, and so on.

In conclusion, strong leadership is needed to set in motion and promulgate the strategies and tactics that will prevent our country from being engulfed by cyber vulnerabilities. There are individuals and organizations across the country, represented in part by those of us testifying today, who are eager to support and assist you in doing so. We are optimistic and encouraged that there are those of you who are stepping forward to protect the United States from cyber harm such that we can continue to harness cyber power for continued American success and innovation.

Thank you.

[The prepared statement of Dr. Griffiths follows:]

PREPARED STATEMENT OF JOSÉ-MARIE GRIFFITHS, PRESIDENT, DAKOTA STATE UNIVERSITY

**The Problem**

We have grown accustomed to attacks on computer systems that exploit the inevitable flaws resulting from vast conceptual complexity. Our computer systems are the most complex artifacts ever built, and the growth of complexity has far outstripped our ability to manage it. The problem is that we now live, breathe and have our being within a cyber universe driven by a critical and vulnerable multi-dimensional infrastructure. These dimensions include the vast range of products, providers, demands for increased proficiencies, the pervasiveness of cyber, and the enormous number of people now interacting with and dependent on our technology systems.

**Products**

The products of our cyber systems are muti-layered and varied, but generally they fall into one of the three tiers of hardware (the computer), firmware (permanent software programmed into the read-only memory of the computer), and software (applications loaded onto the computer). We have grown used to cyber attacks occurring at the software level.

However, Meltdown and Spectre were unusual in that they exploit flaws in the design of the complex interaction between the three levels of cyber products, and especially processes in the firmware, code that comes embedded in hardware devices. Cyber vulnerabilities in firmware are not only much harder to prevent or detect but also in most cases, unavailable to mitigate or remediate. The shock of the threat from this newly identified class of vulnerabilities comes from the sheer number of devices they impact and how persistent they will be over time.

A specific piece of application software can be removed from a computer and other applications on the machine will continue to work. Some firmware can be replaced but firmware can never bede entirely removed; without firmware code the hardware will not function. Changing the firmware of a cyber device may rarely or never be done during its lifetime; some firmware memory devices (especially Internet of Things devices like kitchen appliances or home security systems) are permanently installed and cannot be changed after manufacture. There are millions of diverse devices now in use across the planet with a wide variety of firmware embedded in them. Full protection can only come from replacing vulnerable equipment with new devices that contain fundamentally more secure chips and components. This replacement process will take years and will primarily depend on the devices' eventual retirement or demise. In the meantime, many devices will remain exposed to these niche, but potentially effective, cyber attacks.

**Providers**

No matter how you count them, there are many thousands of hardware/firmware providers globally and they compete fiercely. Third-party smaller specialized providers often operate with slim profit margins and are forced to cut corners to lower prices. Most marathoners have components from at least 10 different companies in as many countries. The screen, battery, microphone, camera, etc.—each requires highly specialized design and manufacturing. No one company—or country—can competitively produce more than a few of them. The Heritage Foundation, in their report on cyber supply chain security, noted that "Increased demand has led to acute competition and, consequently, more outsourcing and innovation to lower costs

and remain competitive. This can be seen in the U.S. computer manufacturing sector, which over the past five years has declined at an annual rate of 21.8 percent as computer manufacturing has increasingly moved abroad . . .the expanding market for computer products, innovative and useful software applications, and faster chip designs means that even these industries are seeing international competition and outsourcing that will likely grow over time."

The vast majority of users have no idea of the component makeup of a technology device, much less who made the piece or where. When users send a text, very few question who made the modem their marathoner is using to send it. However, the design and production of every piece of technology comes with certain goal and value choices. Is the goal of a company—or a country supporting that company—merely to manufacture and deliver a component piece of hardware and be done with it? Or is the goal of the company to embed within that piece of hardware the ability for the company—or country—to surrepetiously maintain access to that device, its user and activities, on an ongoing basis, using that information to further its own endeavors? The Internet of Things is exponentially expanding the number of cyber devices we rely on, from crockpots to cars. The computer screen on a fridge—are those in the home assuming that the device is built with a value of privacy for what goes on in someone's kitchen that the manufacturer doesn't share? Very often the users of a cyber device have very little understanding of its full capabilities. Recently a user who had installed an Internet-connected video doorbell in his home was amused by the actions of a delivery man who clearly did not understand the ramifications of the device. The user had a pleasant conversation from work over his smartphone connected to the home doorbell video cam, instructing the delivery man where to leave his packages. The delivery man dutifully did so, and then, apparently unaware that the user could still see him, walked over to the side of the house, dropped his pants, and urinated on a retaining wall. The delivery man's assumption of privacy was not shared by the device's design and functionality.

**Proficiencies**

We want our technology to be fast and faster, tuned to the vagaries of our personality, workstyle, activities and preferences, and easy to use. The less we have to figure out or do to make it work, the better. But every added cyber proficiency comes with a set of decisions made by someone about access, privacy, control, and more. Autonomy means freedom from the will of another. But every autonomous device is based on a set of assumptions defined and built in by someone. Do we know—or care—who that someone is, and the basis for their choices and assumptions?

**Pervasiveness**

Cyber devices are now embedded in almost every aspect of work and play, and thus we are now facing serious vulnerabilities in our supply chain. Rapid technological advancement and the constant rush to market with added functionalities has resulted in complex and sophisticated integrated circuits now virtually ubiquitous in every device, in every country. They are relied on to control critical infrastructure subsystems such as power, finance, communications, transportation, healthcare and agriculture.

In the past, attackers worked to exploit security gaps that might exist in corporate of national defense IT systems, today the gaps they are exploiting are in the integrity of the supply chain. As the threat landscape evolves, it is essential for an effective supply chain security strategy to proactively minimize exposures throughout the lifecycle from cradle (secure integrated circuits (IC) design, fabrication and manufacturing) to grave (ethical e-waste disposal) and everything in between. Modern IC computer chips are enormously complicated. For example, an average desktop computer chip has over 1 billion transistors. In addition, the manufacturing process is not entirely predictable and there can be significant variances in the chips produced. The complexity of both design and production create multiple opportunities for practically undetectable cyber infections at the very beginning of the supply chain.

Cyber systems are increasingly complex and the dependency on third party libraries of software code in the supply chain seems to be growing. For example, most of today's integrated circuits use at least some common off-the-shelf components (COTS), mostly in the form of third-party intellectual property. This should be considered a top security issue because much of it is integrated into the chip as trusted code, regardless of whether it actually is. As the Internet of Things/Everything, Cloud of Everything (IoT/E, CoT) evolves rapidly to be autonomous and inexpensive, the use of COTS will expand even more dramatically and the need to encapsulate this potential security risk will be even more pressing. Security issues with COTS include undocumented or unverified code and sloppy programming that opens de-

vices to intrusion. This makes it very difficult, if not impossible, for an organization to test all of the software code they actually use and potentially ship to a client. There have been several notable supply chain incidents of companies unknowingly distributing malware with dire impacts. However, it is not at all clear where the responsibility for ensuring safe software code lies. Is it the obligation of the third party company or the company or organization that used and distributed dangerous code? And who decides? We do not yet have best practice guidelines for these types of issues, but they are far overdue.

The risk of dangerous firmware can be the most difficult to defend against. Firmware is embedded in hardware and can be put there either at the point of creation or at some other stage as it moves through the supply chain. This malevolent code can be extraordinarily difficult to detect. Some contain logic bombs that are set to go off at a designated time in the future, or only when a certain event occurs to trigger them. There is great potential for this malicious code to be used to damage or destroy key components of critical infrastructure, which could result in high economic costs or even political turmoil.

The only way to ensure absolute cyber safety would be able to ensure that the entire supply chain of relevant electronic components occurs in the United States and is performed by carefully screened and vetted, trustworthy employees. The system would need to include all stages of the supply chain from design, creation, fabrication, assembly, to distribution. Strict surveillance of the manufacture of such electronics would need to occur, and protocols would need to then be in place to ensure that no modifications have been made and that the electronics are created exactly to specifications. Unfortunately, this is simply not pragmatic as the costs of having to do all of this, including manufacture, would be astronomical and unsustainable without years of public investment. Presently most cyber device manufacturing occurs in Asia at very inexpensive rates. U.S. tech firms would never be able to compete in a world market. Furthermore, because most electronics are created, assembled, and distributed outside the this country, U.S. Government regulated security processes would be irrelevant for the vast majority of the supply chain.

The statistics of the pervasiveness of cyber today are staggering. There are currently more than 8 billion connected devices globally, according to a new report by IHS Inc. That works out to four devices for every household in the world. As of 2014 there were more cyber devices than people in the world, including a growing number—about 250 million—that only communicate with other machines. And all of these devices are multiplying five times faster than the human population is (a rate of about two people per second, or 1.2 percent annually). Over 3.8 billion people use the Internet today, which is 40 percent of the world's population, and we are busy users. MG, a website design and online marketing company published a set of technology facts and stats that includes: "More than 570 new websites are created every minute; there are over 3.5 billion searches per day on Google; every minute 24 hours of video is uploaded to YouTube; more video content is uploaded to YouTube in a 60-day period than the three major U.S. television networks created in 60 years; 340,000 tweets are sent per minute and 500 million tweets are sent per day; there are more than 300 million photos uploaded to Facebook every day with 800 million likes per day." Not only are cyber systems becoming more complex, that complexity is multiplied millions of times over by the pervasiveness of their presence.

**People**

The human element of the problem is perhaps even a greater challenge than the number of devices involved. Getting users to click on automatic software updates has only ever been marginally successful, even when enormous efforts are made to reach those users and explain the importance of the update in protecting their machine and data. The human element in the mix can extend the lifecycle of exploited vulnerabilities, not only through noncompliance but also value tradeoffs. For example, users sometimes decide not to install patches and updates if a side effect of the protection is a hefty performance degradation. Some of the initial firmware code distributed to address the Spectre/Meltdown vulnerabilities resulted in machines refusing to boot up and others slowing down by as much as 30 percent. These problems were quickly resolved, but they demonstrate the risks and challenges of fixing complex system problems. To explore potential impacts of running non-remediated software, researchers recently set up a set of computers, each running a different operating system software, many no longer the current version. They then connected the machines to the Internet and monitored how long it took before the machine experienced a successful cyber attack. One machine running (outdated) OS software still in use in over 80 percent of large corporations lasted only 13 seconds before experienced a cyber attack and was compromised. Writing replacement non-vulnerable

firmware code and getting it installed in every existing device that needs it around the world is even more challenging. Meltdown and Spectre exposed hardware/firmware design assumptions that were reasonable when they were created. However, technological sophistication and knowledge has now developed to the point that the basic firmware approach and architecture can now be exploited to trick the computer into revealing sensitive data, like user names and passwords.

After the Spectre and Meltdown vulnerabilities were discovered, researchers anticipated that similar flaws would eventually be revealed as well, and that has happened recently. New categories of security exploits often follow a predictable lifecycle, which can include new derivatives of the original exploit. Sometimes the fix for these derivatives benefits from the fixes created for the original exploit. However, it also complicates and extends mitigation and remediation. IT professionals have often likened this to the "whack the mole" game: no sooner is one security breach beaten down but a new one erupts through a different hole.

**Potentials**

Within this grim problem context, what are the potentials for fixing the problem? I believe that in the U.S. we have the people and organizations who can design and implement protective strategies and tactics to keep us safe. But we need both carrots and sticks.

We need articulated standards, guidelines and best practices. These are the floor not the ceiling, but it's a good start. The collaboratively-developed and public NIST guidelines are far more effective than what we saw when Spectre/Meltdown was discovered: corporations circling the wagons, hiding what was going on and trying to fix it by themselves. That was not totally a self-serving move—you don't want adversaries to know your flaws before your fix—but it also showed that we need best practice established standards, participants, and processes for responsible coordinated disclosure. An increasing number of organizations are developing and adopting formal or informal vulnerability disclosure programs. Formalized programs include published policies describing how information about security vulnerabilities will be received and addressed, and how vulnerabilities may be disclosed to affected parties and/or the public. These policies may also describe authorized methods for discovering vulnerabilities in the organizations systems, services and products and how—and how quickly—a component vendor must respond. For example, Google's Project Zero gives vendors 90 days to respond and implement a fix before Google goes public with a vulnerability that they discovered. This puts the pressure on the vendor to respond, and in a timely manner. The Cybersecurity Unit of the Computer Crime and Intellectual Property Section, Criminal Division of the U.S. Department of Justice has recently published *A Framework for a Vulnerability Disclosure Program for Online Systems* which provides an excellent starting point for organizations to develop their own programs. Coordinated vulnerability disclosure is most likely to minimize risk to technology users.

Vulnerabilities privately disclosed and fixed through coordinated disclosure practices by all software vendors appear to work best. They do not create panic by early disclosure without solutions and do not alert criminal elements of current vulnerabilities. The balance between early public disclosure and tested solutions is tenuous at best. However, coupled with a clear and consistent messaging, the potential damage can be minimized.

Who to do this? The country needs to identify a strong leader to take control of planning and response; coordinate with others and avoid the almost universal aversion to admitting weakness. Clarity and consistency in messaging are important but must be tailored to different audiences. We need to pull together and structure government, corporate, and academic/research oversight and engagement in cyber security. And from those collaborations we need a system of rewards for good cyber citizens and punishment for rogues.

We need best practices for building secure products. Given the conceptual complexity of today's computer systems, perhaps the ultimate solution would be the automated evaluation of designs with the aim of mathematically proving that under all circumstances a design will behave in a way that is considered secure—in particular by not leaking secret data. This is a long range project but significant improvements could be achieved through partial results in the form of weaker properties and by establishing desired properties in a less rigorous fashion. A necessary and long-overdue first step is a new and improved hardware-software contract. Both sides need to work to an interface—the instruction set architecture which presents the contract between hardware and software functionality, and it must be adequately specified for ensuring security.

We need a far more comprehensive and robust cyber education system in this country, both to develop professionals and increase the cyber knowledge of the gen-

eral population. And that educational program must include consideration cyber ethics and commitment to individual and corporate responsibility and societal cyber participation. Traditional university computer science programs tend to not delve too deeply into software development, let alone secure software development. While the trend seems to be changing, this has created a significant security skills gap in the current cyber workforce. Organizations are struggling as to how to address this with their current workforce. It is often difficult for a company to readily identify the skills of their employees to address gaps in organizational cyber security skill and systems.

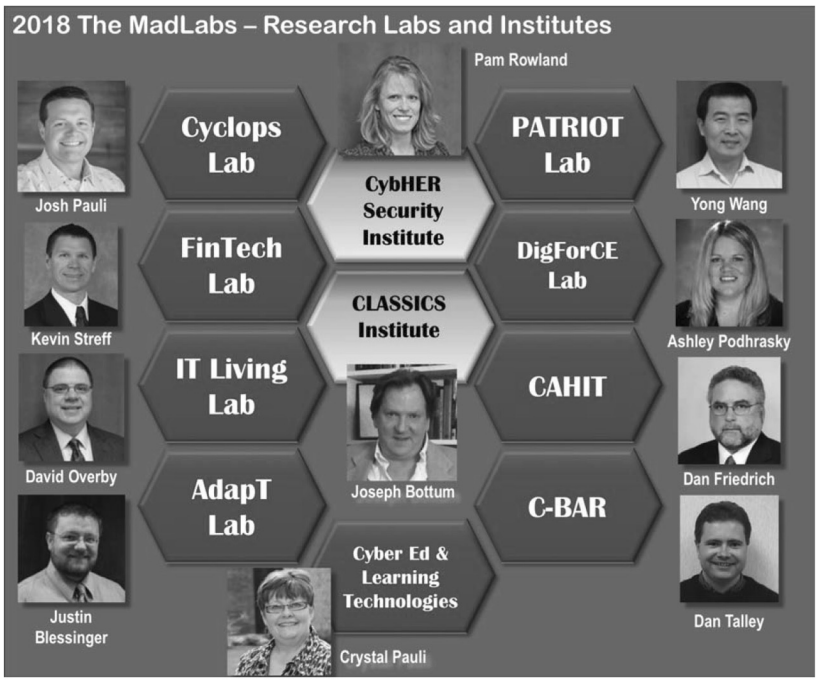
We also need much better publicly required and shared cyber knowledge. The FDA requires that food manufacturers list a product's ingredients and its country of origin. Reading labels I can make an informed decision—is the less expensive brand worth it if it is full of chemicals and preservatives, or comes from a country whose values the buyer opposes? We have no such listing requirements for the technologies we buy. Why not?

**Properties**

Problems and potentials lead to where the rubber meets the road—the needed properties and resources to move forward. We must leverage this country's intellectual assets, especially the human capital in U.S. universities.

Dakota State University (DU) in Madison, South Dakota, was founded in 1881 and is a public university in the state South Dakota university system. In 1984, a remarkably prescient South Dakota state legislature decided that South Dakota needed to dive in to the technology revolution, and DU was the educational institution to lead the way. DU has developed into a powerhouse school of technology-intensive and technology-infused undergraduate through graduate degree programs. DSU's Beacom College of Cyber and Computer Sciences, one of its 4 colleges, has over a thousand students studying cyber defense; secure software development and engineering; computer science principles and best practices; and the ethical and social issues of technology use. DSU has multiple Academic Center of Excellence designations in education, research, and regional resource development from the U.S. National Security Agency and Department of Homeland Security. The university's cybersecurity students have competed and won notable national titles against universities ten times DSU's size. The university continues to graduate an impressive stream of much-in-demand tech savvy professionals, who have landed jobs in top government, education, and business and industry organizations, nationally, and internationally. Small in size, DSU has become a big player in cyber workforce development and research and development.

DSU has developed the Madison Cyber Labs—MadLabs—a cyber research hub of research clusters that leverages the "mad skills" of our faculty, staff and students in collaborations with government and corporate partners, from local and area partners all the way through Federal agencies. The MadLabs is a reproducible model of using the intellectual resources of a university to engage in product and penetration testing; vulnerability assessments; and detection, remediation, and mitigation tool development. Ten clusters across multiple disciplines—and more planned—combine disciplinary and cyber experts for targeted innovation. Present MadLabs labs and institutes include:




- *Cyclops Lab* (Cyber Classified Operations) The Cyclops lab is a secure facility for the conduct of classified, sensitive and confidential research and development. Cyclops is working Federal agencies and private corporations on multiple cyber security projects.
- *PATRIOT Lab (Protection and Threat Research for the Internet of Things)* The PATRIOT Lab is focused on the security of the devices and related cloud services that comprise the Internet of Things (IoT). The structure and nature of IoT devices may make them an important vector for malicious attacks and the Patriot Lab researches and develops solutions for these vulnerabilities.
- *FinTECH Lab (Financial Technology*) The mission of the FinTech MadLab is to develop software and processes that support the security and reliability of the financial services industry. Initially, this will include addressing Automated Clearinghouse (ACH) fraud and wire fraud but will expand to many financial transactions. The FinTECH MadLab will support the traditional financial platforms and emerging technologies such as Block chain, digital currency and online platforms. An industry advisory board will guide the development of this MadLab.
- *DigForCE Lab (Digital Forensics for Cyber Enforcement)* The digital forensics MadLab is a resource for government agencies, businesses and attorneys that have a need for the extraction, preservation and analysis of data from digital devices. This includes data from traditional devices like computers and phones and non-traditional devices such as gaming consoles. The digital forensics MadLab will also provide staff training for various organizations and a statewide call center for businesses and individuals to use for cybersecurity questions and analysis including a safe way of forwarding suspect e-mail, files and documents.
- *Campus IT Living Lab (DSU's IT infrastructure protection and related research)* The Campus IT Living Lab performs testing on technology hardware and software solutions to determine if the solution can be implemented in a campus environment. Some of these areas include IT infrastructure, classroom multimedia, and facilities. Utilizing the Campus Living IT Lab, Information Technology Services (ITS) will collaborate with DSU faculty and students on projects to determine the viability of different technologies in a campus environ-ment.

- *CAHIT (Center for the Advancement of Health Information Technology)* The mission of CAHIT is twofold: First CAHIT intends to research the interplay of "aging in place" and the Internet of Things (IoT). Secondly, CAHIT will address the unique security concerns of connected medical devices, both in the home and in medical institutions. CAHIT will utilize their existing industry partnerships and their strength in information security and information analysis in developing their research proposals.
- *AdaptT Lab (Research in Adaptive Technologies)* Working collaboratively in teams the AdapT Lab researchers work to creatively explore, develop, test and modify real-world assistive technologies that can be used to break through barriers, digital or physical. We are also committed to educate others to become knowledgeable and skilled in using and developing assistive technologies in their fields, to increase employment and life participation for those experiencing disabilities or constraints.
- *C–BAR Lab (Center for Business Analytics Research)* The C–BAR MadLab is a research and analysis platform for the College of Business and Information Systems (BIS). The goal is to make the expertise of BIS faculty available to businesses organizations, education entities, and government agencies to assist with their projects and apply analytics to assist in solving problems.
- *Cyber Education and Teaching Technologies Lab* The mission of the Education MadLab is to expand Cyber Education to K–12 teachers and students across the state of South Dakota. The lab will utilize DSU faculty to provide this education within the K–12 districts and on the campus of DSU. The Education MadLab is partially funded by an NSA grant supporting DSU as a Regional Resource Center.
- *CybHER Security Institute (Women in Cyber Security)* CybHER's mission is to empower, motivate, educate, and change the perception of girls and women in cybersecurity. By providing resources for girls from middle school through collegiate programs and into professional careers, CybHER will allow women to foster positive and encouraging relationships within this industry through original and curated content that educates and motivates women. Ultimately, our goal is to increase diversity by introducing more girls to cybersecurity, who will then transition to women in collegiate programs, and highly trained professionals.
- *CLASSICS Institute (Collaborations for Liberty And Security Strategies for Integrity in a Cyber-enabled Society)* The Mission of the CLASSICS Institute is to raise the deep questions about the cyber revolution including those related to: Artificial Intelligence (AI); Security; Privacy; Integrity; and Ethics. The institute will consider these issues in the context of how they relate to public policy.

Across U.S. universities we have the potential to develop a nationwide distributed force that could be mobilized to address initial vulnerabilities and test solutions through multiple disciplines.

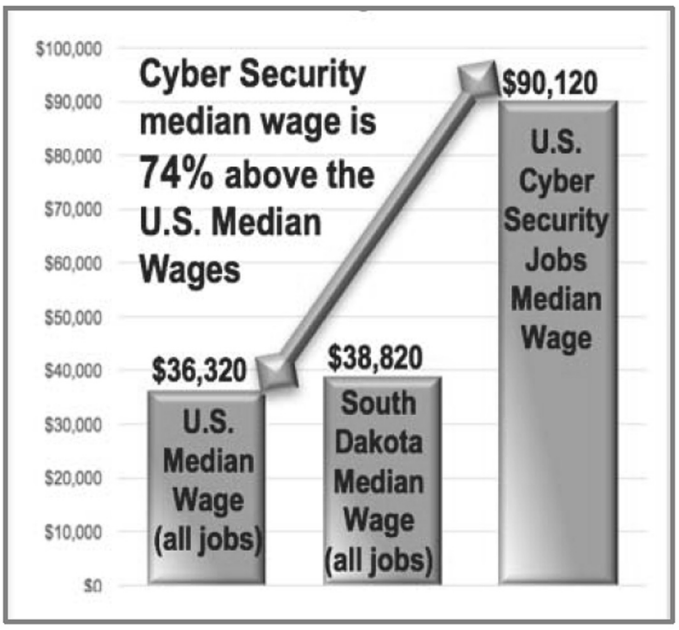
We must increase cultivation of a cyber workforce. The shortage of skilled cyber professionals is seriously impacting the ability of organizations—and Federal and state government—to protect our cyber resources. As of next year, 2019, it is expected that there will be more than 2 million unfilled cybersecurity jobs in the world. Eighty-four percent of U.S. companies reported that half or fewer of applicants for their cyber security jobs were qualified. The talent pool of cyber warriors is not keeping up with the growing pace and severity of cyber warfare.

Across the country and the world, increased education is associated with both higher wages and lower unemployment. The greatest barrier to U.S. economic success and growth in the 21st century will be a workforce dominated by those without post-high-school education. Research shows that technology-centric professionals and endeavors—Dakota State's mission focus—have an outsized impact on economic growth, because they provide better-paying, longer-lasting jobs than other start-ups, and they contribute more to innovation, productivity, and competitiveness. There are significant differences between tech-based start-up companies and the typical start-up companies:

| Firm Characteristics | Tech-Based Start-Ups | Typical Start-Ups |
|---|---|---|
| Examples of Businesses | Biotech, IT products or services | Restaurants, laundromats |
| Growth Path | Large potential for significant employment and revenue growth | Addition of few jobs in first few years, then bankruptcy |
| Job Creation | Tend to employ more high- and semi-skilled workers | Tend to employ more semi- and low-skilled workers |
| Wages | Pays more than twice the national median wage | Pays less than the national median wage |
| Job Multipliers | Creates up to five indirect jobs in other industries | Creates little to no net new jobs |
| R&D Investments | Invests heavily in R&D | Little to no R&D investment |
| Trade | Focused on trade with international markets | Sells predominately in local markets |

*https://itif.org/publications/2017/11/28/how-technology-based-start-ups-support-us-economic-growth*

The Information Technology and Innovation Foundation, ranked as one of the world's leading science and technology think tanks examined the top ten tech-centric manufacturing sectors and services in terms of their contributions to the U.S. economy. They found that across the board tech firms contribute to the economy and economic growth of a region far beyond their comparable size. One tech job generates at least 5 other jobs in the community. For example, while only 3.8 percent of U.S. companies are tech-centric and they account for only 3.6 percent of U.S. jobs, these companies account for 27.2 percent of U.S. exports, critical to business success in the new global economy. The importance of STEM professionals as key to economic success continues to grow. 66 percent of all DSU degree-and certificate-seeking students are in STEM programs. It is interesting to note that according to the U.S. Bureau of Labor Statistics, nationally seven out of the largest ten STEM occupations are technology-centric.




DSU's surging enrollment reflects an understanding that tech professionals are in demand and the jobs are good—good working conditions, high salaries, and stable

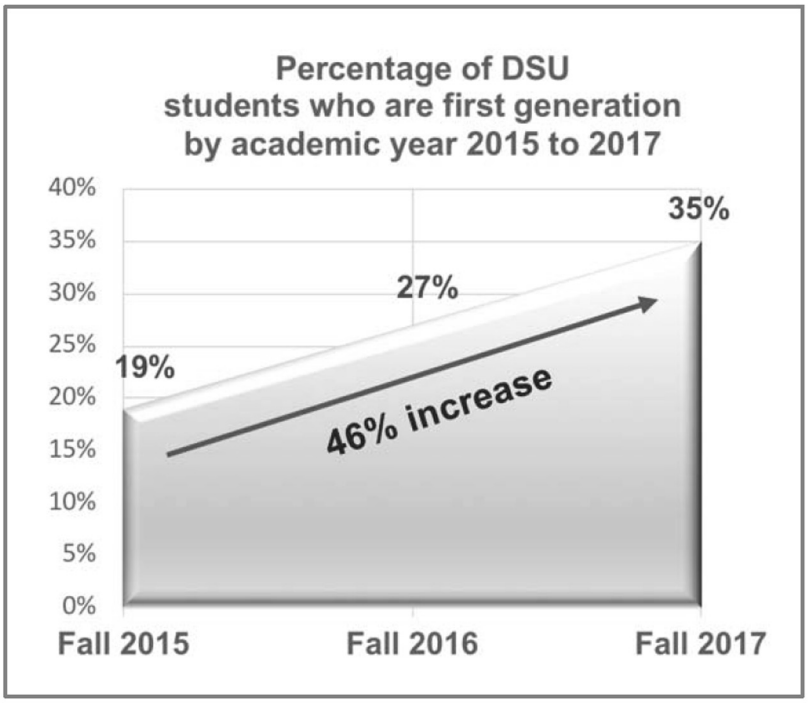
employment. However, unless grant and scholarship funding is increased—significantly—for all of the country's high school graduates, this trend will not be sustained. Three factors are especially indicative at DSU of the increasing need for additional funding for students to complete a college degree: dropping Pell grant recipient numbers; the number of students qualifying for subsidized loans compared to the number receiving South Dakota's state-funded needs-based scholarship; and the increasing number of first-generation students.

The Pell Grant program is an indicator of the number of students from lower income families pursuing a college education. According to the Free Application for Federal Student Aid (FAFSA), most Pell grant money goes to students with a total family income below $20,000. The maximum Pell Grant award in 2016–17 in the U.S. covered just 29 percent of average in-state public university tuition, fees, room, and board. This is in stark contrast to the Pell Grant award in 1997–98, when the award covered 87 percent of average in-state public university tuition, fees, room and board. This means that at a time when young adults more than ever need a college education to access a good job and the U.S. needs a college-educated workforce to stay competitive and sustainable, Federal support has gone from covering almost all of the cost of a college education to covering less than a third. These days qualifying for the maximum Pell Grant award doesn't even get a student half way to covering the expense of their degree.

DSU's percentage of Pell grant recipient students (as a percentage of the entire student headcount) has dropped 8 percent in the last two years, and we expect that trend to continue. According to the College Board, in 2016–2017 32 percent of U.S. college undergraduates were receiving Pell grants. The conservative estimate is that 50 percent of high school graduates in 2015–2016 would have qualified for a Pell grant. When even the maximum Pell Grant only gets a student a little more than a third of the way to paying for their schooling, many young adults are discourage from even attempting to finance a college education.

Another indication of the growing financial need of college students is the number who qualify for subsidized loans versus those who receive monies from state-funded support, for example the South Dakota Needs-Based Scholarship Fund. Federal recipient qualifications for subsidized loans are based on the student's available resources, which includes a calculation of their Estimated Family Contribution (EFC). Subsidized loan qualification thus does identify those students who most likely come from lower-income homes. Two years ago, 758 DSU students from South Dakota qualified for subsidized Federal loans. However, there was only enough money in the South Dakota Needs-Based Scholarship Fund to provide scholarship monies for 21 of those 758 students, or a minute 3 percent of those who likely qualified actually received state-funded support for their education. Many states across the country are in even greater more dire straits trying to provide support for students' higher education, especially following the dramatic cuts in state budgets during the recent recession.

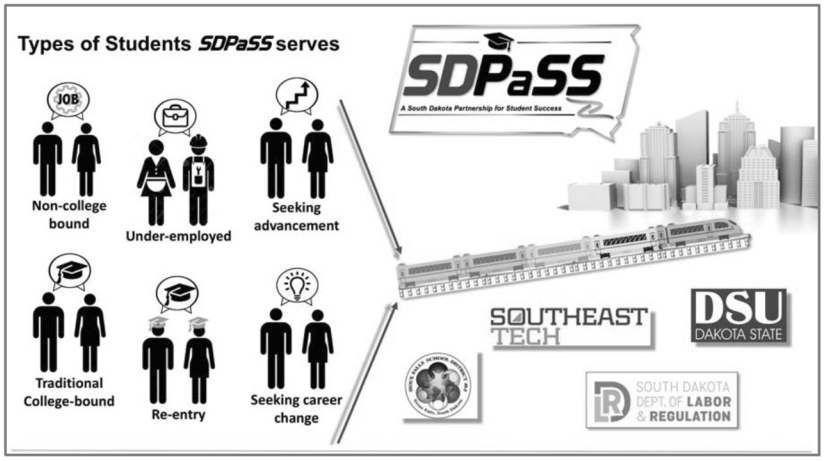
Dakota State is indicative of those universities that are working hard to recruit and retain first-generation students, those who are the first in their families to obtain a college degree. From Fall 2015 to Fall 2017 DSU's population of first-generation students has increased 46 recent.

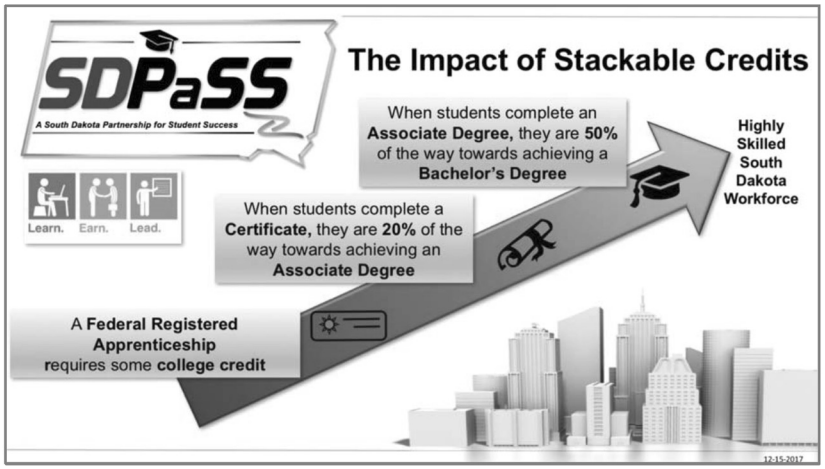



While certainly not all first-generation students qualify for need-based support, according to the Economic Policy Institute "Americans with no more than a high school diploma have fallen so far behind college graduates in their economic lives that the earnings gap between college grads and everyone else has reached its widest point on record." Those holding only a high school diploma have actually seen their average salary decrease by an average of 3 percent. There are nearly 1.5 million fewer office administrative and clerical jobs now than there were before the recession, according to an analysis by Georgetown's Center on Education and the Workforce. Manufacturing employment is also 1.5 million lower than when the recession began in 2007. The construction industry had offered a lifeline to many high-school educated workers, particularly men, during the housing boom in the 2000s. Yet construction now employs 840,000 fewer people than it did nine years ago. Since the recession, the fastest-growing industry for high school-only grads has been a mostly low-paying sector that includes restaurants, hotels, and amusement parks, according to Georgetown's analysis. Therefore, it is a reasonable conclusion that generally first-generation students will have a significantly lower EFC than non-first-generation students and need more financial support to obtain a college degree.

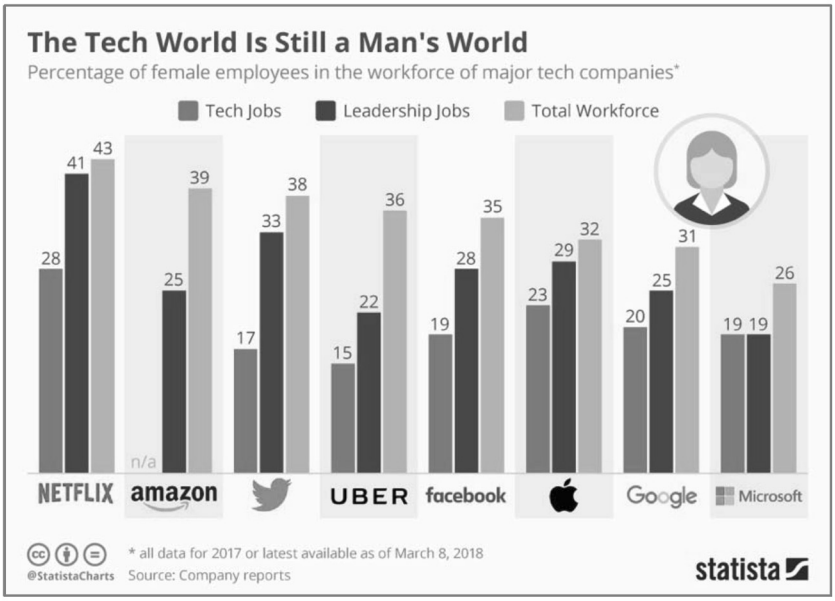
South Dakota has set the ambitious goal of by 2025 to have 65 percent of the state's under-35 workforce have some post-secondary education. The state has launched *SDPaSS,* the South Dakota Partnership for Student Success, a system of step-wise stackable cyber education programs and credentials that make it easier for high school graduates to continue their education and qualify for higher skill better paying jobs while meeting the needs of companies for cyber professionals. Those already in the workforce can access *SDPaSS* to retool or advance their career. A layered educational program ensures that achievement at one level, *e.g.,* obtaining a professional certificate, is acknowledged and the course work directly flows into the requirements of the next academic level, *e.g.,* an associates degree. The four core partners—Dakota State University, Southeast Tech, the Sioux Falls School District, and the South Dakota Department of Labor and Regulation (DLR)—are collaborating with businesses to design, refine, and implement the program. This collaboration is essential to ensure that the program stays relevant to evolving commercial trends, cyber innovations, and workforce needs. *SDPaSS* components include:

- Internships in business/industry supervised by faculty at Dakota State University, Southeast Tech or the Sioux Falls School District
- Registered apprenticeship connections and guidance through the South Dakota DLR
- Academic certificates in cybersecurity, or network services or software development
- Associate degrees in network and security administration (DSU and Southeast Tech), software development (DSU), and software support (Southeast Tech)
- DSU baccalaureate degrees in network & security administration, cyber operations or cyber defense.




We must get more women into cyber careers. We will never have enough cyber professionals if the field remains so male dominant. 77 percent of women in the workforce have reported that no high school teacher or guidance counselor ever mentioned cyber security as a possible career. The MadLabs has the CybHER Institute, which has reached over 10,000 Kindergarten through 12th grade girls, educating and exciting them about cyber careers for women. CybHER has held over 130 summer camps, events, presentations, and programs in the last four years, and they are constantly expanding their impact.


However, we cannot solve the numbers problem, *i.e.,* not enough cyber professionals, until we are able to recruit and retain more cyber Ph.Ds as faculty to educate the next generation of students. All university cyber programs are facing tremendous threat in their ability to fulfill their purpose because of the increasing challenges of recruiting and retaining tech-skilled faculty. Tech savvy, especially computer and cyber sciences faculty, are few in number and have multiple lucrative job options outside higher education. The publication *Inside Higher Ed* noted recently that it is a supply and demand story on steroids.

On the supply side, U.S. universities are graduating relatively few Ph.D.s in computer and cyber sciences. According to the Federal Integrated Postsecondary Education Data System (IPEDS) only 2 percent of all degrees conferred in the cyber sciences are doctorates, compared to 8 percent in the sciences, math, and engineering fields. Only 18 percent of these PhDs are taking teaching positions in higher

education; another approximately 10 percent take non-teaching positions at universities, generally in full-time research.

On the demand side, according to many estimates, with a doctoral degree in any of the cyber sciences an individual can on average earn up to five times more in industry than they can as a university professor. Over the course of a career the salary gulf widens. As a result, market competition continues to grow for any cyber sciences professional interested in teaching. A recent report for the National Academies of Sciences, Engineering and Medicine revealed that between 2009 and 2015 there was a 74 percent increase in the number of cyber sciences bachelor's degrees awarded across U.S. colleges and universities. Doctoral-granting institutions as a group reported a 300 percent increase in cyber sciences degrees awarded. Clearly, students are flocking to tech-centric degree programs, just as they are at Dakota State, where the university has seen dramatic increases in enrollment over the last few years. The career opportunities created by achieving a degree in a tech field are unquestionable. Basically 100 percent of DSU's cyber program graduates move immediately into professional-level cyber jobs—well-paying interesting employment in excellent government or corporate organizations. (DSU's cyber graduates are split about 50/50 between government and corporate placements.) Those who don't move into a career placement have either enrolled in advanced degree programs or for some personal reason are not immediately purusing employment.

However, across the U.S. cyber sciences faculty hiring to teach these students is falling farther and farther behind. The Computer Research Association's comprehensive Taulbee Survey reported that 1,780 Ph.D. degrees in cyber sciences were awarded in 2015. Given that only 18 percent of these Ph.D.s took teaching positions in higher education, there were only 320 new Ph.D.s available to fill faculty slots in the 1,577 institutions that offer cyber sciences degrees. The National Academies report extrapolated this out to highlight that those 1,577 institutions can therefore expect to hire 0.2 new Ph.D.s per year, or one Ph.D. every five years. Eighty percent of new Ph.D.s who do move into teaching positions do so at research-intensive institutions. That means that colleges and universities without a robust research environment and community will be doing well to hire one new cyber sciences Ph.D. every 27 years. This is another reason why Dakota State launched the MadLabs. DSU's R&D endeavors are not only critical to productively leveraging DSU's intellectual assets to contribute to South Dakota's economic development but also to strengthen the university's ability to recruit and retain cyber-centric faculty.

A recent study in Computing Research News found that 18 percent of college and university cyber science faculty searches in 2017 failed entirely. Survey respondents at 155 institutions reported looking for 323 tenure-track positions and filling just 241. Even Stanford University, where computer science is the number one major and research opportunities abound, is experiencing the tenure-track faculty shortage. Stanford reports that in the last decade the university has lost twice as many faculty members to other jobs as it has in the previous 40 years.

Finally, we must put into place expected cyber security protections and engagement across every infrastructure sector. Utilities, manufacturing, education, agriculture and food safety—cyber defense and cyber warriors must become as ubiquitous as the technology that requires their aid.

**Conclusion**

There have been prophets in our midst for decades warning of this technological tsunami, and powerful cyber waves are now pounding the shores of almost every human endeavor across our country and around the world. Cyber threats to our Nation's critical infrastructure are real and a serious problem. However, the United States also has the potentials and properties to fix it. This country needs leadership to set in motion the strategies and tactics that will protect our enterprises from being engulfed by cyber vulnerabilities. There are individuals and organization across this country, represented in part by those testifying today, who are eager to support and assist congressional efforts to provide that leadership. We are optimistic and encouraged that there are those who are stepping forward to protect the United States from cyber harm such that we can continue to harness cyber power for continued American success, innovation, and world-leading life, liberty, and the pursuit of happiness.

The CHAIRMAN. Thank you, Dr. Griffiths.

Mr. Sridharan.

**STATEMENT OF SRI SRIDHARAN, DIRECTOR, FLORIDA CENTER FOR CYBERSECURITY, UNIVERSITY OF SOUTH FLORIDA**

Mr. SRIDHARAN. Chairman Thune, Ranking Member Nelson, and distinguished Committee Members, my name is Sri Sridharan. I am the Director for the Florida Center for Cybersecurity hosted at the University of South Florida. Thank you for inviting me to provide testimony on cybersecurity vulnerabilities, lessons learned from Spectre and Meltdown.

While the Spectre and Meltdown vulnerabilities are ostensibly the topic of today's hearing, the truth is in the world of cybersecurity, they are old news. They have been discovered, researched, and patched. What they represent, however, is something of far greater concern: the multitude of unknown vulnerabilities that most assuredly still lurk in cyberspace. This, of course, poses a threat to our national security.

The Meltdown and Spectre vulnerabilities existed for 20 years, built into the chip design. It took us 20 years to discover a vulnerability that affects nearly every modern operating system and the most popular computer processors used in millions of devices. A foreign threat actor could have quietly exploited one or more of these vulnerabilities without our knowledge, and they could have been doing so for 20 years.

And although the vulnerabilities are now known, we are still not safe because statistically at least 25 percent of users do not apply the patches needed to mitigate these vulnerabilities.

My point is that Meltdown and Spectre are symptoms of a much larger problem. Cybersecurity is a race with no finish line. The question is not if vulnerabilities exist. They do. They are out there, and as fast as we discover and patch them, new ones are introduced. It is simply the nature of rapidly advancing technology. The real question is who will find it first.

We are living in the Information Age. Our information, our currency, our medicine, our economy, and our secrets are digitized and so is our conflict. The nation state threats have already fired the first shots of cyber warfare with the U.S. We must act now to ensure that our cybersecurity forces, military, public, and private, are prepared to win these battles.

We need a large cybersecurity workforce. We need more programs, more camps, more competitions that educate kids and inspire them to pursue cybersecurity careers. We need to create a clear path from education to employment so that people of all skill levels can easily transition into cybersecurity careers. If you build it, they will come. But people need to know these opportunities exist, which brings me to my final topic of communication.

Here is the critical issue: the lack of a clear, rapid report-and-respond mechanism for national cybersecurity threats. Currently multiple organizations bear responsibility for national cybersecurity defense, DHS, NSA, NIST, the military, the FBI, and so on. To which of these organizations should the researchers have reported their discovery? When a vulnerability is reported, what is the mechanism to alert critical areas of our government?

In the case of Spectre and Meltdown, industry responded quickly with patches and solutions but only after they were made aware

of the problem. We can get a better handle on cyber hacks and breaches if we are more proactive than reactive. To this end, we need, one, a larger cybersecurity workforce. We are dealing with a severe shortage today. Create awareness, provide education and training to businesses and citizens and teach to practice good cyber hygiene. Better coordination and dissemination of critical information. To empower and hold accountable certain government organizations that can navigate through the complex bureaucratic process. To act with a sense of urgency, and last, to let the government play an important coordinating role.

Chairman Thune, Ranking Member Nelson, and esteemed Committee Members, I thank you for allowing me to share my thoughts. I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Sridharan follows:]

PREPARED STATEMENT OF SRI SRIDHARAN, DIRECTOR, FLORIDA CENTER FOR CYBERSECURITY, UNIVERSITY OF SOUTH FLORIDA

Chairman Thune, Ranking Member Nelson, and distinguished Committee members,

My name is Sri Sridharan, and I am the Director of the Florida Center for Cybersecurity hosted at the University of South Florida. Thank you for inviting me to provide testimony on Cybersecurity Vulnerabilities—Lessons Learned from Spectre and Meltdown.

While the Meltdown and Spectre vulnerabilities are ostensibly the topic of today's hearing, the truth is, in the world of cybersecurity, they are old news. They have been discovered, researched, and patched. What they represent, however, is something of far greater concern: the multitude of unknown vulnerabilities that most assuredly still lurk in cyberspace, waiting to be discovered and potentially exploited by cyber thieves, especially foreign nation-states. This, of course, poses a threat to our national security.

The Meltdown and Spectre vulnerabilities existed for twenty years, built into the chip design. It took us twenty years to discover a vulnerability that affects nearly every modern operating system and the most popular computer processors, used in millions of devices. Unfortunately, we have no way of knowing if it was, in fact, the researchers who found it first. The attacks that exploit these vulnerabilities are difficult to detect. A foreign threat actor could have quietly exploited one or more of these vulnerabilities without our knowledge, and they could have been doing so for twenty years.

And, although the vulnerabilities are now known, we are still not safe because, statistically, at least 25 percent of users do not apply the patches needed to mitigate these vulnerabilities. That's what we saw with the WannaCry ransomware attack last summer. Microsoft discovered a vulnerability and issued a patch in March 2017, however not everyone updated their systems. On May 12, 2017, foreign nation-state threat actors unleashed a ransomware attack designed to exploit that vulnerability that infected 300,000 computers in 150 companies and even interrupted the operations of Britain's National Health Service. One month later, despite worldwide media attention and additional updates from Microsoft, another foreign nation-state—later identified as Russia—used the same vulnerability to attack computers in several countries including the U.S., with most infections targeted at Ukraine.

My point is that Meltdown and Spectre, WannaCry and NotPetya, are symptoms of a much larger problem: cybersecurity is a race with no finish line. The question is not 'if' vulnerabilities exist. They do. They are out there, and as fast as we discover and patch them, new ones are introduced. It is simply the nature of rapidly advancing technology. The real question is: who will find it first?

We are living in the Information Age. Our information, our currency, our medicine, our economy and our secrets are digitized, and so is our conflict. Some recent headlines:

- *Cyberscoop,* June 2017, "How China's cyber command is being built to supersede its U.S. military counterpart;"
- *The Independent,* January 2018, "Cyberwarfare with Russia 'now greater threat than terrorism,' warns British Army chief;"

- *The Hill,* June 2018, "North Korea's nuclear threat is nothing compared to its cyber warfare capabilities."

In other words, these nation-state threats have already fired the first shots of cyberwarfare with the United States. We must act now to ensure that our cybersecurity forces—military, public and private—are prepared to win these battles.

How do we do that? How can we make sure that it is our researchers who discover vulnerabilities rather than foreign threat actors? How can we ensure that the United States remains the world's leading cyber power?

The answer is people. I'm sure everyone here is aware of the well-publicized difficulties the Department of Homeland Security has been facing in hiring skilled cybersecurity workers.

- *Federal News Radio,* May 2016, "DHS sweetens cyber workforce recruiting with new bonuses;"
- *Fed Manager,* October 2017, "DHS Staffing Woes, Cybersecurity Preparedness Highlighted In Hearing;" and more recently, in April 2018,
- *The Hill* reported, "DHS chief on unfilled cybersecurity positions: We're working on it."

We need to work harder and faster. We need more programs, more camps, more competitions that educate kids and inspire them to pursue cybersecurity careers. We need to create a clear path from education to employment so that people of all skill levels can easily transition into cybersecurity careers. Indeed.com reports the current median salary for an entry-level information security analyst at $80,908. The national average entry-level salary is $45,361 (iCIMS, *The Class of 2017 Job Outlook Report*). If you build it, they will come. But people need to know these opportunities exist, which brings me to my final topic: communication.

I would like to take a moment to commend the fine work of the researchers who discovered Meltdown and Spectre and their efforts in alerting manufacturers and the public. However, I wish to caution everyone here that I believe luck played a large role in avoiding disaster. Quoting from "Meltdown," a paper written jointly by the three teams that made this discovery, "We would like to thank Anders Fogh for fruitful discussions at BlackHat USA 2016 and BlackHat Europe 2016, which ultimately led to the discovery of Meltdown" (meltdownattack.com/meltdown.pdf, p. 15). BlackHat is one of the world's largest—and most notorious—information security events in both the U.S. and Europe. It is notorious because it attracts not only distinguished academics and industry professionals, but also experts with, let's say, a flexible moral code.

It was reported that researchers first alerted Intel on the afternoon of December 3, a Sunday. I applaud their sense of urgency, but must ask, at what point was the National Security Agency or the Department of Homeland Security notified? An article written by *The Verge* chronicling the discovery and disclosure of Meltdown and Spectre reads, "Perhaps most alarming, some crucial outside response groups were left out of the loop entirely. The most authoritative alert about the flaw came from Carnegie Mellon's CERT division, which works with Homeland Security on vulnerability disclosures. But according to senior vulnerability analyst Will Dormann, CERT wasn't aware of the issue until the Meltdown and Spectre websites went live, which led to even more chaos."

These two moments reveal a critical issue: the lack of a clear, rapid report-and-respond mechanism for national cybersecurity threats. Currently, multiple agencies and organizations bear responsibility for national cybersecurity defense: DHS, NSA, the military, the FBI. To which of these organizations should the researchers have reported their discovery? Do they have duty to report? When a vulnerability is reported, what is the mechanism to alert critical areas of our government?

In the case of Spectre and Meltdow, industry responded quickly with patches and solutions, but only after they were made aware of the problem. We can get a better handle on cyber hacks and breaches if we are more *proactive than reactive.* To this end, we need:

- A larger Cybersecurity workforce (we are dealing with a severe shortage today)
- Create awareness, provide education and training to businesses and citizens and teach them to practice good cyber hygiene
- Better coordination and dissemination of critical information (attacks, discoveries, patches et al)
- To empower and hold accountable certain government organizations that can navigate through the complex and beauracratic process

- To act with a sense of urgency
- To let the government play a major coordinating role

Chairman Thune, Ranking Member Nelson, and esteemed Committee members, I thank you for allowing me to share my thoughts, and I look forward to answering your questions.

The CHAIRMAN. Thank you, Mr. Sridharan.

As I noted in my opening statement, concerns have been raised about the adequacy of the coordinated vulnerability disclosure, or the CVD process, and the timing of the notice to the U.S. Government.

How could industry guidance provide more detailed advice on when and whether to notify the U.S. Government and how to coordinate complex, multiparty disclosures for vulnerabilities like Spectre and Meltdown that affect so many companies in different industries? And I would open that up to anybody on the panel who would like to respond to that. Yes, sir, Mr. Manion.

Mr. MANION. Thanks for the question.

So the current guidance that I am familiar with does account for this sort of notification. However, in light of the Spectre and Meltdown disclosures, that guidance may need to be updated or made more clear or more forward in the guidance. So it is certainly possible to change that guidance. My organization actually participates in standards development that helps that guidance develop. But there is also a practice that has to happen as well. So it may be possible that through actually practicing that type of government notification more often, that will set the standard and the norm for continued behavior in that direction.

The CHAIRMAN. Anybody else on that?

[No response.]

The CHAIRMAN. Next question. I will direct this to Ms. Dodson. NIST is well known in the cybersecurity arena for serving as an honest broker and for convening stakeholders to address complex problems. How could NIST facilitate new public-private partnerships to address responses to complex cybersecurity vulnerabilities going forward? And as sort of a follow up, for example, could NIST convene stakeholders to discuss improvements to CVD guidance and best practices?

Ms. DODSON. Thank you for that question.

There is a large body of work that we can continue to build upon, the work of CERT/CC as an example, the standards body's work. Our sister agency, NTIA's multi-stakeholder processes help support processes around vulnerability disclosure in a way to understand the complexities.

In addition to that, I think the tie-back to supply chain is critically important and thinking about supply chain kinds of guidelines, et cetera.

So NIST is continuing to work with stakeholders in public-private partnerships to continue to convene discussions around supply chain, around vulnerability management, getting the word out, raising awareness, working with standards bodies, et cetera. So, we are committed to doing that.

The CHAIRMAN. Well, we hope you will step up your efforts in that regard.

As our oversight has discovered and I would direct this to Ms. Kim. And thank you, by the way, for coming today. Arm played a key role in responding to these vulnerabilities and notifying your business partners. You testified that Arm has refined its vulnerability handling process, including recognizing the importance of working with government stakeholders. So maybe you could tell us what impact these refinements have had so far, and is Arm considering any other ways to improve the process?

Ms. KIM. Yes. Thank you for asking that question.

We certainly have put in a lot more effort as far as engaging with the research community, and that is an industry-wide effort, including all the players involved in both Spectre and Meltdown and additional ones as well. We have certainly seen, for example, this latest flavor, which is an ongoing area, you know, collaboration that was closely done with the researcher, notification and disclosure to the relevant need-to-know parties following the coordinated disclosure guidelines. So we feel like we have made great progress and focusing on the balances that we struggle with, which is making sure that the public is safe while we are developing the mitigations needed to protect against those vulnerabilities.

The CHAIRMAN. And to include government stakeholders?

Ms. KIM. Absolutely. I mean, we welcome and appreciate the collaboration that we have been able to develop to date. At least Arm continues to plan for open dialogue, and where NIST and DHS and other government agencies are helpful, we will absolutely leverage all and every resource we can get.

The CHAIRMAN. I am a big believer in public-private partnerships, and I think in this case, it is going to be really essential that that happen.

Dr. Griffiths, good to see you. As I mentioned, DSU is a world leader in educating cybersecurity professionals. Given that responding effectively to cyber vulnerabilities is both a technology and a people issue, how can universities play a larger role in developing our nation's cybersecurity workforce?

Dr. GRIFFITHS. Thank you for that question.

I think clearly universities are actively engaged in trying to address the issue of the cybersecurity workforce shortage. As I mentioned, one of the critical factors that limit our ability to move as quickly as we could is the availability of faculty. We have 1,000 students in the Beacom College of Computer and Cyber Sciences. We could easily have 2,000 students, but we would not have the sufficient faculty to actually conduct the teaching at the level of quality and integrity that we expect. So we have a supply problem in terms of sufficient people to come into the teaching environment.

The number of Ph.D.s that are produced in the cyber sciences is 2 percent relative to 8 percent for other STEM disciplines, and people can earn significantly more times the academic salary by going into the government sector or the corporate sector. So we are in constant competition. And we are constantly trying to attract faculty to come and work with our students. I think that is a critical bottleneck that we have around the country quite frankly.

The CHAIRMAN. Senator Nelson.

Thank you.

Senator NELSON. Thank you, Mr. Chairman.

It has been reported that Intel informed Chinese companies of the Spectre and Meltdown vulnerabilities before notifying the U.S. Government. As a result, it is highly likely that the Chinese Government knew about the vulnerabilities. An official from the Department of Homeland Security is quoted as saying, "we certainly would have liked to have been notified of this."

Ms. Kim, did Arm inform any other governments or Chinese companies about Spectre and Meltdown vulnerabilities before the public disclosure on January 3rd, 2018?

Ms. KIM. Thank you, Mr. Nelson.

We notified our customers as stated, the architecture customers that we were working with. Who they may have communicated to is not something that I have knowledge of. But from a global customer base perspective, we do have architecture customers in China that we were able to notify to work with them on the mitigations as well.

Senator NELSON. Did it occur to you that you should notify the U.S. Government?

Ms. KIM. Certainly, as we have demonstrated this past few times, we have had open dialogue. At that point, again given the unprecedented scale of what we were looking at, our focus was on making sure that we assessed the full impact of this vulnerability, as well as get to potential impacted customers, and focus on developing mitigations. We have clearly demonstrated that our communication channels and open dialogue with DHS and any other government agencies will continue. So I believe that is something that you will see going forward.

Senator NELSON. So it did not occur to you to notify them this past time, but you are going to in the future. Is that what you are saying?

Ms. KIM. No. We did. We notified on the last two flavors that were discovered before notification. The initial June Spectre and Meltdown, again as I said, was a very, very unprecedented event where, as Mr. Manion described, multiple complexities, multiple parties and we were mainly focused on assessing the full scope and impact, as well as mitigations.

Senator NELSON. Do you think you can get out of this yourself, or do you think you need help?

Ms. KIM. As I have stated, we certainly welcome the partnership and collaboration, and we have found those to be incredibly helpful. We will continue to partner closely and collaborate with the U.S. Government.

Senator NELSON. What do you think about this, Mr. Manion?

Mr. MANION. So I also agree. Like I said, there are many, many vulnerabilities. However, Spectre and Meltdown vulnerabilities affecting core CPU hardware really truly are unprecedented. And that introduced a lot of complexity and difficulty into what otherwise would have been an average, normally difficult coordination process.

A number of things probably combined to lead to the insufficiency of U.S. Government notification. What we focus on, when we work with industry, Arm and other vendors, is to try to do better the next time, which Arm in this case has demonstrated they are already doing, and which is something we are actively working

with other industry contacts to remind them of the existing practice of notifying critical infrastructure and important service providers before public disclosure happens to avoid costly surprises.

Senator NELSON. So let me see if I can restate what you just said. You think that 7 months, after having notified their customers, to notify the government is a rather long time.

Mr. MANION. It is a rather long time. In our professional assessment, it is probably too long particularly for very special new types of vulnerabilities like this.

Senator NELSON. Ms. Kim, how long after you discovered the vulnerability until you notified the customers?

Ms. KIM. As I stated, we notified the architecture customers within 10 days of learning about it. We needed to validate and verify whether the conditions of this vulnerability could be reproduced and to understand a little bit more about its impact to our architecture designs.

Senator NELSON. Mr. Sridharan, in your testimony you state that we need to let the government play a major coordinating role. Do you want to just underscore why this is important in light of what we have been talking about?

Mr. SRIDHARAN. Thank you for that question. Absolutely.

There has got to be some coordinating body that works in the private-public partnership, as we have defined it, to make sure all the stakeholders know what the issues are. Right now, that single coordinating role does not exist. It is spread between different agencies. It is spread across different verticals. And with DHS saying there are 16 critical infrastructures that we need to protect the security of the nation, we have got to have a much better coordinating role that an agency needs to play, one, to disseminate the information; two, disseminate the vulnerabilities, as well as how to patch them; and three, to make sure that steps are taken so that it does not happen again. That is what I was implying, Senator.

Senator NELSON. And, Mr. Manion, how could you all have been more helpful to them if you had known about it?

Mr. MANION. Thank you for the question.

So had the CERT Coordination Center been involved in advance of the first round of Spectre and Meltdown disclosures, our typical practice again, the coordinated disclosure practices were followed by the vendor group. However, we would have advised changing some of the parameters of the disclosure process. For example, notifying more vendors, more operating system vendors, possibly more hardware vendors earlier in the process and absolutely including the U.S. Government, particularly the DHS NCCIC, which is a standard practice that we follow, well before the public disclosure dates. One week in advance of the public disclosure date is insufficient time. In this case, it leaked one week early, which removed any chance to notify government. The DHS NCCIC has a long history of being able to keep the embargo and keep the secrecy of such information. So I do not think it is a problem of DHS NCCIC leaking the information prematurely.

Senator NELSON. Mr. Chairman, I have a letter by several safety advocates to insert in the record.

The CHAIRMAN. Without objection, it will be entered in the record.

[The information referred to follows:]

*July 10, 2018*

Hon. JOHN THUNE, Chairman,
Hon. BILL NELSON, Ranking Member,
Committee on Commerce, Science, and Transportation,
United States Senate,
Washington, DC.

Dear Chairman Thune and Ranking Member Nelson:

In preparation for tomorrow's hearing "Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown," we write to highlight the critical problems related to the cybersecurity of connected and autonomous vehicles (AVs). As these cars will be "computers on wheels," it is absolutely essential that strong protections be in place to safeguard against potentially catastrophic instances of vehicle hacking. We respectfully request that this letter be included in the hearing record.

Given recent high-profile cyberattacks and the tremendous threat that hacking will pose to connected and automated cars, we are very concerned that these potential risks are not being adequately addressed. In 2015, hackers demonstrated their ability to take over the controls of a sport utility vehicle (SUV) that was traveling 70 miles-per-hour on an Interstate outside of St. Louis, MO. By accessing the vehicle's entertainment system using a laptop computer, hackers located miles away from the vehicle were able to send disruptive commands to the SUV's dashboard functions, steering, brakes, and transmission. This incident is likely just a preview of the types of hacking that will be possible as vehicles become even more reliant on complex electronic systems and outside communications.

Moreover, there is a very real and dangerous possibility that instances of hacking will not only affect one individual vehicle, but could very well impact entire fleets or model lines—posing a severe risk to occupants of the hacked vehicles as well as other road users. These attacks could also clog roads, stop the movement of goods and hinder the response of emergency vehicles. Of additional concern, there are a number of tragic examples of conventional vehicles being used as weapons by terrorists. The potential for remote hacking of connected and automated vehicles by these malicious actors could have unimaginable implications for our national security. Moreover, these risks will only be exacerbated as commercial motor vehicles, specifically large trucks and buses, become more reliant on autonomous systems and are used in platoons.

Currently, Section 14 of the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act (S. 1885), only requires manufacturers to have a cybersecurity plan in place. This is woefully inadequate and has no requirements that any protections be implemented. Instead, the legislation should be improved to direct the National Highway Traffic Safety Administration (NHTSA) to issue a minimum performance standard for all AVs (including SAE Level 2 vehicles). The agency should be required to issue this final rule within a reasonable deadline of three years after enactment. In fact, the July 6, 2018 edition of *Science Magazine* included an article penned by Joan Claybrook and Shaun Kildare which called for a cyber standard and suggested that regulators "look across industries and adapt standards from other modes and fields (banking, military, aviation, etc.) to ensure that AVs have a means for detecting and responding to an attack appropriately and preventing a widespread threat to safety." (Please see full article attached.)

Further, we support the establishment of a method for sharing cybersecurity problems and vulnerabilities among manufacturers so that all systems can be updated accordingly. To mitigate against widespread impacts, establishing a method of quickly identifying issues and disseminating that information across all participants is critical.

The public recognizes the acute threat of cybersecurity attacks on vehicles, and for good reason. A poll conducted by Morning Consult earlier this year showed that 67 percent of adults responded that they were somewhat or very concerned about cyber threats to driverless cars. An ORC International poll from January 2018 showed that 81 percent of respondents supported the United States Department of Transportation issuing rules to protect against hacking of cars that are being operated by a computer.

We urge you to include the need for robust protections against vehicle hacking in tomorrow's timely discussion. Furthermore, the pending AV START Act should not be enacted into law without requirements that sufficiently account for the reality of cybersecurity threats, including hacking into driverless cars. Thank you for

your consideration of our position. We look forward to continuing to work with you to ensure the safety of all road users.

Sincerely,

Catherine Chase, President
Advocates for Highway and Auto Safety

Joan Claybrook, President Emeritus
Public Citizen and Former NHTSA Administrator

Jason Levine, Executive Director
Center for Auto Safety

Jack Gillis, Executive Director
Consumer Federation of America

Rosemary Shahan, President
Consumers for Auto Reliability and Safety

John M. Simpson, Privacy and Technology Project Director, Consumer Watchdog

cc: Members of the Committee on Commerce, Science, and Transportation

ATTACHMENT

*INSIGHTS*

POLICY FORUM

TECHNOLOGY DEVELOPMENT

# *Autonomous vehicles: No driver...no regulation?*

## Driverless cars are on the road with no federal regulation, and the public is paying the price

*By* **Joan Claybrook[1]** *and* **Shaun Kildare[2]**

According to the latest statistics from the U.S. National Highway Traffic Safety Administration (NHTSA), 37,461 people were killed on the nation's roads in 2016 (*1*). Autonomous vehicle (AV) technology has the potential to reduce this number substantially. However, proper safeguards must be established immediately by federal regulators to govern the testing and deployment of AVs and ensure public safety. We must not undermine current safety standards for the sake of AV development. Moreover, reconsidering current requirements may be necessary to take advantage of this revolution. Nearly two-thirds (64%) of respondents in a recent CARAVAN public opinion poll expressed concern about sharing the road with driverless cars (*2*). If commonsense protections are not in place to govern AV development, and problems occur, the public will reject AVs, and the opportunity this new technology presents to improve public safety will be lost.

AV technology is still very much in development, as evidenced by the serious and fatal crashes that have occurred this year. In January of 2018, a Tesla Model S that was operating under its "Autopilot" system crashed into the rear of a stopped fire truck in California (*3*). On 18 March, an AV operated by Uber struck and killed a pedestrian crossing a road in Tempe, Arizona (*4*). Only 5 days later, a Tesla Model X was involved in a fatal crash in California, striking a safety barrier before bursting into flames (*5*). On 11 May, a Tesla crashed into the rear of another fire vehicle in Utah while operating under its Autopilot system (*6*). These crashes illustrate that sensors and algorithms of AVs are still having trouble identifying road hazards and potential obstacles reasonably expected to be in the driving path. The lack of regulation has allowed these unproven vehicles onto our roads. The crashes that have occurred were not unforeseeable and have shaken the public's trust in the technology. Commonsense requirements for the performance of AVs are necessary to protect the public and instill confidence in the technology.

Over 50 years ago, Congress passed the National Traffic and Motor Vehicle Safety Act of 1966 because of concerns about the death and injury toll on our highways. The law required the federal government to establish minimum vehicle safety performance standards to protect the public against "unreasonable risk of accidents occurring as a result of the design, construction or performance of motor vehicles" (*7*). Although motor vehicles have changed dramatically since that time and will continue to do so in the future, the underlying premise of this crucial law has not.

There are currently many regulatory gaps that need to be filled. Federal regulators should develop a list of operational scenarios and a range of conditions under which AVs must be evaluated to ensure that the public is not being placed in harm's way through the introduction of these vehicles. For example, problems associated with different weather and fouling conditions for different types of sensor need to be studied. There should be a minimum "vision test" for the AV system to make sure that it can properly identify its surroundings, including other cars, pedestrians, cyclists, road markings, and traffic signs, and respond appropriately. Moreover, manufacturers must be required to execute comprehensive testing and development before taking these vehicles onto public roads. To protect the public, strict protocols must also be established for testing of these vehicles on public roads. Recent work internationally has identified many of the same concerns with the development and deployment of AVs as noted throughout this work (*8*).

AVs that require monitoring by a human driver have been the first introduction of AV technology to the general public. However, humans are inherently bad at monitoring semi-autonomous systems and are readily distracted (*9*). Manufacturers must find a way to keep a driver engaged in the driving task, and regulators must require that engagement in a meaningful way. This is a conclusion reiterated in the findings of the National Transportation Safety Board (NTSB) investigation of a fatal Tesla crash in Florida in 2016 (*10*).

It is vital that there be standardized, mandatory data reporting. There needs to be a central repository by which all AV manufacturers and federal regulators are routinely made aware of situations identified during testing or deployment that have led to collisions or failures. Currently, there is no transparency regarding the algorithms that form the basis for AV function and thus no way to determine whether there are better approaches to solving problems that resulted in collisions or serious system malfunctions. The information required, however, is more than just that covered by an incident report but must include details on the dynamics of the collision, and more important, how the decision process of the AV may have led or contributed to the crash. Only through data collection and analysis can future regulatory needs be developed and justified. There are already examples of this type of data sharing for safety's sake, such as in commercial aviation (*11*).

Additionally, the possibility of a catastrophic cyberattack on transportation increases as the number of AVs on the road increases. Federal regulators must look across industries and adapt standards from other modes and fields (banking, military, aviation, etc.) to ensure that AVs have a means for detecting and responding to an attack appropriately and preventing a widespread threat to safety. The need for NHTSA to develop a strategy to address cybersecurity was raised more than 5 years ago in a report on the subject by the National Research Council of the National Academies (*12*); however, little progress toward meaningful regulation of this aspect of AV performance and safety has been achieved.

Despite the need for regulation, NHTSA, the federal agency responsible for keeping people safe on America's roadways through enforcement of vehicle performance standards, has issued mere voluntary guidelines that are unenforceable and place no mandates on the industry to develop and test AVs safely. In addition, the agency has failed to act to address the shortcomings of AV technology that have already been identified. For example, the NTSB determined that the driver of a Tesla Model S who had been killed in a 2016 crash in Florida had not been en-

[1]*President Emeritus, Public Citizen, Washington, DC, USA. From 1977 to 1981, she was administrator of the National Highway Traffic Safety Administration.* [2]*Director of Research, Advocates for Highway and Auto Safety, Washington, DC, USA. Email: joan@joanclaybrook.com; skildare@saferoads.org*

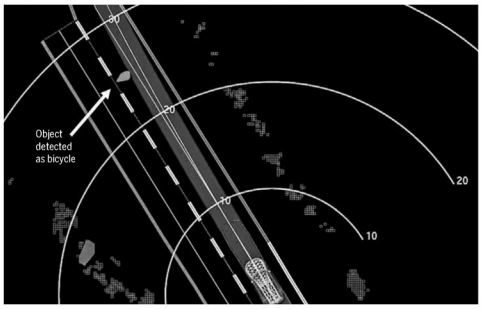



IMAGE: NTSB

**Uber self-driving system data playback from the fatal, 18 March 2018, crash of an Uber Technologies, Inc., test vehicle in Tempe, Arizona. Yellow lines show meters ahead of the vehicle. According to the NTSB preliminary report (https://goo.gl/2C6ZCH), although the pedestrian pushing a bicycle was first detected 6 s before the crash, she was categorized by the self-driving system as an unknown object, as a vehicle, and then as a bicycle. At 1.3 s before impact, the self-driving system determined that emergency braking was needed. However, the automatic braking system was not enabled, and no alert was provided to the driver who was supposed to be monitoring the system.**

gaged in the driving task, and that a probable cause was the operation design "contributing to the car driver's overreliance on the vehicle automation." Even worse, from an engineering standpoint, is that the design of the system allowed misuse. The NTSB found that these problems were not Tesla's alone but are industry-wide (*13*). Yet, NHTSA still has not initiated regulatory proceedings to address these serious safety issues. NHTSA needs to issue regulations governing the safe operation of these vehicles to ensure that development, testing, and eventual deployment into the public domain do not endanger lives.

Compounding the problem is legislation currently pending before Congress (*14*). Both a bill passed by the House of Representatives (SELF DRIVE Act, H.R. 3388) and a measure currently pending before the Senate (AV START Act, S. 1885) will allow automakers to receive broad exemptions from existing federal motor vehicle safety standards and ignore the need for NHTSA to issue minimum safety requirements. In 2015, Congress exempted test vehicles from having to comply with federal safety standards (*15*). The current legislation would allow for the potential sale of millions of AVs that can be exempt from standards that ensure occupant protection and crashworthiness. It would allow for wide-scale commercial introduction of AVs that fail to meet federal safety standards in order to increase industry profits. If this provision is not drastically altered, our nation's roads risk becoming corporate proving grounds for unverified technology, and the American public will end up being unwitting subjects in a potentially deadly experiment.

Another concern, for those cars that can be driven either autonomously or by a human driver, is that the Senate bill dangerously departs from well-settled federal law by allowing manufacturers to disconnect steering wheels, brakes, and other safety systems, when such a vehicle is operated in an autonomous mode, without any government review and approval. Furthermore, neither bill encompasses all AVs, including those that depend on a human driver to monitor their operation. These vehicles are already on the road, have been involved in multiple deadly crashes, and will comprise a sizable portion of the AV fleet for years to come. Neither bill being considered by Congress requires NHTSA to deal with the regulatory issues that we describe and develop critical standards that will be essential to assuring the proper development and operation of AVs. In addition to all of these concerns, Congress has not provided NHTSA with sufficient funds to deal with the expanded duties it will have in response to the advent of AVs. AVs are already being tested in states and cities across the country. Some state and local governments have started to put in place the first requirements to preserve public safety in the absence of any substantive action by the federal government. Unfortunately, both bills before Congress will preempt these regulations, despite NHTSA having yet to issue any federal standard for AVs. This unprecedented attack on the historic state responsibility to protect their residents will create a regulatory vacuum that will needlessly put the public at risk. Until NHTSA issues safety standards and regulations for AVs, state and local governments have every right, and in fact a duty, to protect their citizens. Traditionally, states are allowed to act where the federal government has not taken specific action; however, the issue of preemption may have to be resolved by the courts. NHTSA has failed to respond meaningfully to the development of AV technology. Although the technology has the ability to save lives once developed, at the same time it can risk lives (and has already claimed several) if it is not executed properly. A federal framework developed around ensuring safety, not just supporting corporate development, is necessary. Congress must end the deregulatory efforts and focus on balancing productive competition while maintaining the levels of safety required by established law and practice. A failure to put proper safeguards in place will result in the continued erosion of the public confidence in this potentially lifesaving and game-changing technology. ■

## REFERENCES


1. National Center for Statistics and Analysis, *2016 Fatal Motor Vehicle Crashes: Overview*. Traffic Safety Facts Research Note. Report no. DOT HS 812 456 (National Highway Traffic Safety Administration, Washington, DC, October 2017).
2. ORC International, CARAVAN Public Opinion Poll: Driverless Cars (12 January 2018).
3. P. Valdes-Dapena, "Tesla in Autopilot mode crashes into fire truck," *CNN Tech*, 24 January 2018.
4. E. Rosenfield, "Tempe police release video of deadly Uber accident," *CNBC*, 21 March 2018.
5. D. Shephardson, "U.S. opens probe into fatal Tesla crash, fire in California," *Reuters*, 27 March 2018.
6. K. Allen, "Tesla Model S was in Autopilot mode during Utah crash, driver says," *ABC News*, 15 May 2018.
7. Public Law 89–563.
8. International Transport Forum, Safer Roads with Automated Vehicles? (ITF, 2018).
9. http://acrs.org.au/files/papers/arsc/2015/CunninghamM%20033%20Autonomous%20vehicles.pdf
10. National Transportation Safety Board, Collision between a Car Operating with Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016. Accident Report NTSB/HAR-17/02. PB2017-102600 (12 September 2017).
11. www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18195
12. *Transportation Research Board Special Report*, vol. 308, *The Safety Challenge and Promise of Automotive Electronics: Insights from Unintended Acceleration* (Transportation Research Board, Washington, DC, 2012); www.nap.edu/catalog.php?record_id=13342
13. Collision Between a Car Operating with Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida, May 7, 2016; NTSB, Accident Report NYST/HAR-17/-2.
14. S. 1885, American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act, 115th Congress, 1st Session (2017); H.R. 3388, Safely Ensuring Lives Future Development and Research in Vehicle Evolution (SELF DRIVE) Act, 115th Congress, 1st Session (2017).
15. Fixing America's Surface Transportation Act, Sec. 24404, Public Law 114-94 (2015).


10.1126/science.aau2715



*Published by AAAS*

The CHAIRMAN. Thank you, Senator Nelson.
Senator Gardner.

**STATEMENT OF HON. CORY GARDNER,**
**U.S. SENATOR FROM COLORADO**

Senator GARDNER. Thank you, Senator Thune. Is it all right with Senator Hassan?

Senator HASSAN. It is fine.

Senator GARDNER. Thank you. I would be happy to yield my time.

Senator HASSAN. That is all right.

Senator GARDNER. Thank you, Senator Hassan. Thank you, Mr. Chairman. Thanks to the witnesses for being here this morning.

This is obviously a very important issue, vulnerabilities, protecting our Federal networks from cyber attacks, important matters to Congress to consider. And I am pleased that we are taking the opportunity to do so today. I am grateful for the hearing.

As the Co-founder of the Senate Cybersecurity Caucus and the Chair of the East Asia Subcommittee on Foreign Relations where we have jurisdiction over international cybersecurity that is a topic that we think about often. Ms. Dodson, I wanted to direct the first series of questions to you.

Thanks again for appearing today. Thank you for all the phenomenal work that NIST is doing on the campus in Colorado from quantum computing to IoT research. NIST is a critical Federal player across a whole range of industry stakeholders. The gravity of these issues we are covering are being handled by NIST and many of the reasons why I have been supporting increased funding for the agency during my time in the Senate because of the work you are doing and you are talking about here today. So I encourage all my colleagues to consider supporting these efforts at NIST and other places as well.

A quick question for you. Do you think that the Federal Government today is currently purchasing unsecured devices?

Ms. DODSON. So, thank you for that question.

As we have all discussed, security is really about people, processes, and technologies. And it is a continuum. So we can look at cybersecurity capabilities from the very basic all the way up to the very, very sophisticated. Certainly, depending on the needs and the requirements in the Federal Government for particular applications, NIST has always advocated a risk management approach to get the level of security that is needed.

Senator GARDNER. But I think the answer is yes.

Ms. DODSON. Your question is do we have unsecured products.

Senator GARDNER. And the answer is yes, and the government is currently purchasing unsecured devices. The answer is yes.

Ms. DODSON. We have had some that could be improved, yes.

Senator GARDNER. But I think the answer is, is the government currently purchasing unsecured devices?

Ms. DODSON. So, I cannot speak for the entire Federal Government, but are we——

Senator GARDNER. Let me ask it this way. Are all of the purchases the Federal Government makes secured?

Ms. DODSON. No.

Senator GARDNER. Thank you.

So do you think it would be wise for the Federal Government as a matter of general practice to acquire or procure devices with unchangeable and preset passwords or other fixed or hard coded credentials?

Ms. DODSON. I think we need to have a risk management approach and we need that sort of flexibility. In our identity management work at NIST, we advocate not just for passwords that are not changeable but, actually, to have more advanced capabilities for——

Senator GARDNER. As a matter of general practice, would anybody on the panel purchase, acquire, or procure devices with unchangeable and preset passwords or other fixed or hard coded credentials? Just a quick yes or no, if I could.

Mr. MANION. Yes, depending on the application.

Senator GARDNER. You would buy it if you had to.

Mr. MANION. For a very low security application.

Senator GARDNER. But I think that you would prefer to avoid that. Right? Correct, OK.

Ms. Dodson, do you believe it would be wise for the Federal Government as a matter of general practice to acquire software or firmware that cannot be updated by vendors who sell those devices to the Federal Government?

Ms. DODSON. I am sorry. Can you repeat that?

Senator GARDNER. So should the Federal Government purchase or acquire software or firmware that cannot be updated?

Ms. DODSON. We should have mechanisms to be able to update and address vulnerabilities.

Senator GARDNER. So we should not be buying software that cannot be updated, firmware that cannot be updated as a matter of general practice. That is correct?

Mr. Manion, do you believe overall Federal Government security is improved when vendors participate in a coordinated vulnerability disclosure program, understanding that these programs probably need to be improved?

Mr. MANION. Absolutely. It is a much better situation when government and industry are working together and everyone is informed. Otherwise, you have a horrible surprise and the cost of the surprise that we had with Meltdown and Spectre.

Senator GARDNER. And thank you for this. I ask these questions because Senator Warner and I have introduced a bill called the IoT Cybersecurity Improvement Act that would address each of these issues. It would require security clauses in vendors' contracts with the Federal Government that would address the need for updateable software and firmware. It would prohibit insecure approaches like hard coded credentials, and it would require the issuance of guidelines for vendor participation in a coordinated vulnerability disclosure program.

The Federal Government I believe needs to do a better job from a procurement perspective about ensuring that we have more secure devices and more secure software. I am not naive enough to think that we are going to have absolutely 100 percent security at all times, but by implementing some very basic security standards

and practices in our acquisition process, the Federal Government can absolutely raise the bar.

And so I am glad to hear that people agree with me that we can do better, that we can find some of these basic ideas that are in the bill, and the ideas in the bill are not entirely off the mark. I look forward to working with my colleagues on this panel on legislation to help find a better way for more device security.

And, Mr. Sridharan, I would like to just talk about legislation that I have introduced with Senator Coons that would create a standalone cybersecurity committee here in Congress, the idea being we have about a dozen committees that have some form of jurisdiction in cybersecurity. It would be nice if we had one committee of jurisdiction that could combine the expertise of the other committees under one committee that could actually have oversight of cyber policy, cyber direction.

So thanks very much to all of you for being here.

Thanks, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Gardner.

Or we could just take all those committees' jurisdiction and put them under Commerce.

Senator GARDNER. I am fine with that too. I am fine with that. [Laughter.]

The CHAIRMAN. Back to regular order. Sorry about that. Senator Hassan.

**STATEMENT OF HON. MAGGIE HASSAN,**
**U.S. SENATOR FROM NEW HAMPSHIRE**

Senator HASSAN. Oh, no. It is just fine. Thank you so much, Mr. Chair, and I want to thank you and the Ranking Member for holding this hearing today. And I want to thank all of our witnesses for being here.

I want to start with a question to Ms. Dodson and Ms. Kim. There is some confusion about the actual remediation steps taken by these processor companies in the wake of the discovery of the Meltdown and Spectre vulnerabilities. So the question is, did these companies actually patch the vulnerabilities, or did these companies just take steps to make it harder for hackers to access these processors? In other words, did these companies eliminate all risks associated with these vulnerabilities? And if not, what can be done to fully eliminate the vulnerabilities?

Ms. KIM. So great question. There are certainly both in many instances where we attempt to recreate the conditions in which these vulnerabilities could be exploited and where possible mitigations and patches and so forth are developed. As far as ones that we cannot reproduce, it is difficult for us to do that. But we believe the complexity and sort of the extreme difficulty of these research areas creates a necessary hurdle, that it is not a standard widespread issue.

Also, while it is not common for many to accept downloads and updates and patches, we believe that the education of consumers to always be vigilant about making sure that the latest updates and security patches are applied because both Spectre and Meltdown require malicious code to be present on a device. So there has

to be some access to that particular device in order to exploit it using this method.

Senator HASSAN. Thank you.

Ms. Dodson.

Ms. DODSON. Thank you for the question.

We understand that we will continue to be dealing with Spectre and Meltdown issues for years. I think Mr. Manion mentioned that there was a variant that came out just recently, as in yesterday. So, we will continue to need to be vigilant. We need to continue to work on our capabilities to build stronger systems. We need to instill resiliency in our people, processes, and technologies as we are dealing in cybersecurity.

Senator HASSAN. So that leads me to kind of my second question, and it is really a follow up to what Senator Gardner was also asking about.

Ms. Dodson, you are the only government witness on the panel. So are you aware of how many United States Government computers currently have processors containing these vulnerabilities?

Ms. DODSON. So NIST as an organization works to provide remediation and work with industry in a public-private manner to actually provide capabilities for patching, et cetera through our National Vulnerability Data base. The actual number of patches that have been applied across the U.S. Government is an operational issue under the purview of DHS. So I can look into that.

Senator HASSAN. Well, I would appreciate that because I would like to know how many of our government computers still have this vulnerability and whether all of them have received the mitigation updates that would make it more difficult for a foreign actor to try to exploit these government computers.

Ms. DODSON. We have made those patches available through our National Vulnerability Data base to both government and industry.

Senator HASSAN. But the question remains who is checking to see whether those patches have actually been installed.

Ms. DODSON. The Department of Homeland Security put out a binding operational directive for critical patches for the U.S. Government systems, and so the reporting goes to them.

Senator HASSAN. I will just conclude by this comment. DHS, supported by Congress, is working hard to try to defend our government systems from foreign cyber attacks. Just recently, the U.S. Government took action to address the prevalence of the Kaspersky software in our systems, while last month the Senate passed a defense bill that banned the use of ZTE products by the Federal Government. So we are focused on this.

I am a cosponsor of the bill that Senator Gardner and Senator Warner introduced. So it is really troubling and concerning that many, if not all, computers used by the government contain a processor vulnerability that would allow hostile nations to steal key datasets and information. It is even more troubling that these processor companies knew about these vulnerabilities for 6 months before notifying DHS. So we need to consider additional ways to require the Federal Government's equipment suppliers to promptly notify DHS of potential breaches or vulnerabilities that could weaken our Federal systems.

I know that there is a lot more work to do here, but I just wanted to make sure that we are all clear about that and look forward to working with you more on it. Thank you.

The CHAIRMAN. Thank you, Senator Hassan.

Senator Udall.

**STATEMENT OF HON. TOM UDALL,**
**U.S. SENATOR FROM NEW MEXICO**

Senator UDALL. Thank you, Chairman Thune. I think you are right. I am perfectly happy to work with you and have the Commerce Committee do all of the work on cybersecurity. I think somebody needs to pull it all together. And you got a good staff. They can do it.

Ms. Dodson, today I am going back and forth between this hearing and one in the Rules Committee on election security preparations where NIST is also testifying. We know that foreign nations like Russia are trying to interfere in our elections and have accessed State election systems in the past. There is no doubt about that. How serious a threat are these vulnerabilities for our State and local election systems, and what are the prospects for securing them from these vulnerabilities when the relevant computers are in the hands of State agencies with modest budgets and cyber expertise?

Ms. DODSON. NIST continues to work with states and with industry. So, one of our recent developments, the Framework for Improving Critical Infrastructure of Cybersecurity, is used by many states today. And that gives a process and a framework for states to address vulnerabilities in their systems, including in elections and including in the hardware and software that they are using.

In addition to that, through our framework version 1.1 process, we have increased the relationship of supply chain risk management and how to apply that not just for the current voting machines but also to be able to take a look at the supply chain both up and down the scale for the software that they are depending on for those elections.

Senator UDALL. Do you believe that NIST can serve as a pre-disclosure clearinghouse that could help test possible patches and assess the damages that could occur from a vulnerability such as Spectre and Meltdown?

Ms. DODSON. NIST's role through our work in vulnerability management is to be able to make the information publicly available so that organizations can understand those vulnerabilities in products and services that they are using, they can understand how those products and services' vulnerabilities have looked in the past and understand the patches. In addition to that, we provide metrics that help understand the severity of a vulnerability as organizations prioritize patching. So, our role really is not on the pre-disclosure. It is really at the time of disclosure.

And increasing awareness of those sorts of capabilities is critically important as we think about the Internet of Things and the work that Senators Gardner and Warner are doing in the IoT cybersecurity bill. As a matter of fact, today we are hosting at NIST a workshop on cybersecurity and privacy related to IoT be-

cause this will continue to expand as we think about cyber physical systems coming together.

Senator UDALL. Thank you.

Mr. Manion, in your testimony, you stated that the most effective coordinated vulnerability discourse, or CVD, process follows the supply chain. But should this process change if a company in the supply chain is owned by a foreign government and are there security considerations that should apply?

Mr. MANION. Thanks for the question.

So when we are dealing with large vendors and large industry, as we are, very often you already have a multinational company. And of course, the Internet does not stop at national borders. So it is practically quite difficult to avoid notifying non-U.S. persons and organizations. The relationships of those persons and organizations to their national governments and which governments those are is just almost a step too far to really have any control over. So it is worthy of consideration. However, in the interest of getting the vulnerabilities fixed quickly, we fall on the side of probably more open notification and collaboration.

Senator UDALL. Thank you.

And I will probably ask this question for the record also. Sandia National Laboratory conducts a significant amount of research on chip integrity and other cybersecurity work, and I would think that they might be a clearinghouse in the circumstances that we have just talked about. All of you are nodding. So yeses for the record for Manion and Dr. Griffiths and Dodson.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Udall.

I would ask unanimous consent to include an article from a tech news website noting that another Spectre variant was recently discovered. The article is dated July 10, 2018. It is calling this new disclosure Chipzilla. So clearly we need to be vigilant and improve our public-private partnerships. So we will include that, without objection, in the record.

[The information referred to follows:]

Security

# ANOTHER DATA-LEAKING SPECTRE CPU FLAW AMONG INTEL'S DIRTY DOZEN OF SECURITY BUG ALERTS TODAY

## CHIPZILLA PREPS FOR QUARTERLY PUBLIC PATCH UPDATES

By Chris Williams, Editor in Chief 10 Jul 2018 at 17:00

*Exclusive* Intel will today emit a dozen security alerts for its products—including details of another data-leaking vulnerability within the family of Spectre CPU flaws.

This bundle of disclosures is the start of the processor giant's efforts to move to a quarterly cadence of updates, we understand. Rather than drop surprise alerts onto *its security advisory page* at irregular intervals, Intel hopes to gradually adopt a routine similar to Microsoft's monthly Patch Tuesday, albeit once every three months.

Urgent security updates will be pushed out in between these quarterly batches. Some fixes may be emitted outside of this quarterly cadence if they are due to be released on a specific date in a coordinated disclosure with other organizations, and that date falls outside Intel's schedule.

Motherboard manufacturers, computer makers, operating system developers, and other Intel partners, will privately get a long heads up before these quarterly updates are made public. For instance, today's patches were shared with manufacturers in March, allowing them to prepare to roll out fixes to customers.

From what we understand, Intel hopes to give folks—from IT administrators to ordinary netizens—time and notice to plan for installing security updates at regular-ish intervals, rather than relying on them to look out for sporadic patches.

**Speculative execution continues to haunt**

The new Spectre-class side-channel vulnerability in Intel's processors, to be disclosed today, can be exploited in a bounds-check bypass store attack. This means malicious code already running on an Intel-powered computer can potentially extract passwords, cryptographic keys, and other sensitive information, from other running software threads by altering the flow of speculative execution.

Despite the word "store" in the attack, no actual code or data in memory is altered. However, as far as the CPU's speculative execution engine is concerned, function pointers and return addresses are overwritten in the attack, allowing the malicious code to change the CPU's course, and infer the contents of memory that should be out of reach.

This can be done by speculatively overwriting variables and other temporary values, or by speculatively overrunning buffers by tricking the processor into specula-

tively executing more iterations of a loop than anticipated. Even memory that should be read-only can be speculatively written to in order to potentially perform side-channel extraction of data. Vulnerable code can be as trivial as . . .

```
uint8_t buffer[256];
int i;

for(i = 0; i < 256; i++)
  buffer[i] = *src++;
```

More technical information on bounds-check bypass store attacks *can be found, here,* in section 2.2.1, and *here in a paper* out today by Vladimir Kiriansky and Carl Waldspurger.

The good news is that *software mitigations available* today for Spectre variant 1 will thwart bounds-check bypass store attacks. Thus, web browsers and other applications employing anti-Spectre mechanisms should be safe.

For programmers and compiler writers, this means slipping *LFENCE* instructions into code, before it reads from memory, to act as a barrier, or clipping array bounds using a bitmask, as described *here, in section four.*

The other good news is that there is little or no malware known to be circulating in the wild exploiting Spectre vulnerabilities to steal information: it is far easier for miscreants to persuade people to download and install software nasties disguised as legit applications, trick them with phishing e-mails, or attack holes in e-mail clients and PDF readers, to commandeer their PCs.

Instead, Spectre, for now, remains a fascinating insight into the world of CPU design, where engineers across the industry trade off a little security for a little more performance.

**Streamlining**

"As we continue working with industry researchers, partners and academia to protect customers against evolving security threats, we are streamlining security updates and guidance for our industry partners and customers when possible," a spokesperson for Intel told *The Registeron* Tuesday.

"With this in mind, today we are providing mitigation details for a number of potential issues, including a new sub-variant of [Spectre] variant 1 called Bounds Check Bypass Store, for which mitigations or developer guidance have been released.

"More information can be found on *our product security page.* Protecting our customers' data and ensuring the security of our products is a top priority for Intel."

More than half of today's Chipzilla advisories were the result of research carried out by its own staff, whose minds have been doubly focused on the security of their products following the *Meltdown and Spectre* disclosures *earlier this year.* The alerts will cover things from firmware to Intel's flavor of Python.®

The CHAIRMAN. Let me just ask and this would be to Ms. Dodson at least initially. But in your testimony, you mentioned that the National Vulnerability Data base is the authoritative source on security vulnerabilities. Yet, according to press reports, it takes an average of 33 days after public disclosure to complete the cataloging process and entry in the data base.

So what steps are you taking to ensure that public vulnerabilities are posted in more real time?

Ms. DODSON. So NIST publishes the vulnerability as soon as we receive it. However, we do spend time on the analysis of that and the scoring. But from the process of disclosure to the time that the information is submitted to be put in the National Vulnerability Data base so that it has a numeric number and ends up in a position where NIST can post it does take time. We are working closely with the community to develop automated tools that large vendors would be able to use as they are disclosing vulnerabilities to short-

en that gap. From the NIST perspective, we are looking at different technologies like analytics to help us as we are scoring those vulnerabilities. But a big part of this is getting the word out, helping people understand how to disclose vulnerabilities and the steps that occur in that process so that we can have adequate information in the government to be able to post them.

The CHAIRMAN. But is there a way of doing that more quickly?

Ms. DODSON. Yes, and we are continuing to work on our side and we are continuing to educate product developers and service developers on how to provide the information so that we can shorten the overall time from the time that a researcher finds a vulnerability and attempts to make this publicly available. There are steps that we all must take.

The CHAIRMAN. This is sort of a broad question. I would like to get a response from each of you. But if you look at this from your perspective of your organization, what are the most important steps that your organization could take to enable government and industry to address cybersecurity vulnerabilities more effectively? Who would like to start? Mr. Manion?

Mr. MANION. Thanks for the question.

So speaking for the CERT Coordination Center, we are already sort of knee deep in this work. The steps we have in mind and in some cases already executing on are continuing to raise awareness that this ability to receive a vulnerability and analyze it, publish it, publish the fixes, integrate with the record of the National Vulnerability Data base. This is not a special case. Anyone producing software has to do this. It is a basic part of doing business, a necessary requirement. So advocating that this exists, providing guidance on how to do it, support for it, operational support in some cases, support in updating guidelines and standards to advise others how to do it, that is where a lot of my team's work is focused.

The CHAIRMAN. Good.

Ms. Kim.

Ms. KIM. As we have talked about, security is an ever-evolving field. New research happens all the time. So from an industry perspective, we are prioritizing engaging with the various researchers to make sure that the White Hat and the good actors are ahead of the curve and taking responsible steps to determine the necessary mitigations and then critically open dialogue and ongoing partnership with the U.S. Government to make sure that all the necessary parties are informed and that we can get the open communication when necessary.

The CHAIRMAN. Anybody else? Dr. Griffiths?

Dr. GRIFFITHS. Well, we are slightly different as an academic institution, but our researchers have identified some vulnerabilities not at the level of Spectre or Meltdown, but we do then report it to the agencies and partners that we are working with. But in effect, what we have been given in academe is a great case study for educating our students to explore what happened, why it happened, how it happened, what is being done as a result of it so that our students can actually learn how to put protections in place proactively rather than just reacting to the next generation of problem.

The thing that is really intriguing about this is the Spectre and Meltdown create a whole new class of vulnerability, in fact so much so that I believe people at first did not believe that it was possible. And so we have to be open to the fact that new classes of vulnerability may be discovered and then we will get the derivatives that are now coming from Spectre and Meltdown. And we need not to be complacent about the nature and the intensity of the serious threats that come from outside. I think that we maybe got a little bit complacent because we saw similar types of things. It is a hack. We can fix it. I think we have to be forever vigilant about the bad actors that are out there particularly at the Nation state level.

The CHAIRMAN. Thank you.

Mr. Sridharan.

Mr. SRIDHARAN. I think a couple of points. I think most of it has been made by other panelists here.

I think it is important that we identify the vulnerabilities by fostering innovative research and identifying where these problems are.

Second, we need to create the awareness in the small to medium to large businesses, industry as a whole, and citizens to make sure that if a patch is made available, there are fixes available, that they apply the patch. That is just as important as anything else.

Last but not the least, I think Dr. Griffiths mentioned just a second ago, we need to become more proactive in this role, not be reactive all the time as we have been. Until that mechanism changes, dynamic changes to becoming more proactive, we are going to be having these types of committee hearings.

The CHAIRMAN. Well, I hope that although these are great case studies for Dr. Griffiths' students at Dakota State University, that we have fewer case studies in the future. But I think these threats are always with us, and the question is what can we do proactively to better prevent these types of things from happening in the future. And these are all good suggestions and ideas.

We have been joined by Senator Markey. So I will recognize him. Senator Markey.

**STATEMENT OF HON. EDWARD MARKEY,**
**U.S. SENATOR FROM MASSACHUSETTS**

Senator MARKEY. Thank you, Mr. Chairman.

Americans right now are suffering from the dark side of the digital revolution, and cybersecurity experts have determined that defects in computer chips have made virtually every computer in the world vulnerable to cyber attacks for the past 20 years. Every single computer in the world is vulnerable. And with as many as 50 billion IoT, Internet of Things devices, or we could call it Internet of Threats devices projected to be in our pockets and homes by 2020, cybersecurity will continue to pose a direct threat to economic prosperity, privacy, and our nation's security.

So this is something that we have to deal with. And it is why I was proud to join Congressman Lieu in introducing the Cyber Shield Act. My bill will establish an advisory committee on cybersecurity experts from academia, industry, consumer advocacy, community, and the public to create cybersecurity benchmarks for IoT devices such as baby monitors, cameras, toasters, refrigerators,

toys, et cetera. Internet of Things manufacturers can then voluntarily certify that their product meets these industry leading cybersecurity and data security benchmarks and display this certification to the public.

My bill will also reward manufacturers adhering to the best data security practices while also ensuring consumers can make more informed choices.

Mr. Manion, do you think that creating cybersecurity certification regimes, such as the Cyber Shield Act does for IoT devices, would be helpful for consumers and small businesses when they are making purchasing decisions?

Mr. MANION. Thank you for the question.

Generally yes. Cybersecurity information is lacking to a consumer when you are making a purchasing decision. So providing more information I think would be useful. It is important to take care on what is being measured by the certification. However, we think that measuring that a manufacturer has certain processes in place, has a lifespan of support for the device, those kinds of things are measurable and would provide a consumer an indication that their device is more secure or at the very least would receive security support when something comes up.

Senator MARKEY. Good. So I agree with that.

So disclosing cybersecurity vulnerabilities and issuing remedies is only effective when those remedies are actually adopted. Regrettably all too often these cyber fixes are ignored, and that is not good cyber hygiene. Regrettably consumers may be unaware of some basic effective ways to protect themselves from cybersecurity threats such as updating or patching their software.

And that is why I joined with Senator Hatch and Congresswoman Eshoo in introducing the Promoting Good Cyber Hygiene Act. Our legislation directs NIST, the National Institute of Standards and Technology, to establish a baseline set of voluntary best practices for good cyber hygiene that are made available online.

Mr. Sridharan, do you think our legislation would help consumers practice better cyber hygiene?

Mr. SRIDHARAN. I totally believe that that is the right thing to do. As part of my testimony, I also stated that practicing good cyber hygiene will solve a lot of the problems that we face in the cyber world. And NIST playing a key role in communicating best practices to all walks of life will go a long way in mitigating those problems.

Senator MARKEY. Should we require vendors to educate their consumers about how they can protect their devices?

Mr. SRIDHARAN. I think vendors should do a better job of educating than they do today. I think there are still a lot of gaps in parents, for example, knowing what the little toy that is connected to the Internet can do and cannot do, and they do not follow instructions from the vendors in terms of changing the password, for example. So these are real problems.

Senator MARKEY. Should the vendors be required to better educate their customers?

Mr. SRIDHARAN. "Required" is an interesting word. Just mandating it, then I do not know how you enforce it unless you have

a very large organization that enforces it. But if there is a way to do it, I would be all for it.

Senator MARKEY. OK, great. Thank you. Somehow or other we have to bridge that gap, though, because like you are saying, in the hands of parents, without some kind of instruction given to them, unfortunately, it will not ultimately, in many instances, be effective. So thank you all so much for everything you are doing.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Markey.

Senator Wicker is on his way over here. So I will just ask one more question until he gets here, and this would be to Ms. Kim.

The question is, when vulnerabilities affect multiple companies as we saw with Spectre and Meltdown, is there a potential for conflicts of interest to arise or competitive disadvantage as a result when one company coordinates the response and remediation of a complex cyber vulnerability as opposed to an independent third party?

Ms. KIM. That is a great question.

I think that given at least from Arm's perspective, our collaboration and actual industry cooperation was unprecedented. It was open dialogue amongst competitors, industry partners, relevant customers. And each company has a different relationship with its own supply chain and customers. So again, as we sort of looked forward, we certainly learned a lot from the initial Spectre and Meltdown and subsequently have put in a lot more discussion and openness within the process, as well as including the U.S. Government.

The CHAIRMAN. Well, you did not run into any sort of conflicts or anybody gaming it or creating an advantage for somebody——

Ms. KIM. I can only speak from Arm's perspective, and we certainly did not feel that way.

The CHAIRMAN. Very good.

Mr. Manion, did you have a comment on that?

Mr. MANION. Not specifically to Meltdown and Spectre, but we are often on the inside track, on the private track of these disclosures. Our experience has been we have observed vendors typically will not compete on security is the phrase. So it is a regular practice for the most part, and that is a good thing.

The CHAIRMAN. Well, that is good to hear.

We have been joined by Senator Wicker. Are you locked and loaded?

## STATEMENT OF HON. ROGER WICKER, U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Well, Mr. Chairman, I have three hearings going on at the same time.

The CHAIRMAN. I hear you.

Senator WICKER. So thanks for filibustering till I could get here.

Senator MARKEY. May I just say that I have been the person who arrived to make sure there was more time expended so that you could arrive?

Senator WICKER. You have been 5 minutes ahead of me all morning.

[Laughter.]

Senator WICKER. But I must tell you, Ed, at EPW I sort of cleaned up the mess that you left.

[Laughter.]

Senator MARKEY. And welcome again.

Senator WICKER. Who wants to talk about training smart young people to move into the field of discovering this sort of thing, the need for a larger cybersecurity workforce? How are we going to get there? Have any of you looked at my Cyber Scholarship Opportunities Act, which expands scholarships for students pursuing degrees in this area? Who wants to talk about that? Yes, sir.

Mr. SRIDHARAN. That is something that the Florida Center for Cybersecurity is very focused on, and we work with the 12 State institutions across the entire State of Florida to foster education in cybersecurity. To date, for example, just from the 12 State institutions, we have got 43 programs, graduate, undergraduate, and certificates that is offered around the State. If you take all of the educational institutions across the State, there are over 100 programs.

So it is extremely important not only to teach the students enrolled in these programs but also to create the interest in the younger generation, high schoolers and middle schoolers, who show an aptitude for cybersecurity because they are more adept at learning it very quickly than some of the older generation is. And as such, we have summer boot camps. We go and train the trainers as well as talk to the different constituents and stakeholders in the school districts to make sure that they get involved at a very young age.

We have to create a very large cybersecurity workforce. Last year, 300,000 jobs went unfilled around the Nation. 13,000 of them were in Florida alone. That is an alarming number which is going to increase exponentially. So we need to take this very seriously and create the cyber workforce that we need.

Senator WICKER. Before I turn to you, Dr. Griffiths, what salary would a young person start out at, and how much training would they need?

Dr. GRIFFITHS. There are various levels of education. Our bachelors graduates are starting at about $85,000 to $90,000. Our masters graduates are starting in the low 100s.

Senator WICKER. That ought to get somebody's attention.

Dr. GRIFFITHS. It certainly should.

But there are two other areas, in addition to what my colleague has talked about. What we do in the university sector, we are also working at two other ends of the spectrum. We are working with K through 12, with elementary schools. We have two elementary schools in Sioux Falls. We have three elementary schools and two middle schools that have a heavy computer and cyber hygiene curriculum, and we are looking potentially at extending that and broadening the base of participation. We are also working with our college of education so that every one of our education graduates has a certification in technology, which includes cybersecurity.

And then at the other end of the spectrum, we are working on workforce development. We built a set of stackable credentials working with the technical institutes, working with our school districts, and working with the State department of labor. We have got certificates which you can carry into associate degrees, which

you can carry into masters degrees. This is an approach to allow people who might not be destined for a traditional 4-year university career but sort of want to actually get an apprenticeship in industry, get some credentials while they are there, work for a couple more years, then decide to go on and add some courses to get their associate's degree, et cetera. That is addressed both to graduating high schoolers, as well as under-employed graduates of high school, as well as people who wish to change careers. And we think that also is a replicable model. We are working it in Sioux Falls, and we expect that to extend across the state and beyond.

Senator WICKER. Yes, sir. Mr. Manion?

Mr. MANION. Very briefly, as a hiring manager, I am a huge fan of the existing Federal Scholarship for Service Program that exists currently. I am not sure how it scales. I am not sure of your experiences with it. But I am very happy to see Scholarship for Service students' resumes come across my desk.

Senator WICKER. Yes, Ms. Dodson.

Ms. DODSON. The National Institute of Standards and Technology coordinates the National Initiative for Cybersecurity Education working with academia, working with K through 12 programs. And through these kinds of collaborations, we are able to share lessons learned like Dr. Griffiths' work that they are doing in South Dakota and other states.

We also have put out, with our other Federal agency partners, a guide that can be used for people who actually need this workforce to understand the kinds of skills that they need and to be better prepared to help students and to bring students together with potential employers, as well as that workforce readiness so that we are prepared not just today but we are prepared for tomorrow in the cybersecurity challenges that will face us.

Senator WICKER. Mr. Chairman, it seems that South Dakota and Florida have very excellent leadership.

[Laughter.]

The CHAIRMAN. No argument there, Senator Wicker.

Senator WICKER. I yield back.

The CHAIRMAN. Thank you, Senator Wicker.

We have been joined by Senator Blumenthal.

Senator Blumenthal.

## STATEMENT OF HON. RICHARD BLUMENTHAL, U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thanks, Mr. Chairman.

As many of us know, Intel's failure to notify the Federal Government beforehand is particularly controversial in contrast to its notification of two Chinese technology companies, namely Lenovo and Alibaba. A cybersecurity expert was quoted by the "Wall Street Journal" claiming it is, "a near certainty," that the Chinese Government was aware of Spectre and Meltdown before the U.S. Government. Given the Chinese Government's past history of exploiting cyber vulnerability, Intel's action certainly raises some serious security concerns.

Mr. Sridharan notes in his prepared remarks that, "unfortunately we have no way of knowing if it was in fact the researchers

who found it first. The attacks that exploit these vulnerabilities are difficult to detect."

Let me ask Ms. Kim and Mr. Manion, have Spectre or Meltdown been observed since the disclosure? And would these vulnerabilities have been attractive to foreign intelligence services and why?

Mr. MANION. Thank you for the question.

To my knowledge, there have been no observed attacks in the wild, just proof of concept or test code that has been tested. That is my knowledge.

In terms of the risks posed by these vulnerabilities, certainly an intelligence agency would use any means at their disposal, I would imagine, to gain their goal. However, with Meltdown and Spectre, it is necessary to already be on the computer you are trying to attack. So you would need to first gain that access. Most likely an adversary would already need a different vulnerability or a different way in to even be able to attack the Meltdown and Spectre vulnerabilities. So it might be part of a toolkit, and it certainly could be useful for reading secrets off a machine that contains that information. But again, it would be part of a chain, and by itself it does not pose an immediate risk without other vulnerabilities or exploits.

Ms. KIM. Thank you, Senator Blumenthal.

I completely agree with that. We have not seen any exploits to date, and I would stress again that we have encouraged the education and awareness of the public to make sure that they are applying the security patches and that they are vigilant about malicious code being present on the devices, which is a requirement.

Senator BLUMENTHAL. At the end of April, Arm ceded control of its Chinese operations to a joint venture run with local partners, as you may know. These chips will almost certainly be used around the world. But China has been and become less forthcoming about its vulnerabilities.

What assurances does Arm have that vulnerabilities discovered computer chips designed in China will be properly disclosed and what will Arm do to guarantee continued cooperation?

Ms. KIM. From an operational perspective, I, unfortunately, am not prepared to address that today. I can say that from a vulnerability research area, we continue to look at, across the board, global threats and work with our partners, our customers, and the industry to make sure that we are addressing the mitigations necessary. It will be something, as we have mentioned, that will continue to arise from other ongoing research, and our best efforts to be open with DHS, NIST, and other government agencies will continue as we have been since the discovery of this.

Senator BLUMENTHAL. Why are you unable to address it from an operational standpoint?

Ms. KIM. I am, unfortunately, not prepared for that. We were addressing Spectre and Meltdown. I am not necessarily into the details of the joint venture operations at this point.

Senator BLUMENTHAL. Do you regard that as important?

Ms. KIM. Absolutely.

Senator BLUMENTHAL. And would you be prepared to respond to questions in writing about it?

Ms. KIM. We can certainly respond back after this.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Blumenthal.

I do not think we have anybody else coming. So you guys will be off the hook here momentarily.

But we will keep the record open so that if members have questions they want to submit for the record, they can do that. And we will do that for 2 weeks. And I would ask, of course, Senators to submit their questions as soon as possible, and then upon receipt, if our witnesses could submit their written answers to the Committee as well as soon as possible, that would be greatly appreciated.

But I think a great hearing today, an issue that we are going to be talking about for a long time. And I think today we got a good context for what we need to be doing as we move into the future. And so we appreciate very much all of you being here and providing your insights and responding to questions to members of this Committee. But we look forward to continuing the dialogue in the future. So thank you for your good testimony, for your good work.

And with that, this hearing is adjourned.

[Whereupon, at 11:45 a.m., the hearing was adjourned.]

# A P P E N D I X

## RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO DONNA DODSON

*Question 1.* Your testimony described the utility of the National Vulnerability Database (NVD), which is administered by NIST as a repository of reported vulnerabilities found in different types of systems. According to a report produced by the cyber security firm Recorded Future, DHS's U.S. Computer Emergency Readiness Team (US–CERT) takes up to 33 days on average after the public disclosure of a software vulnerability to complete the cataloguing process and create a new entry in the database, while China's version takes on average 13 days. Are you able to describe what procedural differences might account for this longer process?

Answer. That report is not entirely correct. New vulnerabilities are posted to the National Vulnerabilities Database (NVD) as soon as the National Institute of Standards and Technology (NIST) receives them. NIST subsequently updates the entries with severity metrics, the complete range of affected platforms, remediation recommendations, and links the information to vendor alerts. Both the number of vulnerabilities in the NVD and use of the NVD continues to grow. Since January 2017, each month we have seen an average of 10 percent growth in the amount of data downloaded from the NVD. NIST is working aggressively to ensure that it can continue to provide this important information in a timely fashion.

*Question 2.* Your testimony also mentioned the expanded areas of focus like the Internet of Things that the database is expected to cover. How will the wider range of technologies included impact NIST's efforts to maintain the database, especially as database use continues to grow?

Answer. With more and more products connecting to the Internet, NIST expects the number of entries into the NVD to continue to increase. Part of our strategic planning is to ensure the continued usefulness of the NVD data by extending our ability to receive, assign metrics, and publish information that covers these new technologies. Our plans include using machine learning, natural language processing, and artificial language technologies; leveraging vendor self-scoring capabilities that are NIST verified; training and hiring new vulnerability analysts; and extending the used standards to cover new technologies. We are projecting our future needs for maintaining the NVD based on, not only a historical view, but the projected growth of technologies like the Internet of Things.

*Question 3.* As it relates to identifying cybersecurity vulnerabilities within our Federal agencies, modernizing the Federal Government's IT systems needs to remain a top-priority. According to the GAO's High Risk Series report, the Federal Government annually spends over $80 billion on information technology (IT), but more than 75 percent of this spending is for "legacy IT." The Modernizing Government Technology (MGT) Act was signed into law last year in an effort to bolster agencies' capabilities to defend themselves from cyber threats at home and abroad by replacing outdated and vulnerable systems. Could you please describe the threat that "legacy IT" specifically poses to Federal agencies' cyber infrastructure?

Answer. Legacy information technology poses risks to an organization's infrastructure for several reasons. Often legacy software and hardware are more susceptible to malware. Sometimes there are no patches, updates or technical support for legacy software and hardware for remediation when a vulnerability is discovered. NIST continues to provide guidance to agencies managing risk across their organization to assist with the challenges of "legacy IT" while encouraging organizations to update software and hardware and maintain a rigorous program to patch these products.

*Question 4.* My subcommittee has held hearings on private and public sectors' use of "bug bounty programs" to incentivize the expertise of outside cybersecurity researchers to identify cyber vulnerabilities in a timely fashion. Can these types of arrangements be used to in supply chain cybersecurity disclosures? If not, why?

Answer. Yes, bug bounty programs may provide an additional and valuable capability for organizations to identify vulnerabilities in their supply chains. However, these types of programs frequently require organizational, technical, and legal infrastructures, as well as a skilled and knowledgeable workforce, to help them achieve the desired outcome in a manner that protects the organization. NIST generally encourages research into tools and processes that support greater visibility and understanding of cyber supply chain risks. NIST also encourages organizations to share incident handling activities related to supply chain incidents with supply chain partners.

*Question 5.* Your testimony covered the stakeholder engagement following the development of the Cybersecurity Framework. As outside comments and feedback from workshops continue to shape the Framework (including the expansion to supply chain guidance), what do you see as the next step to effectively promoting coordinated vulnerability disclosure among private and public stakeholders?

Answer. With subject matter such as supply chain risk management (SCRM) and coordinated vulnerability disclosure (CVD) incorporated into the Cybersecurity Framework, NIST will advocate of the adoption of the Cybersecurity Framework both nationally and internationally which will help increase awareness and understanding of CVD. This awareness and understanding will naturally help organizations implement more detailed guidance such as NIST Special Publication 800–161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations. Further, basic dialogues about CVD can be enriched through International Organization for Standardization (ISO) and Forum of Incident Response and Security Teams (FIRST) guidance.

*Question 6.* As NIST's Supply Chain Risk Management Program continues to work with private and public stakeholders to identify best practices and standards related to the supply chain ecosystem, could you please describe how interoperability of technologies is accounted for in these considerations? Are you able to give specific supply chain examples where interoperability has a pronounced role?

Answer. An interoperable supply chain platform (automated digital processes that help buyers and suppliers integrate and optimize their order and delivery processes) is essential to most organizations' supply chain infrastructure. Since supply chain platforms are often a system-of-systems that involve order management, returns management, sourcing, finance, inventory visibility, transportation management, and warehouse management—all of which may involve various physical and digital technologies—it is necessary that each of these sub-systems interoperates for an organization's supply chain infrastructure to function seamlessly. NIST has case studies available that discuss supply chain platforms and interoperability, for example, NIST's case studies on Exostar and Smart Manufacturing are available at: *https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/Best-Practices.*

---

## Response to Written Questions Submitted by Hon. Maria Cantwell to Donna Dodson

*Question 1.* I don't think these are new or complex ideas, but at hearing after hearing on this topic, experts put out the call for national coordination to advance these initiatives. According to Department of Homeland Security there were 290 cyber-attacks on our Nation's critical infrastructure in 2016.

I am particularly worried about our energy grid and the integrity of our voting infrastructure in the absence of a robust national strategy. What are the ingredients to an effective national strategy?

Answer. The Trump Administration is focused on the issue of cybersecurity, and in particular cybersecurity for critical infrastructure. On May 11, 2017 President Trump issued Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructures. EO 13800 directed a coordinated, whole of government response to cybersecurity threats, and has resulted in numerous actions by the Administration to strengthen our cyber-defenses. The reports provided by the Department of Commerce, Department of Homeland Security, Department of Energy, Department of Defense, and other government agencies were used to inform the National Security Strategy that the President adopted on December 17, 2017. The work directed by EO 13800 and the National Security Strategy provide an appropriate framework with the essential ingredients for deterring and responding to cyberthreats.

The Trump Administration understands that our economic and national security depend on how we respond to challenges in cybersecurity. In September, the Trump Administration published the National Cyber Strategy—the first fully articulated cyber strategy in 15 years. Among other things, the National Cyber Strategy sets

forth how the U.S. will protect the American people, the homeland, and the American way of life as well as promote American prosperity. These efforts specifically commit to protecting our democracy and securing our democratic processes as well as prioritize risk reduction activities in key areas like energy.

*Question 2.* Where should responsibility for implementing a national strategy lie? Is there a legislative solution that would work here?

Answer. As detailed in the response to question 1, President Trump is directing a comprehensive, whole of government effort to improve America's cyber capabilities. EO 13800 and the National Security Strategy are two milestones in that effort, which is ongoing and evolving as new threats emerge.

NIST's role in cybersecurity is to research and develop information security standards to protect information systems. A key example of this role can be seen in NIST's role in developing and promoting the Cybersecurity Framework. *We are willing to work* with the White House and other agencies to consider questions around responsibilities for national strategies and related legislative needs.

The Trump Administration recognizes that the responsibility of securing cyberspaces requires administration efficiency across the entire Federal Government, as well as collaboration with the private sector.

*Question 3.* Can you lay out what you think is necessary to ensure we have the cybersecurity workforce we need to be safe and secure?

Answer. The Trump Administration is focused on the issue of cybersecurity, and in particular cybersecurity for critical infrastructure. On May 11, 2017 President Trump issued Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructures. EO 13800 directed a coordinated, whole of government response to cybersecurity threats, and has resulted in numerous actions by the Administration to strengthen our cyber-defenses. The reports provided by the Department of Commerce, Department of Homeland Security, Department of Energy, Department of Defense, and other government agencies were used to inform the National Security Strategy that the President adopted on December 17, 2017. The work directed by EO 13800 and the National Security Strategy provide an appropriate framework with the essential ingredients for deterring and responding to cyberthreats. The report is available at *https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf*.

In addition to the recommendations in the report, here at NIST we are taking a multifaceted approach that includes aggressively pursuing the strategic goals of the National Initiative for Cybersecurity Education (NICE) to 1) accelerate learning and skills development to create a sense of urgency in the public and private sectors to make cybersecurity education and training a higher priority, and 2) nurture a diverse learning community to take a long-term view of the pipeline needed to create the cybersecurity workforce needed in the future.

*Question 4.* What else can the government and private sector do to fill this very pressing cybersecurity skills gap?

Answer. As recommended in the May 2018 Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (available at *https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf*), one strategy for the Federal Government is to ensure ongoing support for the CyberCorps Scholarship for Service Program that provides a steady stream of students to the Federal Government who provide service in return for the compensation that they receive in the form of tuition, room and board, and fees. A second strategy recommended in the report is to ensure that Federal pay and benefits are competitive with what job seekers can obtain from private sector employers. Finally, we must commit to developing Federal employees through training, rotational assignments, exchange programs with industry, and other creative efforts that creates a workforce with up-to-date skills and the motivation to remain in Federal service.

*Question 5.* The North American Electricity Reliability Corporation, or NERC, has said that they are aware of these vulnerabilities, but they do not expect them to have operational impacts on the energy industry. The Energy Information Sharing and Analysis Center (ISAC) has confirmed that they sent a warning about the vulnerabilities to members of their information sharing portal.

While it is not likely that the energy sector is the prime target of actors trying to exploit these vulnerabilities, it is true that on some level, all infrastructure sectors are at risk.

Given what we know about the hardware weaknesses presented by these two cyber vulnerabilities, what industries would you say are both:

(a) most vulnerable because of a lack of mitigation efforts? and

(b) a disruption in that industry would have the greatest effect on the Nation's health and safety?

Answer. NIST's role in cybersecurity is to research and develop information security standards to protect information and information systems. Our role is non-operational, and we defer to DHS and those agencies with operational roles to assess which sectors are most vulnerable and disruption of which would have the greatest effect on the Nation's health and safety.

---

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TOM UDALL TO DONNA DODSON

*Question.* Far too many Americans are killed and seriously injured on our Nation's roads each year. I am hopeful that someday connected vehicle technology and autonomous vehicles may help to reduce this preventable death and injury toll. However, I am deeply concerned that these advanced vehicle technologies will be vulnerable to hacking without proper safeguards in place, and therefore endanger motorists and road users on a whole new level.

Are you concerned that connected and autonomous vehicles will be targets for malicious hackers including possibly terrorists? What are the potential implications and risks associated with a cyber-attack of these vehicles? Could you provide this Committee with examples of cybersecurity standards that are in place in other industries that have been successful? What types of benefits have been realized by requiring such safeguards?

Answer. Whenever we see an increase in connectivity and reliance on automation, there are increased concerns about the possibility of malicious activity. The possible attacks can range from violations of privacy and trust to loss of life. We have already seen and addressed these concerns in other areas. For example, there are extensive cybersecurity regulations in the nuclear industry issued by the Nuclear Regulatory Commission. The Department of Energy and the National Institute of Standards and Technology have been assisting with the development and implementation of cybersecurity controls under the North American Electric Reliability Corporation Critical Infrastructure Protection plan. While no technical standard or regulation can remove all risk, the use of technical standards developed in open, transparent and consensus-based processes can increase the security of a sector. Since, like the grid, the automated transportation sector will be interconnected, development of standards would help further a common understanding and acceptance of basic cybersecurity. Currently, industry and government are working on autonomous vehicle security in standards bodies, such as SAE international, the Alliance for Automotive Manufacturers, the Association of Global Automakers and the Auto ISAC. NIST will continue to work with the Department of Transportation as they implement safety and cybersecurity plans called for in the DOT's *Preparing for the Future of Transportation, Automated Vehicles.*

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO DONNA DODSON

*Question 1.* Small Business Cybersecurity: We have over 240,000 small businesses in Nevada and they're really worried about cybersecurity, it's something I hear about most often from them. With the inter-connectedness of our economy now a small business can be vulnerable even when they're not directly attacked because their information can be shared with a large company who is more likely to be a victim. This leaves them very vulnerable and since they often don't have a lot of resources to combat cyber threats, they don't have a lot of options for increasing security.

Can you speak to how viable cyber security type programs, like bug bounties for example, or others, are for small and medium sized businesses?

Answer. Yes, bug bounty programs may provide an additional and valuable capability for organizations to identify vulnerabilities in their supply chains. However, these types of programs frequently require organizational, technical, and legal infrastructures, as well as a skilled and knowledgeable workforce, to help them achieve the desired outcome in a manner that protects the organization. NIST generally encourages research into tools and processes that support greater visibility and understanding of cyber supply chain risks. NIST also encourages organizations to share incident handling activities related to supply chain incidents with supply chain partners.

This necessary infrastructure may make it more challenging for some organizations, including small-and medium-sized businesses to leverage and benefit from these types of programs. However, other groups have tailored programs for small-and medium-sized businesses, including the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), Small Business Administration (SBA), the Federal Bureau of Investigation's (FBI) InfraGard program, and the National Cyber Security Alliance that offer valuable resources to these organizations.

*Question 2.* What does NIST do, specifically, to help out small businesses?

Answer. The National Institute of Standards and Technology (NIST) has a long-standing and on-going effort supporting small business cybersecurity. NIST's Small Business Cybersecurity Program collaborates with Federal and other partners to understand the cybersecurity needs of small businesses and identify and/or develop guidelines, practices, and other resources to meet those needs. Small businesses may find *Small Business Information Security: The Fundamentals* (NIST Interagency Report 7621 Rev. 1) a valuable publication for understanding important cybersecurity activities. This publication is available at NIST's Computer Security Resource Center Web Site (www.csrc.nist.gov), specifically *https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final* and works in coordination with the Cybersecurity Framework.

Additionally, NIST collaborates with the Department of Homeland Security, the Federal Trade Commission, the Small Business Administration, the FBI's public-private partnership InfraGard program, and non-governmental organizations to conduct outreach to small businesses across the country. NIST, working through its Hollings Manufacturing Extension Partnership Program, also communicates the importance and availability of cybersecurity standards and best practices to small manufacturers across the Nation.

NIST looks forward to continuing to work with small-and medium-sized businesses.

*Question 3.* What else can we do federally to help these businesses prepare for cyber-attacks?

Answer. The Federal Government can continue to work closely with industry and other stakeholders to raise small business cybersecurity awareness and highlight the resources that are available to help them understand and manage cybersecurity risks. This work should include continued and increasing engagements between DHS's NCCIC, sector-specific agencies, and their industry stakeholders. NIST will continue to develop and issue additional best practices and other resources with small business concerns in mind. NIST, working with government and industry partners, can also provide practical examples of solutions at its National Cybersecurity Center of Excellence that are tailored to small-and medium-sized businesses that have limited technical capabilities, time, and resources.

*Question 4.* Do you have the ability to work with the Small Business Administrations in the states to aid these small businesses?

Answer. Yes, NIST regularly collaborates with SBA and Small Business Development Centers as well as other Federal and private sector partners to understand the needs of small-and medium-sized businesses and develop guidelines, practices, and other resources to meet those needs. These efforts help small-and medium-sized businesses understand and effectively manage cybersecurity risks to their business objectives.

*Question 5.* Cybersecurity Workforce Development: One reported estimate is that the gap in the needed pool of cyber professionals could be as large as 1.8 million by 2022.

What would you recommend we focus on to make progress on this challenging issue?

Answer. The Trump Administration is very focused on the challenges presented by the changing cybersecurity workforce landscape. On May 11, 2017 President Trump issued Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructures. Section 3(d) of Executive Order 13800 directed the Secretary of Commerce and Secretary of Homeland Security to jointly assess the needs and challenges facing the United States with respect to the cybersecurity workforce and submit a report. The joint Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce included recommendations and specific actions that could to improve the situation. The report is available at *https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf*

The 1.8 million workforce shortage by 2022 (from ISC2 Information Security Global Workforce Study) is a global estimate. CyberSeek.org, funded by NIST, estimates

that there are currently 301,000 open cybersecurity jobs in the United States. This gap represents jobs that span entry-level through advanced-level positions. In addition to the recommendations in the report, NIST is taking a multifaceted approach that includes aggressively pursuing the strategic goals of the National Initiative for Cybersecurity Education (NICE) to (1) accelerate learning and skills development to create a sense of urgency in the public and private sectors to make cybersecurity education and training a higher priority; and (2) nurture a diverse learning community to take a long-term view of the pipeline necessary to create the cybersecurity workforce needed in the future.

*Question 6.* Blockchain and AI: Nevada has been a leader in developing various blockchain startups. This kind of activity across the country has led us to include policy in the 2017 defense bill that included a provision to allow the public sector to invest in modernization projects that could include the use of blockchain technology. This development is coming as we see exciting developments in Artificial Intelligence.

Can you speak to the potential of how blockchain and AI technologies may be used to help improve security and efficiency within the public and private sectors?

Answer. New technologies being used by the public and private sector have great potential to improve security and efficiency across our economy and to improve our daily lives. Artificial Intelligence (AI) technologies are a further step that can improve the efficiency of some of our more pressing cybersecurity challenges as well as help grow our economy. The use of AI can enhance or even replace many manual cybersecurity tasks that are time consuming and error prone. This can speed the ability to identify vulnerabilities, anomalies, and threat activity and assist in closing the time gaps between identifying these issues and responding to them. We also must be cognizant that AI systems and other technological advances can be used to compromise cybersecurity approaches.

Blockchain technology is still being explored in many different use cases for many different business purposes. This type of distributed ledger can help with the security issues through improved information integrity, by recording transactions publicly so that they cannot be changed once published. Blockchain technologies can provide a foundation of trust in data or activity occurring in our digital world.

Both AI and blockchain are still emerging and NIST will continue to work with industry and the other Federal agencies on their application, while also conducting research in the foundational technologies that will allow us to maximize their potentials.

*Question 7.* IoT: In recent months, the FBI has warned of sophisticated Russian-linked hacking campaigns could be infecting hundreds of thousands of routers and home network devices around the world. As we move to the Internet of things, where nearly everything is connected, it will be even more important to deter data breaches.

What special considerations should be given as we move towards an economy powered by this technology?

Answer. Internet-connected devices generally sense, collect, process, and transmit a wide array of data, ranging from consumer personally identifiable information to proprietary company data to infrastructure data used to make critical real-time decisions or to effect a change in the physical world. Just as there are a variety of new uses, the Internet of Things (IoT) ecosystem's nature brings new security and privacy considerations. These considerations include—but are not limited to—constrained power and processing; the ability to manage, update, and patch devices at scale; and a diverse set of new applications across consumer and industrial sectors.

Unlike personal computing devices, many IoT devices have highly predictable communication patterns. Alone this could create vulnerabilities in the use of these devices, but with proper network traffic management, the use of devices for malicious purposes can be highly constrained. If widely deployed, such traffic management techniques could prevent attackers from compromising IoT devices and limit the impact of devices that are compromised.

The Internet Engineering Task Force standards body is working to standardize those patterns and create the management technologies used to manage these devices. NIST is actively supporting this standards effort.

NIST also recently released a draft report, NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks for public comment. Draft NISTIR 8228 identifies high-level considerations that may affect the management of cybersecurity and privacy risks for IoT devices compared to conventional information technology (IT) devices.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JON TESTER TO DONNA DODSON

*Question 1.* Government Notification: Reports indicate that when Intel discovered the Spectre and Meltdown vulnerabilities, firms first notified Chinese technology companies Lenovo and Alibaba. However, the U.S. Government only found out about these vulnerabilities after the security vulnerabilities became public.

Hiring top cybersecurity talent at DHS is challenging due to Federal hiring logjams—including security clearance delays, salaries, and private sector competition.

(A) What strategies should we implement to improve the Federal Government's cybersecurity workforce at agencies such as DHS?

Answer. The Joint Department of Commerce—DHS Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (available at *https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf*), contains 20 recommendations, each of which would improve the Federal Government's cybersecurity workforce. For example, supporting CyberCorps: Scholarship for Service Program, ensuring that compensation for Federal employees is competitive with what they could earn from private sector employees, and committing to developing Federal employees through training, rotational assignments, exchange programs with industry.

*Question 2.* How do we keep pace with geo-strategic competitors such as Russia and China?

Answer. Cybersecurity threats pose a persistent economic and national security challenge to the Nation while also impacting individual firms and their customers. The Trump Administration takes these challenges seriously and took a major step toward addressing these challenges when the President signed Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical infrastructure.

Executive Order 13800 directed the Secretary of Commerce and Secretary of Homeland Security to jointly assess the needs and challenges facing the United States with respect to the cybersecurity workforce and submit a report. The joint Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce included recommendations and specific actions that could to improve the situation. The report is available at *https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf*

As discussed throughout the report, one of the most important ways we can keep pace with geo-strategic competitors is through the development of a well-educated and well-trained cybersecurity workforce. It is critical to continue American leadership in science, technology, engineering, and mathematics fields. The report highlights The National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE), which is a partnership between government, academia, and the private sector that seeks to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with public and private sector partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals.

This Administration's commitment to cybersecurity was further demonstrated in September the publication of the National Cyber Strategy—the first fully articulated cyber strategy in 15 years. Among other things, the National Cyber Strategy sets forth how the U.S. will protect the American people, the homeland, and the American way of life as well as promote American prosperity.

*Question 3.* Human Element: Software patches are only as good as the person installing them. Most folks out there aren't nearly as tech savvy or as familiar with cyber-hygiene best practices as the folks on this panel. This whole system of patches and updates seems to break down when the average user is not aware of the problem, does not take the time to install updates or even know how to do so.

How would you recommend U.S. consumers, businesses and government entities—including Congress—better equip ourselves and the American people for the ever-changing cyber vulnerabilities we face?

Answer. Cybersecurity awareness continues to be an important tool to better equip users (including consumers, businesses, and government entities) to understand cybersecurity vulnerabilities in the context of their digital interactions. Beyond awareness, it is critical that the cybersecurity capabilities built into products, technologies and services continue to improve, and provide users with greater security at the time of market availability. This includes, for example, ensuring that IoT devices can be upgraded and patched remotely, as well as greater use of automation to simplify and improve the processes by which users are advised about the cybersecurity implications of the products and technologies they use.

*Question 4.* What role should private industry play in making the average consumer aware of cyber vulnerabilities to their software or hardware, whether it on their CPU, smartphone, or car? What role do you believe should the U.S. Government should play?

Answer. Raising consumer awareness of cybersecurity vulnerabilities requires public and private collaboration, and a sustained multidisciplinary approach that provides consumers with simple and actionable information. The government, private sector, and non-profits—individually and in collaboration—have current and active programs and approaches to raise consumer awareness of cybersecurity vulnerabilities and increase consumer understanding of their role in protecting products, technologies, and networks, as users that rely on the Internet and digital ecosystem. Some examples of this work can be found at places such as DHS's STOP. THINK. CONNECT Campaign, the Anti Phishing Working Group, local Information Security and Audit Control Association (ISACA) chapters, local FBI InfraGard chapters, and by the FTC to just name a few.

---

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. JERRY MORAN TO JOYCE KIM

*Question.* My subcommittee has held hearings on private and public sectors' use of "bug bounty programs" to incentivize the expertise of outside cybersecurity researchers to identify cyber vulnerabilities in a timely fashion. Can these types of arrangements be used to in supply chain cybersecurity disclosures? If not, why?

Answer. In short, yes. As you correctly point out, bug bounty programs serve a valuable purpose in that they incentivize researchers to identify and responsibly notify affected companies of potential vulnerabilities in products so the companies can address the problem. Often the existence of a bug being brought to a company by a researcher, either through a bug bounty program or not, begins the process of assessing the vulnerability, developing any necessary mitigation, distributing the mitigation, and ultimately making a public disclosure about the vulnerability. Thank you for your work on, and support of, bug bounty programs as they contribute to responsible cybersecurity practices.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO JOYCE KIM

*Question 1.* I don't think these are new or complex ideas, but at hearing after hearing on this topic, experts put out the call for national coordination to advance these initiatives. According to Department of Homeland Security there were 290 cyber-attacks on our Nation's critical infrastructure in 2016.

I am particularly worried about our energy grid and the integrity of our voting infrastructure in the absence of a robust national strategy. What are the ingredients to an effective national strategy?

Answer. Arm takes its role in secure product design very seriously. That said, as a processor design company we develop foundational technology, and do not provide complete information technology systems so are not in the position to provide expert perspective on system security.

*Question 2.* Where should responsibility for implementing a national strategy lie? Is there a legislative solution that would work here?

Answer. Again, Arm can only speak from the perspective of an upstream supplier of processor designs, however, NIST and DHS are both doing significant work in this space and have significant expertise in this area.

*Question 3.* Can you lay out what you think is necessary to ensure we have the cybersecurity workforce we need to be safe and secure?

Answer. In general, there is a widely reported and recognized shortage of workers with cybersecurity training. This makes individuals with these skills very valuable to private and public sector employers. The November 2017 report from the Secretary of Commerce and the then-Acting Secretary of the Homeland Security entitled *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future,* makes many good recommendations to address these concerns. Further, legislation such as *S. 754, the Cyber Scholarship Opportunity Act of 2017* and fully funding Federal programs like the Department of Defense's Cybersecurity Scholarships program will help address these issues. Additionally, programs like the National Institute of Standards and Technology's *National Initiative for Cybersecurity Education* (NICE)

are doing great work to increase the number of students and individuals in cybersecurity related fields.

*Question 4.* What else can the government and private sector do to fill this very pressing cybersecurity skills gap?

Answer. As you noted at the Washington Post event on Artificial Intelligence earlier this year, workforce needs and education are constantly evolving. The U.S. K–12 educational system has made great strides in better educating students with science, technology, engineering, arts and mathematics skills, but there is still much work to do. As the use of technology proliferates in every sector, it is going to be increasingly important that workers in all fields have these skills, including cybersecurity skills. The Federal Government needs to ensure all educational programs make these increasingly essential skills a priority. Private sector partnership from technology companies also contributes to addressing this gap as it focuses on addressing skills that are in high demand. Arm currently partners with universities in the U.S. and is exploring K–12 programs around preparing teachers to educate students on STEM skills.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO JOYCE KIM

*Question 1.* In your testimony, you recognize the need to inform the U.S. Government earlier in the process—testimony that could contradict other industry stakeholders. Are you concerned that "pre-disclosure" to the U.S. Government could result in more aggressive "pre-disclosure" pressure from foreign actors?

Answer. We do think strict requirements from the U.S. Government—such as requiring companies to notify the U.S. Government as soon as a vulnerability is discovered or requiring companies to turn over technical details of vulnerabilities—would lead to similar requirements elsewhere. This would defeat the overall purpose of coordinated vulnerability disclosure and undermine one of the key principles provided in all widely utilized CVD guidance, which is to only share information with those entities that can contribute to mitigating the issue.

We recognize, however, the U.S. Government has a role in providing information to the public and protecting its own systems. We believe allowing flexibility for companies to determine the appropriate time to engage the government to help them do this is the best path forward. From Arm's perspective, we now acknowledge that time is before public disclosure, but there needs to be flexibility as each vulnerability is unique and no two responses will be the same including the timeline on which mitigations will be developed.

*Question 2.* Do you agree with some industry assessments that "pre-disclosure" notice to a non-regulatory agency such as NIST would spur other foreign governments to force "pre-disclosure"?

Answer. Yes, it is reasonable to assume rigid pre-disclosure requirements to any government entity would be replicated in other countries.

*Question 3.* Sandia National Laboratory, located in New Mexico, conducts a significant amount of research on chip integrity and other cybersecurity work. Do you believe that our national laboratories can serve as clearinghouses for these kind of complex cybersecurity vulnerabilities?

Answer. Arm works closely with Sandia National Laboratory on a number of projects and values the relationship and tremendous work done at the Laboratory. In particular, we were pleased to contribute to the announcement in June 2018 of the Astra Supercomputer, which will be the most powerful Arm-based supercomputer in operation.

Currently the National Institute of Standards and Technology acts as a clearinghouse for all know vulnerabilities by maintaining the National Vulnerability Database. We believe there is value in having one single entity maintain a complete list of known vulnerabilities.

*Question 4.* The public could overreact to a problem—but under-protect their computers and devices. Do you have an idea how many customers fully installed security patches recommended by your company? How did you assist users of your chips to fully comply with security patches?

Answer. Due to our position in the supply chain, we design processors but do not manufacture chips, we are several steps removed from end user devices so cannot state with any certainty how many customers installed the security mitigations. Due to this, we had to work closely with our business customers to ensure they could pass the mitigations on to their customers, whether they be additional business partners in the supply chain or end users.

*Question 5.* In Dr. Griffiths' testimony, she called for labeling components' countries of origin for technology. Do you agree that this could help consumers become better informed about the need for strong cyber-hygiene practices? Are there other ways to help consumers develop these practices?

Answer. Although nearly all of our products are designed in the United States and the United Kingdom, we do not support country of origin labelling. Device security and integrity depend more on how a product is made than where it is made. The U.S. Federal Government has required component country of origin disclosure for certain types of information technology, however, even that is generally only for high-impact systems. The Federal Trade Commission has done and continues to do significant work to educate consumers on cyber-hygiene through public awareness campaigns, public events, social media content, and numerous other methods. That work should be continued and bolstered. The private sector is also taking steps to remove the "human factor" from cyber-hygiene, particularly insecure passwords, though greater use of features like fingerprint or facial recognition biometric authentication, voice-recognition technology, and even technology that can recognize patterns in a user's gait.

*Question 6.* Some Spectre vulnerabilities were present in processors from multiple vendors. What barriers, if any, are there to sharing information with competitors, the government, or academia? Is there sufficient information sharing to develop mitigations as quickly as possible?

Answer. From Arm's perspective, there were no impediments to collaboration, and there was close and frequent communication to ensure the issues were addressed in a timely manner.

*Question 7.* For hardware security issues, how long does it take to develop a mitigation and how long does it take for that mitigation to penetrate the market?

Answer. It is hard to generalize as each vulnerability is unique. For the initial Spectre and Meltdown vulnerabilities it took longer than the 90 days Google Project Zero typically gives companies when they discover a vulnerability. For Spectre Variant 4 which was publicly disclosed in May 2018, Arm had mitigations ready within 90 days. Again, given we only provide mitigations to our customers, not end users, we could not say with any certainty how long it takes to penetrate the market.

*Question 8.* Public disclosure prior to mitigations being in-place can put information and systems at significant risk. For major hardware vulnerabilities, what is your process for disclosure to the U.S. Government, foreign governments, industry partners, and the public?

Answer. Arm's only experience handling vulnerabilities has been this experience with Spectre and Meltdown. In this instance, after receiving the vulnerability, Arm determined in less than a week it was theoretically possible it could be exploited on a rather small percentage of Arm's processor designs. As detailed in my testimony, Arm then contacted its customers that license Arm designs and modify them; this was necessary to determine if their implementation of Arm's designs would be impacted from the vulnerability. Some customers implement Arm's processor designs without modification; these customers were notified later as we did not need to ascertain additional information to begin work on mitigations for them. Google Project Zero notified the public of the original Spectre and Meltdown vulnerabilities on January 3, 2018. Spectre Variant 4 was made public May 21, 2018. Spectre Variant 1.1 and Variant 1.2 were made publicly available July 10, 2018.

*Question 9.* To provide industry time to develop mitigations, do you have effective mechanisms to maintain information embargos?

Answer. We at Arm did not put "embargos" on any of our customers around Spectre and Meltdown, rather we viewed the vulnerabilities as sensitive information that should not be widely disclosed. No one in the technology industry wants their product to be exploited so when a vulnerability is found companies treat that information with the utmost sensitivity. We communicate with our customers to determine if their implementations of our designs are affected which allows us to provide effective mitigations. If they deem it necessary to talk to their customers to properly address the vulnerability, they are free to do so.

*Question 10.* Speculative execution is both the underlying cause of the Spectre family of vulnerabilities and a common technique for high-performance processing. What are the risks posed by industry converging on similar designs?

Answer. As I mentioned in my testimony, the vast majority of Arm processor designs were not affected by these vulnerabilities, but we are not taking that for granted and are working to design our products with security at the forefront of our thinking. Arm has taken this very seriously. Internally, we are revisiting assumptions we previously had about the security of our products. We are engaging in industry groups and broader partnerships to ensure a wide range of perspectives are

considering as many avenues as possible through which products could be exploited by bad actors.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO JOYCE KIM

*Question 1.* Cybersecurity Workforce Development: One reported estimate is that the gap in the needed pool of cyber professionals could be as large as 1.8 million by 2022.

What would you recommend we focus on to make progress on this challenging issue?

Answer. I would reiterate the responses I gave to Senators Cantwell and Tester on cybersecurity workforce shortages. I would also point to the work and policy recommendations of groups like CompTIA, of which Arm is a member. A recent CompTIA report entitled *The Evolution of Security Skills* provides recommendations both the private and public sector can take to improve skilled cybersecurity professionals in the workforce.

At a higher level, Arm believes all students need to be gaining more skills in science, technology, engineering, arts and mathematics and work with universities, non-profits, and other stakeholders to provide tools and training to improve those programs.

*Question 2.* Blockchain and AI: Nevada has been a leader in developing various blockchain startups. This kind of activity across the country has led us to include policy in the 2017 defense bill that included a provision to allow the public sector to invest in modernization projects that could include the use of blockchain technology. This development is coming as we see exciting developments in Artificial Intelligence.

Can you speak to the potential of how blockchain and AI technologies may be used to help improve security and efficiency within the public and private sectors?

Answer. Artificial intelligence (AI) in particular has the potential to make drastic improvements in cybersecurity. The Department of Defense's Defense Advanced Research Projects Agency (DARPA) for instance has funded competitions to create AI cybersecurity tools to automatically scan and detect product vulnerabilities. Other AI is being developed to better predict cyberattacks based on a greater capability to monitor and analyze network activity. Blockchain, while not a key business interest for Arm currently, also has the potential to improve security in numerous ways from providing more secure authentication of IoT devices to securing sensitive information.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JON TESTER TO JOYCE KIM

*Question 1.* Government Notification: Reports indicate that when Intel discovered the Spectre and Meltdown vulnerabilities, firms first notified Chinese technology companies Lenovo and Alibaba. However, the U.S. Government only found out about these vulnerabilities after the security vulnerabilities became public.

Could you describe some of the changes Arm has made to this notification process to the U.S. Government since the Google Project Zero disclosure earlier this year? Will Arm commit to notify the U.S. Government a priori foreign entities?

Answer. Arm has established a working relationship and ongoing dialogue with the U.S. Department of Homeland Security which we did not have prior to the discovery and disclosure of these vulnerabilities. As I discuss in response to a question from Senator Udall, Arm is working with the U.S. Government more proactively than was done when addressing the original Spectre and Meltdown vulnerabilities, however, committing to work exclusively with one government will likely lead to governments in other countries where Arm operates mandating similar cooperation. As a company founded and headquartered in the United Kingdom, many of Arm's UK-based employees were at the forefront of Arm's validation and handling of these vulnerabilities. Following the first vulnerabilities being disclosed in January, we have developed a collaborative working relationship with the U.S. Government and will commit to working with them as well as all impacted customers in a timely manner.

*Question 2.* What are Arm's top priorities when vulnerabilities such as Spectre and Meltdown are discovered? Please describe ARM's procedures when vulnerabilities are discovered?

Answer. As I mentioned in my testimony, these events were unprecedented for the industry and it was the first time in Arm's history as a company, as well as the industry, dealt with such vulnerabilities. Arm's priority in its response was to timely: (1) validate the vulnerabilities and determine which Arm products could be affected, (2) work with our customers to understand how the vulnerabilities affected their products as Arm's processor designs are used in different ways, (3) develop mitigations that addressed the issue with minimal impact on end users, and (4) work with downstream business partners to distribute the mitigations.

Arm has since codified our internal response process based on the publicly available ISO standards for vulnerability handling and disclosure cited in my testimony. Additional information can be found here: *https://www.arm.com/security.*

*Question 3.* Hiring top cybersecurity talent at DHS is challenging due to Federal hiring logjams—including security clearance delays, salaries, and private sector competition. (A) What strategies should we implement to improve the Federal Government's cybersecurity workforce at agencies such as DHS? (B) How do we keep pace with geo-strategic competitors such as Russia and China?

Answer. I would reiterate my response to Senator Cantwell's question about addressing the general shortage of workers with cybersecurity training. There are a number of promising Federal programs in place that need to be fully funded. With respect to Federal hiring specifically, I would also add that industry groups like CompTIA, of which Arm is a member, advocate for updating Federal hiring requirements as on the job training or industry recognized certifications may often be as, or more, appropriate for certain types of cybersecurity work than a traditional four year degree.

*Question 4.* Human Element: Software patches are only as good as the person installing them. Most folks out there aren't nearly as tech savvy or as familiar with cyber-hygiene best practices as the folks on this panel. This whole system of patches and updates seems to break down when the average user is not aware of the problem, does not take the time to install updates or even know how to do so.

How would you recommend U.S. consumers, businesses and government entities—including Congress—better equip ourselves and the American people for the ever-changing cyber vulnerabilities we face?

Answer. Every user of technology needs to be aware of basic best practices for online safety and cyber hygiene. The Federal Trade Commission provides numerous resources and has many consumer awareness campaigns to provide such education. The Department of Homeland Security, the Small Business Administration, and the National Institute of Standards and Technology (NIST) also provide valuable resources to businesses of all sizes on organizational security. In particular, the NIST Cybersecurity Framework is widely recognized as one of the best guidance documents available for how to approach organizational cybersecurity, and was recently updated to include information on vulnerability disclosure, among other things.

*Question 5.* What role should private industry play in making the average consumer aware of cyber vulnerabilities to their software or hardware, whether it on their CPU, smartphone, or car? What role do you believe should the U.S. Government should play?

Answer. I would start by clarifying Arm does not sell products to end users, our customers are other businesses so I don't speak from the perspective of a company that sells products directly to the average consumer. That said, I think it is important for consumers to have accurate, timely information about the security of the products they are utilizing. Many companies that do sell to end users are increasingly making security updates automatic so consumers' products have the latest security features available.

---

## Response to Written Questions Submitted by Hon. Jerry Moran to Art Manion

*Question 1.* My subcommittee has held hearings on private and public sectors' use of "bug bounty programs" to incentivize the expertise of outside cybersecurity researchers to identify cyber vulnerabilities in a timely fashion. Can these types of arrangements be used to in supply chain cybersecurity disclosures? If not, why?

Answer. Although they are closely related, vulnerability disclosure programs are a necessary prerequisite to bug bounties. A bug bounty adds financial incentives to a vulnerability disclosure program. Bug bounties can be useful to focus researcher attention on finding vulnerabilities at an optimal point in the development lifecycle (for example, Microsoft has used bug bounties to motivate vulnerability reports during the beta phase for new versions of software rather than waiting for post-release

reports to trickle in). Bounties can also be used to focus attention on specific software products or components, such as the Department of Defense Vulnerability Disclosure Program scoped to cover internet-facing DoD websites. But a bug bounty alone will not lead to addressing of vulnerabilities unless it is backed by a well-functioning coordinated vulnerability disclosure program that includes deploying fixed software.

A bug bounty could be used to discover vulnerabilities in supply chain components like common libraries or protocols; however, the complexity arises in the resulting coordinated disclosure process, not the bounty program itself. A bounty program aimed at supply chain components may need to consider longer embargos and the question of who owns the program and pays the bounty. Open source projects that create many supply chain components often cannot afford to operate or pay for bounty programs.

*Question 2.* As it relates to identifying cybersecurity vulnerabilities within our Federal agencies, modernizing the Federal Government's IT systems needs to remain a top-priority. According to the GAO's High Risk Series report, the Federal Government annually spends over $80 billion on information technology (IT), but more than 75 percent of this spending is for "legacy IT." The Modernizing Government Technology (MGT) Act was signed into law last year in an effort to bolster agencies' capabilities to defend themselves from cyber threats at home and abroad by replacing outdated and vulnerable systems. Could you please describe the threat that "legacy IT" specifically poses to Federal agencies' cyber infrastructure?

Answer. In general, older systems and software are less likely to receive security updates, and creating and obtaining updates or otherwise defending these systems is more costly. In the case of some long-lived devices, including industrial control systems, hardware can long outlive the software running on it. To mitigate the issue we can:

Identify and assign ownership of legacy systems so that we do not have "orphaned assets" that add to our risk exposure. Some very significant and successful attacks have occurred because a piece of legacy IT was not properly managed and remained unpatched. Regular scanning should be done from both inside and outside of networks to ensure that all assets are properly identified.

Once assets are identified, proper management will include dispositioning the risks that the legacy IT poses to the enterprise. In some cases isolation and access control will help to quarantine the risks of the legacy IT. Ensure that those devices and capabilities are not directly accessible from the internet. In cases where this is not possible, system hardening and monitoring are ways to disable unnecessary services (such as the SMB Protocol) that can pose risks.

Finally, investment in upgrading critical services and assets that are living on legacy IT must be made. There are some activities that are so significant and critical to organizations that they may need to eliminate the risk of legacy IT use.

*Question 3.* As one of a many industry standards for addressing coordinated disclosures, the CERT Coordination Center's guidance suggests that a third-party coordinator may relay or broker information between stakeholders for complicated coordinated vulnerability disclosure (CVD) cases. Could you please describe why this approach may be preferable and in what circumstances?

Answer. Coordinating organizations like the CERT/CC and DHS NCCIC can provide the following capabilities for complex CVD cases:

Understanding the problem—Some vulnerabilities are technically complicated and require a nuanced understanding in order to completely remediate them. Coordinators have access to technical analysts who can provide an objective assessment of the severity and impact of a vulnerability or help to refine the vendors' understanding of the scope of the problem. This can work in both directions: increasing the scope for vulnerabilities that appeared to be simple but turn out to be more complex, or reducing concern for vulnerabilities that initially appeared to be severe but pose less risk once they are better understood.

Coordinating creation of solutions—Researchers and vendors may not know whom to contact in regards to widespread vulnerabilities that affect more than just the products they are aware of. Coordinators maintain contacts across a wide swath of vendors. As neutral third parties, coordinators are also unconstrained by concerns about competitive advantage when vulnerabilities affect competing vendors. Furthermore, a message from a coordinator to a vendor security team can carry more weight than a random report received through the help desk, and sometimes this additional leverage is what is needed to induce vendors to act.

Amplifying public notifications—Public messaging by coordinators usually gets the attention of system deployers as well, which can help to amplify the vendors' attempts to reach their users.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO ART MANION

*Question 1.* I don't think these are new or complex ideas, but at hearing after hearing on this topic, experts put out the call for national coordination to advance these initiatives. According to Department of Homeland Security there were 290 cyber-attacks on our Nation's critical infrastructure in 2016.

I am particularly worried about our energy grid and the integrity of our voting infrastructure in the absence of a robust national strategy. What are the ingredients to an effective national strategy?

Answer. An effective national strategy must be multi-faceted and engage the threat, the current environment, the participants and the future. It must think about cyber both as an element alone and as a component to other activities enabling the United States to achieve its objectives leveraging and through cyberspace as appropriate. The strategy must include at least the following elements:

1- Establishing and gaining consensus internationally to a set of norms of behavior and a commitment to engagement to reduce the threat globally through increasing the capacity of the international community to address threats, investigate on-line malicious activity, and provide technology and policy support in nations with growing dependence on these technologies.

2- Effective identification of key intelligence and enhanced sharing of contextually aware and actionable threat information with associated growth of automation in the employment of this threat information throughout government and industry.

3- Sustaining the capacity of government entities to engage and address the emerging technological trends that affect the risks seen. Establishment and adoption of an effective risk management scheme for USG systems is a key element of the USG modernization effort leveraging the Cyber Security Framework and its appropriate customization to key missions and high value assets.

4- Institutionalization of coordinated government operations to support the private sector in responding to and prevention of incidents. Coordination across government agencies is vital to the success of response and prevention efforts.

5- Application of "levers of influence" including sanctions, confidence building measures, grants, etc. to the cyber dimension looking at levers that are both punitive and positive based on the behavior desired from our partner.

6- Growth of capacity at the state and local levels. U.S. citizens engage with their government most often at the state and local level, and key personally identifiable information (PII) is held in those systems. The workforce demands are felt acutely as well. A specific focus on increasing the capacity and capability of state and local government entities including technology modernization and training is required.

7- Growth of industry participation and adoption of security frameworks and processes and encouragement of industry driven approaches like the Security Accord and NIST CSF. Continued efforts to require corporations to report cyber as a material risk and manage it at the senior-most levels including boards of directors.

8- Sustained efforts in growing workforce through increasing the cyber acumen of leadership, awareness and understanding of the impact throughout the workforce, and key focus on critical skills vital to the operation and security of the environment. Encourage the distribution of these skilled professionals throughout the country and not only in technology meccas like Silicon Valley, Boston, Washington, D.C., etc.

9- Increased quality and efficacy of software that powers much of our world and whose importance will continue to grow with the adoption of AI into all elements of daily life.

10- Increased focus on research and development through the publication and engagement of key priorities across the research community. Growth of the U.S. population in graduate programs in key STEM areas aligned with the research priorities for the United States.

Specifically related to vulnerability disclosure, a national strategy should include stable support—both financial and through careful policy development—for fundamental security information and services that are not provided by the market. Considering the subset of cybersecurity I am familiar with, namely the vulnerability ecosystem, three examples are:

- Vulnerability identification, currently addressed in part by the Common Vulnerabilities and Exposures (CVE) project. Nearly every aspect of vulnerability management and response relies on a standard identification system.
- Supply chain transparency and inventory, so that we know what software we're using and trying to defend. This is an unsolved problem; however work has started in the medical device field and the Department of Commerce NTIA Software Component Transparency effort.[1]
- Coordinated Vulnerability Disclosure, so that every software and device vendor is able and expected to receive vulnerability reports in their products and services and to provide fixed software to users, for the lifetime of the software, service, or device. This work is currently performed by more mature vendors and security researchers and is partially supported by DHS.

*Question 2.* Where should responsibility for implementing a national strategy lie? Is there a legislative solution that would work here?

Answer. Such a national strategy should be overseen by the White House and executed through the National Security Council (NSC), Office of Science and Technology Policy (OSTP), and National Economic Council (NEC) delegated to appropriate Federal departments including Department of Homeland Security (DHS), Department of Justice (DOJ), Department of Defense (DOD), Director of National Intelligence (DNI), and National Institute of Standards and Technology (NIST) with active coordination through the EOP.

*Question 3.* Can you lay out what you think is necessary to ensure we have the cybersecurity workforce we need to be safe and secure?

Answer.

(1) Build a strong foundation through K–12 programs and STEM initiatives.
   a. Include games and game-based learning to reinforce concepts and increase engagement
   b. Create dedicated cybersecurity classes and curricula
   c. Hold cybersecurity summer camps
   d. Ensure cybersecurity professions are represented at career fairs

(2) Ensure community college and university programs implement curricula that the industry values.
   a. Include industry certifications such as CompTIA Security+, especially if that is a recommended certification for employers
   b. Expand scholarship for service programs
   c. Expand regional and national cyber competitions

(3) Fund Ph.D. scholarship programs in computer science.
   a. The 2018 Taulbee survey[1] shows that over 62 percent of all computer science Ph.D.s awarded in the United States went to non-resident aliens. [1] *https://cra.org/resources/taulbee-survey/*
   b. Expanding Scholarship for Service to include Ph.D.s would attract more U.S. citizens into the Ph.D. ranks and therefore expand the capacity of U.S. academic institutions.

*Question 4.* What else can the government and private sector do to fill this very pressing cybersecurity skills gap?

Answer. People must desire these jobs. Motivations often include compensation, location (including working from home), and mission. However, the barrier to entry must be lower. Potential cybersecurity professionals must see these careers and salaries as attainable. Having a strong foundational knowledge of terms, technologies, and career options will help.

The threat landscape is also constantly changing. Annual training and professional development must be planned for and required. Easy access to on-demand training where cybersecurity professionals can rapidly gain hands-on experience with new tools, systems, and best practices is essential.

*Question 5.* The North American Electricity Reliability Corporation, or NERC, has said that they are aware of these vulnerabilities, but they do not expect them to have operational impacts on the energy industry. The Energy Information Sharing and Analysis Center (ISAC) has confirmed that they sent a warning about the vulnerabilities to members of their information sharing portal.

---

[1] *https://www.ntia.doc.gov/SoftwareTransparency*

While it is not likely that the energy sector is the prime target of actors trying to exploit these vulnerabilities, it is true that on some level, all infrastructure sectors are at risk.

Given what we know about the hardware weaknesses presented by these two cyber vulnerabilities, what industries would you say are both:

(c) most vulnerable because of a lack of mitigation efforts? and

(d) a disruption in that industry would have the greatest effect on the Nation's health and safety?

Answer. We appreciate the question; however a complete answer is beyond our perspective. To answer in part, the Meltdown and Spectre vulnerabilities do not pose a serious risk to any sector, or, there are many other vulnerabilities that pose greater risks to different sectors.

Certain types of cloud services (those that provide virtualization and shared hosting) are most at risk to Meltdown and Spectre.

The health care sector seems to have difficulty assigning responsibility and resources for keeping critical systems up-to-date. In some cases, vendors retain control of updates; in others that work falls to users. Unclear boundaries and lack of cybersecurity resources in many providers lead to systems that are not updated to protect against known vulnerabilities, for example, those that contributed to incidents involving "Wanna Cry" and "Petya" malware that affected health care and shipping.

In our work at the SEI in partnership with DHS, we have performed over 600 cybersecurity assessments of the Nation's critical infrastructure. We have seen that across the board we need to shift our focus from security to resilience in order to survive disruptive events like cyber attacks. All of our industries should be balancing their defensive efforts with their mitigation efforts to ensure that not only are they trying to stop cyber incidents, but that they are also prepared to respond to and recover from them.

Our critical infrastructure is complex and significantly inter-related, so it is difficult to say which would have the greatest effect on the Nation's health and safety. We recommend that all 16 sectors approach cybersecurity via an enterprise-wide risk and resilience management process that identifies the most critical assets and applies operational resilience principles to ensure that those assets are able to operate before, during, and after cyber attack.

---

## RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO ART MANION

*Question 1.* Do you agree with some industry assessments that "pre-disclosure" notice to a non-regulatory agency such as NIST would spur other foreign governments to force "pre-disclosure"?

Answer. There is some evidence that foreign governments would follow suit, specifically that China has taken steps to prevent Chinese security researchers from reporting vulnerabilities outside of China.[1][2] Perhaps more importantly, it is not entirely clear what the tradeoffs would be in requiring such notification. On one hand, the U.S. Government could, in some cases, be better technically prepared in advance of a public vulnerability disclosure. On the other hand, significantly increasing the number of people and organizations who are aware of a non-public vulnerability shortens the private embargo period, reducing the benefit of knowing about the vulnerability before public disclosure. Furthermore, most mitigation activities that could be taken to defend against a not-yet-public vulnerability are essentially best practices that should be followed with or without knowledge of impending public disclosures. All the software we use and depend on should be assumed to have undiscovered and undisclosed vulnerabilities and defensive posture should be based on this assumption.

[1] *https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/*
[2] *https://medium.com/@thegrugq/china-and-vulnerability-research-dc617c993c4e*

*Question 2.* For academic institutions, do you have ethical guidelines for handling security vulnerabilities?

Answer. We recommend a general set of coordinated vulnerability disclosure principles to all stakeholders, including security researchers at academic institutions. These principles can be used to form ethical guidelines. The principles we follow and recommend are primarily captured in *The CERT Guide to Coordinated Vulnerability Disclosure* [2] and include:

---

[2] *https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330*

- Reduce harm and risk
- Presume benevolence
- Avoid surprise
- Incentivize desired behavior
- Improve the process

The *Guide* also cites ethical and professional codes of conduct from professional computer organizations and journalism.

*Question 3.* Academic researchers may be funded by grants from the USG, such as NSF or DARPA, or from private industry, or both. For academic institutions, do your funding sources impact your decisions about disclosure or deciding which technologies you evaluate for vulnerabilities?

Answer. Some vulnerability research or assessment engagements include non-disclosure agreements. This practice is more common for private industry contracts. We both follow and advocate that others follow coordinated vulnerability disclosure (CVD) practices. We rarely enter any agreement that constrains our ability to follow CVD practices and requiring such an agreement is a factor (for us) in determining whether or not to accept funding. We recommend that contracts, especially U.S. Government grants and other government funding vehicles, support CVD practices and protect the sharing and publication of legitimate security research.

Funding vehicles can, of course, specify areas of technology, in which case the decision is typically based on our ability to work in that area. In some cases, we seek or advocate for funding to study technologies that we believe are at greater risk or whose security is less well understood.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO ART MANION

*Question 1.* Small Business Cybersecurity: We have over 240,000 small businesses in Nevada and they're really worried about cybersecurity, it's something I hear about most often from them. With the inter-connectedness of our economy now a small business can be vulnerable even when they're not directly attacked because their information can be shared with a large company who is more likely to be a victim.

This leaves them very vulnerable and since they often don't have a lot of resources to combat cyber threats, they don't have a lot of options for increasing security.

Can you speak to how viable cyber security type programs, like bug bounties for example, or others, are for small and medium sized businesses?

Answer. As in many other technically complicated fields, we can't expect consumers and small business to have or be able to afford cybersecurity expertise. Similar to how the responsibility for credit card fraud is placed with those most able and motivated to prevent it—credit card companies—software and device vendors and providers should bear the brunt of cybersecurity responsibility for their customers. Examples of such responsibility include:

- Automatic deployment of security updates
- Secure default configurations for new software and devices
- Simple and effective security user interfaces
- Home routers and gateways that are managed by providers

To your question specifically, coordinated vulnerability disclosure programs or bug bounty programs are designed to elicit vulnerability reports from the broad security research community. With knowledge of these vulnerabilities, vendors and providers can deliver fixes to their customers, ideally before an adversary can take advantage.

*Question 2.* Cybersecurity Workforce Development: One reported estimate is that the gap in the needed pool of cyber professionals could be as large as 1.8 million by 2022.

What would you recommend we focus on to make progress on this challenging issue?

Answer. The data referenced is from the 2017 Global Information Security Workforce Study conducted by Frost & Sullivan for the Center for Cyber Safety and education, with the support of (ISC)$^2$, Booz Allen Hamilton, and Alta Associates.

Our first recommendation would be to cultivate fundamental knowledge and skills as early as possible through K–12 STEM programs. This must go beyond cyber etiquette and online safety programs for students. Teachers, counselors, and schools

need to implement curricula that expose our youth to cybersecurity tools, technologies, terms, and potential jobs. Without the proper cultivation early on, students are not prepared for college programs and professional careers. They may eventually learn of these opportunities, but without the proper foundation, entering the cybersecurity field may seem overwhelming.

To support these efforts, STEM funding and other educational initiatives should directly address cybersecurity needs. States should be funded to create, implement, and tool related programs.

Finally, the power of games and game-based learning should be harnessed. With the ubiquity of computers and mobile devices, most students have powerful resources at their fingertips. They are already leveraging these devices for individual and collaborative games. Similarly, they use social media for information sharing. Innovative programs should be implemented to leverage these resources to bring cyber training at multiple skill levels to these devices. In poorer areas where technology may not be as ubiquitous, additional funding should be allocated to schools and libraries to ensure they have the devices necessary to expose all students to these opportunities.

*Question 3.* Blockchain and AI: Nevada has been a leader in developing various blockchain startups. This kind of activity across the country has led us to include policy in the 2017 defense bill that included a provision to allow the public sector to invest in modernization projects that could include the use of blockchain technology. This development is coming as we see exciting developments in Artificial Intelligence.

Can you speak to the potential of how blockchain and AI technologies may be used to help improve security and efficiency within the public and private sectors?

Answer. Blockchain technology brings to bear a truly distributed computer. Every single computation for each program is run on every single machine connected to the network. This brings immense powers of resilience to blockchain-based programs; to stop a program from being run, a malicious actor would have to bring down every single machine on the network, which—when operating at scale—is often an infeasible task. Additionally, due to the way blockchain-based computer programs—"smart contracts"—are run, blockchain applications associate an identity with every single activity, and all these activities are stored in an unchangeable historical record. That said, blockchain is still mostly a research tool. There are many unsolved challenges, such as finding efficient, inexpensive, and secure techniques for getting all machines on the network to rapidly agree on the program output, as well as how to efficiently store such an enormous historical log while still maintaining all the benefits blockchain brings to the table.

Assuming these and other problems are solvable, blockchain has the potential to provide significant security enhancements. There has been significant discussion on using blockchain technology to replace the existing DNS, or Domain Name System, technology underlying the modern internet. This could provide significant resilience to our aging Internet infrastructure and make attacks such as the 2016 Dyn cyberattack impossible to carry out. The same concept scales down to individual websites and applications. The concept of the traditional DDoS attack—distributed denial of service—is almost impossible against blockchain-based applications. With the blockchain-based system being distributed by default, there is no single server or cluster for an adversary to attack. Killing a single bee does not destroy the swarm. There are also benefits from the unchangeable history of blockchain. Storing logs of computer activity on a blockchain ensures that all forensic evidence is maintained in pristine condition for all time, removing concerns that adversaries may attempt to cover their tracks by deleting traces of their activity.

Unfortunately, as J.K. Rowling eloquently stated, "The trouble is, the other side can do magic, too." Cybercriminals are already using blockchain-based DNS services to make criminal websites that are more difficult for authorities to take down. Malicious actors have taken advantage of the unchangeable nature of blockchain to put criminal and illegal information on blockchains, knowing that such information, once distributed, cannot be removed without taking down the entire chain. More work is still needed to address these and other issues, but there is significant potential.

Artificial intelligence is a very different topic. I direct the interested reader to the recent testimony of Carnegie Mellon University's Jaime Carbonell before the Committee on Science, Space, and Technology[1] for a good treatment of this issue and AI in general. Briefly, AI is likely to be as impactful as the onset of personal computers in the late 20th century, affecting virtually every sector, both government and industry. Applications of AI range from intelligent question-answering systems in modern search engines, to semi-intelligent chatbots in home devices, to voice and facial recognition, to self-driving vehicles and beyond. Specifically within the realm

of cybersecurity, the market is already seeing AI-based cybersecurity solutions that promise to automatically detect and stop malicious network activity, block malware of all types, detect insider threats, and even prevent humans from making mistakes that can inadvertently take down a network. However, adversaries are also deploying AI-based systems intended to defeat cybersecurity solutions. While continued investment in AI research is critical to the continued dominance of the United States in the field of AI, we are rounding a corner where AI-enabled applications are becoming a reality.

[1]: *https://docs.house.gov/meetings/SY/SY15/20180626/108474/HHRG-115-SY15-Wstate-CarbonellJ-20180626.PDF*

*Question 4.* Elections: What are your recommendations for what we can be doing better to strengthen our election security from potential cyber intrusion?

Answer. Many capable experts and groups have provided important recommendations and action plans for the short-term. Our primary recommendation is that for the "as is" infrastructure Congress should consider enabling the owners/administrators of election infrastructure to immediately and continuously apply the NIST cybersecurity framework to their parts of the infrastructure.

Making the election infrastructure efficiently resilient to capable cyber adversaries will require further research and development of effective, efficient, and easy-to-apply cybersecurity protections specifically for the Nation's diverse and disbursed election infrastructure. We recommend that Congress consider authorizing/funding NIST, NSF, and DHS to initiate competitions, experiments, and pilots to improve the cybersecurity and resilience of the interrelated election ecosystem.

Vendors of election systems should be held to the same standards and practices we expect of other IT vendors. For example, vendors should accept and process vulnerability reports and release advisories and updated software as needed. Vendors should use common and widely-accepted cryptographic and authentication mechanisms and not rely on custom, proprietary, and secret mechanisms that cannot be verified or trusted. Vendors should provide public review of custom cryptographic and authentication mechanisms. And vendors should provide out-of-band vote verification, for example, a paper receipt for the voter and a paper tally for election officials. The Federal Government should support state election boards in requiring acceptable security posture and behavior from election system vendors. State election officials must recognize the continual investment necessary to support a secure election infrastructure.

*Question 5.* How can we effectively engage the global cybersecurity community to respond effectively to this challenge?

Answer. Other countries that rely on robust elections often have resources and R&D communities that could join/collaborate with U.S. R&D investments to improve the technologies and practices for resilient elections. Technologies in use across the election infrastructure from voter registration systems to components used in voting devices are built with components from across the supply chain; a focus on securing the global supply chain leveraging the global cybersecurity community is an important step.

*Question 6.* IoT: In recent months, the FBI has warned of sophisticated Russian-linked hacking campaigns could be infecting hundreds of thousands of routers and home network devices around the world. As we move to the Internet of things, where nearly everything is connected, it will be even more important to deter data breaches.

What special considerations should be given as we move towards an economy powered by this technology?

Answer. A primary special consideration in protecting the Internet of Things is that the development tools and network infrastructure for IoT services must have adequate cybersecurity built in that is efficient (easy-to-use by developers and users).

- Congress should consider funding R&D that makes cybersecurity protections more effective and more efficient for the small but capable IoT devices and infrastructure. Ideally innovators will use tools and infrastructure that already have cybersecurity built in.
- Congress should consider asking agencies such as the Department of Commerce to periodically survey industry on the availability, use, effectiveness, and efficiency of the built-in cybersecurity in widely-available IoT tools and infrastructure.
- Congress should consider the importance of secure update mechanisms for IoT devices where vulnerabilities must be mitigated/patched to protect public welfare or critical infrastructures.

- Congress should consider authorizing/funding NIST to create competitions to improve the efficiency (especially of implementation and use) of cybersecurity protections in IoT devices and infrastructure.
- Congress should consider the establishment of a UL-like validation for the safety and security of devices, similar to the cybersecurity assurance program. Engaging a multi-disciplinary community and establishing testable and repeatable elements should be considered as a requirement. Additionally, IoT devices should publish a "software bill of materials" to increase transparency about the risks and vulnerabilities associated with these devices in the network.

Another "special consideration" is that abandoned IoT devices with network connectivity create the prospect of "cyber hazardous waste." That is, as low-cost devices are ignored or abandoned and the original manufacturers discontinue support or even go out of business, the IoT devices left behind will create opportunities for malicious actors to exploit those millions (billions?) of "waste" devices.

- Congress should consider asking industry trade associations how their industries plan to mitigate "cyber hazardous waste."
- Congress should consider asking the Office of Science and Technology Policy to lead an interagency working group to study the problem and recommend studies, policies, technologies, and research.

*Question 7.* Smart Cities: I have been active in the Senate developing bipartisan legislation on expanding the opportunities for local communities to tap Federal funding to build out smart communities. Nevada has been an exciting leader in these kind of emerging opportunities with electric and autonomous buses, traffic management systems, and other new transit options, and that's just in the transportation sector. The possibilities to have technological solutions help address various local concerns communities by communities, or regions by regions, is very exciting and a large undertaking.

How can cities be incentivized to consider cybersecurity when investing in smart technologies?

Answer. Many smart cities initiatives are funded via Federal grants, or Federal matching grants. Those grants should include a requirement to consider the appropriate parts of confidentiality, integrity, and availability and include a report back out from grant recipients on their issues, successes, and innovations in cybersecurity. The reports, with redactions for anything that would pose a security vulnerability, should be published and shared with both future awardees and other smart city granting entities.

*Question 8.* What policies do you believe are necessary to preserve privacy in smart cities?

Answer. Smart cities leverage technology to enhance the quality of life of residents, increase efficiency and effectiveness of providing city services and reduce the environmental impact of urban living. Key to the success of smart cities and to the support of the residents in such an environment is a focus on planning with a multi-disciplinary point of view. The concepts of privacy, and what it looks like in practice through all of the technology employed in a smart city, are not yet resolved. This discussion is vital and must continue as the technology evolves.

Policies that focus on enhancing citizen interactions through technology instead of only mediating them are important. For example, technology that focuses on increasing the convenience and cost effectiveness of city services through the use of mobile devices but is not transparent about the use of data available on the mobile platform only mediates the interaction between citizen and city and reduces the social interaction, which may have an impact on societal well-being. Understanding how to enhance this interaction without oversharing information must be assessed in a multi-disciplinary manner. Most importantly, forming collaborative, multi-disciplinary teams of experts who focus on the different ways the technology could impact the environment AND experiences is the best way to recognized and manage the privacy implications before deployment.

*Question 9.* Private Sector Investment: Within the private sector, is enough being invested in cybersecurity?

Answer. There are multiple estimates about rising cybersecurity budgets—some indicating that worldwide spending will reach over $1T USD cumulatively over 2017–2021. Despite this, the number and negative impact of cyber incidents are increasing each year.

It is difficult to believe that simply more money will solve this problem. A more effective approach is to optimize how money is being spent by shifting from a posture of security to one of resilience. We cannot expect to stop every adversary, but

we are able to identify, protect, and sustain our most critical assets as a way to ensure that organizations can continue to operate before, during, and after disruptions such as cyber attacks. Assets include people, processes, information, technology, facilities, and external relationships (*e.g.,* supply chain partners). This approach also serves to protect organizations from the negative impacts of other disruptions like natural disasters or employee errors/negligence.

A resilience approach is an enhancement to enterprise risk management that focuses on four core concepts:

- Establishing organization risk appetite and risk tolerance ranges
- Prioritizing cybersecurity investments on critical assets and services that keep organization within risk tolerance ranges
- Balancing investments across protection and sustainment activities
- Institutionalizing cybersecurity capabilities for organization maturity

Business objectives and risk appetite provide the guidelines for which assets are most important for success and for "how much" confidentiality, integrity, and availability are required on those assets. This establishes how much budget is required and where it should be allocated within the organization.

In our work at Carnegie Melon University's Software Engineering Institute (SEI) we have assessed and analyzed the resilience capabilities of over 600 private organizations across all 16 of the U.S. critical infrastructure sectors. We note that a significant percentage of cybersecurity funding is focused on protecting assets, but not nearly as much is spent on sustainment activities. This means that we are trying to protect and defend, but we often do not have sufficient capability to respond to and recover from cyber incidents. Balancing investments across protection and sustainment shifts organizations from security to survivability.

Institutionalization, or maturity, is key to endurance. Capabilities must persist over time to ensure high performance and consistent results over time. These practices can be found in maturity models like the CERT-Resilience Management Model (CERT–RMM), which cover both completeness and maturity of cybersecurity capabilities.

Focusing on resilience will enable organizations to more effectively use even limited resources to succeed despite the increasing number of cyber incidents.

*Question 10.* How can companies be incentivized to dedicate sufficient resources to this problem?

Answer. Due in part to rapid pace of developments in cybersecurity (by both offense and defense) and the lack of historical data, it's difficult to measure the effectiveness of cybersecurity defensive investments. This makes it very difficult determine if enough is being invested, and whether the right kinds of investments are being made.

In addition to the focus on resilience, we suggest investment in core, fundamental security controls like authentication, reducing complexity and exposure, and maintaining updated systems and software throughout the supply chain. We seek to develop and establish standard practices like coordinated vulnerability disclosure, that involve vendors accepting vulnerability reports from external parties and providing fixes for vulnerable software on a regular basis, for the lifetime of their products and services. We believe that including such recommendations in standards (including those published by ISO and NIST) is one way to incentivize companies to act responsibly. We have many sector- and industry-wide standards currently, for example, safety standards for the automotive industry. We should also seek to standardize safety and security of our information super highway on the internet. Establishing a minimal security baseline for operating devices on the Internet is one way to incentivize organizations to develop and operate an eco-system that dedicates sufficient resources to the problem.

Providing additional information such as supply chain transparency or a software bill of materials may also provide an incentive. Ideally, armed with standards requirements, inventories of software components (including known vulnerabilities), and possibly other security-related data, buyers can make better informed decisions, resulting in higher quality market incentives coming in to play.

---

## Response to Written Questions Submitted by Hon. Jon Tester to Art Manion

*Question 1.* Government Notification: Reports indicate that when Intel discovered the Spectre and Meltdown vulnerabilities, firms first notified Chinese technology

companies Lenovo and Alibaba. However, the U.S. Government only found out about these vulnerabilities after the security vulnerabilities became public.

Hiring top cybersecurity talent at DHS is challenging due to Federal hiring logjams—including security clearance delays, salaries, and private sector competition. A) What strategies should we implement to improve the Federal Government's cybersecurity workforce at agencies such as DHS?

Answer. There are two primary reasons people stay at a position. The first is financial motivation. DHS and Federal agencies simply need to pay as much as private organizations do. Even with OMB's Federal Cybersecurity Workforce Strategy of 2016, the proposed pay scale and incentives do not match industry average. This is especially true in the Washington, D.C., area. However, excellent methods for attraction and retention are outlined in the Strategy such as incentive bonuses, student loan repayment programs, relocation services, additional leave/vacation, flexible work options, and proposals for special rates of pay.

Programs like the National Science Foundation's Scholarship for Service are a good way to attract talent to Federal organizations. All scholarship recipients must work after graduation for a federal, state, local, or tribal government organization in a position related to cybersecurity for a period equal to the length of the scholarship. Perhaps the conditions could or should be modified to extend that length of service. A similar option would be to create more agency-specific programs that require longer commitments. Employer-paid education in exchange for minimum service time is a fairly common practice in larger organizations.

The second important motivation for employees is understanding and appreciation of their mission. This goes beyond loyalty to the flag and service to the country. They have to actually enjoy what they do, and like their co-workers. DHS and other Federal organizations are challenged with acquiring and retaining top talent. To improve this, they must build an environment that people want to work in. Employees need to respect (and care for) their co-workers, visualize their own internal career path, be rewarded for their successes, and operate in a stable environment. With frequent leadership turnover, organizational changes, and competing priorities, employee engagement is often challenged. DHS (and others) need to ensure a mission-first culture is engrained throughout the organization. This commitment to the team, along with the cause, will help improve retention.

*Question 2.* How do we keep pace with geo-strategic competitors such as Russia and China?

Answer. The U.S. Government must dramatically expand its cyber workforce to maintain (or achieve) parity with near-peer adversaries. Both of these countries recognize the asynchronous power that cyber operations afford and they both invest heavily in creating exceptional talent within their cyber forces. The United States spends the vast majority of NDAAs on kinetic weapon systems yet relatively little in expanding its cyber workforce. At least 80 percent of the DoD's Cyber Mission Forces *do not* have college degrees, and a relatively small percentage of those that do are in computer science. An easy and relatively inexpensive solution is to dramatically expand the CyberCorps Scholarship for Service program. That program produces only several hundred graduates annually. More funding could increase that by an order of magnitude.

*Question 3.* Human Element: Software patches are only as good as the person installing them. Most folks out there aren't nearly as tech savvy or as familiar with cyber-hygiene best practices as the folks on this panel. This whole system of patches and updates seems to break down when the average user is not aware of the problem, does not take the time to install updates or even know how to do so.

How would you recommend U.S. consumers, businesses and government entities—including Congress—better equip ourselves and the American people for the ever-changing cyber vulnerabilities we face?

Answer. At the turn of the 20th century, factory workers endured overcrowded buildings in dangerous conditions. These conditions frequently led to devastating fire outbreaks, often including dozens if not hundreds of fatalities. Over time, the population came to recognize that fires often had specific causes that could be avoided, and that when a fire broke out specific practices could be put in place to minimize both the loss of human life and property damage. We now know these as fire prevention systems and fire drills. Extensive fire prevention regulation exists and has been almost unbelievably effective; there are now fewer than 11 fire deaths per million people each year, an incredible achievement.

Cybersecurity education is in a state similar to that of fire education at the beginning of the previous century. Most Americans are not aware of the risks poor cybersecurity hygiene poses, let alone basic cybersecurity practices themselves. Individual companies occasionally attempt to gently nudge users to adopt modern prac-

tices such as two-factor authentication, secure password usage, and malware prevention, but few have the resources to invest significant efforts in this endeavor. People are becoming inured to cybersecurity breaches, particularly because they do not understand the impact of such a breach on their own safety and security. To them, cybersecurity is like rolling "bad-luck dice"; sometimes the numbers come up against you, and there's nothing you can do about it.

The solution to this problem is extensive education overhaul, starting in early grades. Elementary and secondary school computer science education curricula must be revamped to include cybersecurity best practices. The equivalent of cybersecurity fire drills should be included in cybersecurity regulations; practice against what to do when breaches are discovered, passwords compromised, or data is leaked. These are well-understood scenarios, and the only solution is education.

*Question 4.* What role should private industry play in making the average consumer aware of cyber vulnerabilities to their software or hardware, whether it on their CPU, smartphone, or car? What role do you believe should the U.S. Government should play?

Answer. The nature of the Internet is that everything is connected. An internet-enabled security camera in Omaha may be compromised by adversaries in Russia to attack a U.S. Government facility in Germany. To that extent, vulnerabilities in consumer hardware and software affect every participant of the open internet.

On a different note, vulnerabilities in software can take many forms. Often a vulnerability in a single piece of software can expose an entire machine, enabling exfiltration of documents and information unrelated to the source of the vulnerability. For example, previous bugs found in in Adobe Flash—a small program that extends the functionality of an Internet browser—may enable a malicious user to exfiltrate financial documents, personal information, and even passwords to other systems completely unrelated to Adobe Flash. The creators of software often extend the attack surface of a machine in ways that users may not appreciate.

Vulnerability analysts have long studied the different type of vulnerabilities and have devised ways of classifying their severity. It is imperative that manufacturers of computer software—whether that software lives in a PC, car, or refrigerator—inform users about vulnerabilities that put their personal information at risk. This involves a process known as Coordinated Vulnerability Disclosure, which has been well studied by researchers, including many within the Software Engineering Institute. To be sure, not all vulnerabilities pose the same risk; some may be much more benign. Consequently, not all vulnerabilities require the same timeline for disclosure. Still, the process is the same, and the need for informed consumers remains.

Unfortunately, the disclosure process is expensive, disruptive, unprofitable, and damaging to the company's reputation. To that extent, vulnerability disclosure would benefit from governmental regulation, requiring that companies follow responsible disclosure processes ensuring that consumers remain informed and our national infrastructure remains secure.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO DR. JOSÉ-MARIE GRIFFITHS

*Question 1.* I don't think these are new or complex ideas, but at hearing after hearing on this topic, experts put out the call for national coordination to advance these initiatives. According to Department of Homeland Security there were 290 cyber-attacks on our Nation's critical infrastructure in 2016.

I am particularly worried about our energy grid and the integrity of our voting infrastructure in the absence of a robust national strategy. What are the ingredients to an effective national strategy?

Answer. One resource that can be referenced as an effective strategy is U.S. *Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.* This executive order was put in place to, in part, improve the security of classified networks. The order charges the heads of agencies with classified networks with overseeing the security of those networks. This includes implementing insider threat detection programs as well as regular assessments of the security and compliance of the classified network. The order also charges the Secretary of Defense and the Director of the National Security Agency with developing the technical security controls and policies to safeguard classified information along with assessing the implementation of the technical controls and policies.

E.O. 13587 identified parties to spearhead the implementation and enforcement of proper security controls on classified networks. A similar strategy could be created regarding our Nation's critical infrastructure and voting infrastructure. This

new strategy should also charge an agency or group with developing the strong technical security requirements that should be in place to keep these critical networks secure. Periodic review of these controls is necessary as technologies and threats change. The strategy should also provide for periodic technical assessments on the critical networks to be sure effective security controls are properly implemented. Another component that should be in this strategy that is not found in E.O. 13587 is an incident response plan detailing the parties charged with responding to an incident on these networks.

*Question 2.* Where should responsibility for implementing a national strategy lie? Is there a legislative solution that would work here?

Answer. Our preference would be for legislation that would help establish a public/private partnership, akin to national standards boards in various industries. Regardless, legislation is a blunt instrument that may do more harm than good by defining new areas of civil and criminal liability that make companies less willing to reveal discovered vulnerabilities. The key to robust private participation is to give companies safe harbor for their reporting.

*Question 3.* Can you lay out what you think is necessary to ensure we have the cybersecurity workforce we need to be safe and secure? What else can the government and private sector do to fill this very pressing cybersecurity skills gap?

Answer. The breadth and depth of technology use in this country is now so large as to impact citizens of every age and across an astounding array of our daily activities. As such, it has moved from being the domain and concern of IT professionals to a concern to which we all must attend.

Cyber literacy is now a critically important skill for our citizenry, and as such it must be infused into every subject and skill addressed in our educational system, both formal and informal, from cradle to grave. However, without specific additional monies being made available to school systems and other lifelong educational resources, like public libraries, adding required technology hardware, software, and skilled staff is beyond the resources of many if not most communities.

Dakota State University and South Dakota have models that could be replicated across the country. These models address K–12 education, non-school-based activities to excite young people about cyber careers, and lifelong professional career change support and professional development.

The first strategy is focused on K–12 education and addresses both sides of the equation—the teachers and the learners. Starting with the teachers, every teaching major at DSU graduates with both expertise in the subject(s) they will teach—e.g., science or math—and they also have completed course work to earn certification in instructional/educational technology. Secondly, Dakota State is leveraging its resources and expertise to expand South Dakota's K–12 student cyber knowledge and skills. The university is working with school districts in its region to develop cyber security/hygiene and computer science curricula and enriched learning environments for South Dakota middle school students and teachers. Using a teach-the-teacher model, starting with 6th grade, DSU is working with 7 diverse school districts. Plans are underway to extend these efforts to all 4th—8th graders and their teachers in across South Dakota. There are three key components to the programs:

(1) addressing the developmental needs for cyber-learning for school-age children;
(2) addressing skill-oriented needs in computer science and cybersecurity *e.g.,* dual credit and accelerated dual credit for high school students, and developing a cohort of high school graduates ready to immediately move into college-level cybersecurity coursework or into non-traditional career pathways through apprenticeships and stackable credentials; and
(3) addressing the practice-oriented needs in cyber-learning for teachers of school-age children.

The second strategy is focused on engaging students outside of their school environments in fun and engaging activities exploring cyber skills and careers. Summer GenCyber camps (funded through the National Science Foundation) held at DSU and other universities across the U.S are excellent programs to recruit more students to work in the cyber fields. Multi-year and continuous funds to support GenCyber camps are essential for the success of the program. Extending the funding for a broader variety of camp formats would expose more youngsters to cyber opportunities. Potential new formats include online, weekend, and day camps. Further, opportunities to receive cybersecurity education must also be created for minority students and students in rural areas. DSU also has the CybHER Institute, which is specifically focused on materials and programs to encourage girls, pre-school through college-age, to enter and stay in cyber careers.

The third strategy is focused on ways to meet both the short-term and long-term needs for more cyber professionals through public/private partnerships and collaborations. Four organizations in South Dakota, including DSU, have created a new workforce development program designed to benefit students, area businesses and the state. The four core partners—(1) Dakota State University, (2) Southeast Technical Institute, (3) the Sioux Falls School District and (4) the South Dakota Department of Labor and Regulation (DLR) along with the office of the governor and several business partners, came together to create the South Dakota Partnership for Student Success, or SDPaSS. SDPaSS provides multiple stackable credentials to traditional and nontraditional learners, that is, for those initially seeking post-high school education, those interested in career change, and those seeking ongoing professional development. The programs includes internships in business/industry, registered apprenticeship connections and guidance through DLR, academic certificates in cybersecurity, network services, or software development, associate degrees in network and security administration (DSU and Southeast Tech), software development (DSU), software support (Southeast Tech), and DSU baccalaureate degrees in network and security administration or cyber operations.

SDPaSS addresses the educational needs and abilities of a broad array of students, provides multiple ways for students to acquire vocational relevance in the areas of cybersecurity, network services and software development, increases the number of eligible applicants for high-demand jobs, and coordinates the efforts and resources of community groups—educational institutions, corporations and businesses, and state/federal government—to create tangible workforce development and community economic development.

The final need—and the need is increasing—is for additional funding for needs-based scholarships. DSU is not alone in having more and more first-generation student applicants (*i.e.,* students who are the first in their family to pursue a college degree). Families who are still suffering from the combination of the most recent recession and the changing job environment recognize the need for their children to obtain post-high school education. However, these are also families who often have very little they can contribute to their child's education. We continue to struggle to find the financial resources to enable these qualified motivated students to achieve their degree. The maximum Pell Grant award in 2016–17 in the U.S. covered just 29 percent of average in-state public university tuition, fees, room, and board. This is in stark contrast to the Pell Grant award in 1997–98, when the award covered 87 percent of average in-state public university tuition, fees, room and board. This means that at a time when young adults more than ever need a college education to access a good job and states need a college-educated workforce to stay competitive and sustainable, Federal support has gone from covering almost all of the cost of a college education to covering less than a third. These days qualifying for the maximum Pell Grant award doesn't even get a student half way to covering the expense of their degree.

Dakota State continues to have one of the largest cohorts of students who receive the NSF CyberCorps Scholarship for Service. This program provides excellent merit-based scholarships that address two needs simultaneously: 1) the need for more scholarship support for students to achieve their cyber security degree and 2) the desperate need of federal, state, and tribal government organizations for more cyber security professionals. Students who receive the scholarship are required to work in a job in one of those settings for the same number of years they received the CyberCorps scholarship. These students are often the "brightest and the best" cyber security majors due to the requirements of the scholarship We consistently hear from government employers that they eagerly recruit these DSU graduates and find them highly qualified and a tremendous asset to their endeavors from the individual's first day on the job.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TOM UDALL TO DR. JOSÉ-MARIE GRIFFITHS

*Question 1.* In your testimony, you called for a "strong leader" to take control of planning and response for these types of events. What agency or organization do you have in mind for this role? Could it be a public-private partnership—or could one of our national labs, such as Sandia, play a role?

Answer. Many government agencies have incident response capabilities, red teams that perform offensive-based assessments of government network security, and blue teams that perform defensive-based assessments of government network security. Rather than standing up a new team to take charge in responding to events, consider adding to the responsibilities of an existing organization. National

Security Directive 42 is in place to ensure the security of national security systems, and establishes an interagency group for implementation of the policy. A similar interagency group could be utilized to bring the best from multiple agencies, national labs, and private and academic partners to ensure a swift, intelligent response to such cyber attacks.

*Question 2.* What precautions should the government and industry put in place if there were a clearinghouse at a Federal agency to ensure robust participation?

Answer. The difficulty of any clearinghouse is that it must be both widely accessible, to gain the largest participation and usefulness, and utterly secure, to ensure that it does not become an online tutorial by which hackers can learn new techniques.

*Question 2a.* How do we balance letting the public know about vulnerabilities with telling the world that such vulnerabilities exist?

Answer. Given that these two goals are in tension, there can be no perfect solution. But the present situation is untenable, and it already suffers from the inherent tensions of cyber-security. A widely supported public/private cooperative clearinghouse could at least minimize the risk by providing tiers of access in a context of robust security. The chance to relieve companies of some of the worries of civil liability, by defining best practices, can help ensure participation, as can the possibility of learning techniques for addressing discovered weaknesses.

*Question 3.* For academic institutions, do you have ethical guidelines for handling security vulnerabilities?

Answer. A university should follow the same ethical guidelines that all security researchers should follow. We believe in responsible disclosure given the vast options available to work directly with product vendors on disclosing the vulnerability and mitigating it in a timely fashion. Current approaches, such as bug bounties and companies' willingness to work directly with the security researcher community, provide ample opportunities for everyone to be satisfied with the process.

*Question 4.* Academic researchers may be funded by grants from the USG, such as NSF or DARPA, or from private industry, or both. For academic institutions, do your funding sources impact your decisions about disclosure or deciding which technologies you evaluate for vulnerabilities?

Answer. The funding source only impacts the process because the scope of the grant/contract will dictate which technologies are evaluated. For example, if DARPA funded research to evaluate wireless routers, any vulnerabilities found in those routers would be reported to DARPA as part of the funded work. DARPA may release those to the broader community, but the university's research team would be bound by the terms of the grant/contract. The agreement may allow for responsible public disclosure, but again, that would be negotiated as part of the funding instrument.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO DR. JOSÉ-MARIE GRIFFITHS

*Question 1.* Small Business Cybersecurity: We have over 240,000 small businesses in Nevada and they're really worried about cybersecurity, it's something I hear about most often from them. With the inter-connectedness of our economy now a small business can be vulnerable even when they're not directly attacked because their information can be shared with a large company who is more likely to be a victim.

This leaves them very vulnerable and since they often don't have a lot of resources to combat cyber threats, they don't have a lot of options for increasing security.

Can you speak to how viable cyber security type programs, like bug bounties for example, or others, are for small and medium sized businesses?

Answer. Small-and medium-sized businesses are wise to be concerned about cyber attacks. Around 85 percent of cyber attacks are now targeting small businesses; according to the Department of Homeland Security 74 percent of small and medium businesses reported attacks over 2016 and 2017. And the cost of an attack is high: 32 percent of businesses who reported attacks lost more than $25,000. According to Mandiant, an American cybersecurity company, 97 percent of organizations have already been breached at least once.

This means that the cyber systems of any business are being probed daily for security problems. Knowing about a problem is the first step to fixing it, and so wise businesses should include processes in their operations to identify potential

vulnerabilities. Programs like bug bounties are one strategy for identifying security problems before they are found by those intending damage.

However, starting, implementing and most importantly maintaining a bug-bounty program requires significant expertise, time, and attention. Legitimate researchers do not expect large payouts (though they do need to be compensated appropriately for their time and expertise) but they do expect their findings to be taken seriously and the company to respond promptly.

Companies can leverage the resources they do have available for cyber defense by aligning themselves with researchers and organizations that are involved in cyber security research and defense on an ongoing basis. At Dakota State University, we have an R&D organization, the Madison Cyber Labs (MadLabs) with research clusters and policy institutes in specific business areas, *e.g.,* finance, health care, Internet of Things devices, etc. These labs partner with government and business and industry organizations to research and develop mitigation and defense tools specific to the endeavors of that sector. These partnerships enable DSU faculty, researchers, and students to tackle contemporary real-world cyber security issues while ensuring that partner organizations stay informed and up-to-date on both potential threats and defenses.

*Question 2.* Cybersecurity Workforce Development: One reported estimate is that the gap in the needed pool of cyber professionals could be as large as 1.8 million by 2022.

What would you recommend we focus on to make progress on this challenging issue?

Answer. The breadth and depth of technology use in this country is now so large as to impact citizens of every age and across an astounding array of our daily activities. As such, it has moved from being the domain and concern of IT professionals to a concern to which we all must attend.

Cyber literacy is now a critically important skill for our citizenry, and as such it must be infused into every subject and skill addressed in our educational system, both formal and informal, from cradle to grave. However, without specific additional monies being made available to school systems and other lifelong educational resources, like public libraries, adding required technology hardware, software, and skilled staff is beyond the resources of many if not most communities.

Dakota State University and South Dakota have models that could be replicated across the country. These models address K–12 education, non-school-based activities to excite young people about cyber careers, and lifelong professional career change support and professional development.

The first strategy is focused on K–12 education and addresses both sides of the equation—the teachers and the learners. Starting with the teachers, every teaching major at DSU graduates with both expertise in the subject(s) they will teach—*e.g.,* science or math—and they also have completed course work to earn certification in instructional/educational technology. Secondly, Dakota State is leveraging its resources and expertise to expand South Dakota's K–12 student cyber knowledge and skills. The university is working with school districts in its region to develop cyber security/hygiene and computer science curricula and enriched learning environments for South Dakota middle school students and teachers. Using a teach-the-teacher model, starting with 6th grade, DSU is working with 7 diverse school districts. Plans are underway to extend these efforts to all 4th–8th graders and their teachers in across South Dakota. There are three key components to the programs:

(1) addressing the developmental needs for cyber-learning for school-age children;

(2) addressing skill-oriented needs in computer science and cybersecurity *e.g.,* dual credit and accelerated dual credit for high school students, and developing a cohort of high school graduates ready to immediately move into college-level cybersecurity coursework or into non-traditional career pathways through apprenticeships and stackable credentials; and

(3) addressing the practice-oriented needs in cyber-learning for teachers of school-age children.

The second strategy is focused on engaging students outside of their school environments in fun and engaging activities exploring cyber skills and careers. Summer GenCyber camps (funded through the National Science Foundation) held at DSU and other universities across the U.S are excellent programs to recruit more students to work in the cyber fields. Multi-year and continuous funds to support GenCyber camps are essential for the success of the program. Extending the funding for a broader variety of camp formats would expose more youngsters to cyber opportunities. Potential new formats include online, weekend, and day camps. Further, opportunities to receive cybersecurity education must also be created for minority

students and students in rural areas. DSU also has the CybHER Institute, which is specifically focused on materials and programs to encourage girls, pre-school through college-age, to enter and stay in cyber careers.

The third strategy is focused on ways to meet both the short-term and long-term needs for more cyber professionals through public/private partnerships and collaborations. Four organizations in South Dakota, including DSU, have created a new workforce development program designed to benefit students, area businesses and the state. The four core partners—(1) Dakota State University, (2) Southeast Technical Institute, (3) the Sioux Falls School District and (4) the South Dakota Department of Labor and Regulation (DLR) along with the office of the governor and several business partners, came together to create the South Dakota Partnership for Student Success, or SDPaSS. SDPaSS provides multiple stackable credentials to traditional and nontraditional learners, that is, for those initially seeking post-high school education, those interested in career change, and those seeking ongoing professional development. The programs includes internships in business/industry, registered apprenticeship connections and guidance through DLR, academic certificates in cybersecurity, network services, or software development, associate degrees in network and security administration (DSU and Southeast Tech), software development (DSU), software support (Southeast Tech), and DSU baccalaureate degrees in network and security administration or cyber operations.

SDPaSS addresses the educational needs and abilities of a broad array of students, provides multiple ways for students to acquire vocational relevance in the areas of cybersecurity, network services and software development, increases the number of eligible applicants for high-demand jobs, and coordinates the efforts and resources of community groups—educational institutions, corporations and businesses, and state/federal government—to create tangible workforce development and community economic development.

The final need—and the need is increasing—is for additional funding for needs-based scholarships. DSU is not alone in having more and more first-generation student applicants (*i.e.,* students who are the first in their family to pursue a college degree). Families who are still suffering from the combination of the most recent recession and the changing job environment recognize the need for their children to obtain post-high school education. However, these are also families who often have very little they can contribute to their child's education. We continue to struggle to find the financial resources to enable these qualified motivated students to achieve their degree. The maximum Pell Grant award in 2016–17 in the U.S. covered just 29 percent of average in-state public university tuition, fees, room, and board. This is in stark contrast to the Pell Grant award in 1997–98, when the award covered 87 percent of average in-state public university tuition, fees, room and board. This means that at a time when young adults more than ever need a college education to access a good job and states need a college-educated workforce to stay competitive and sustainable, Federal support has gone from covering almost all of the cost of a college education to covering less than a third. These days qualifying for the maximum Pell Grant award doesn't even get a student half way to covering the expense of their degree.

Dakota State continues to have one of the largest cohorts of students who receive the NSF CyberCorps Scholarship for Service. This program provides excellent merit-based scholarships that address two needs simultaneously: 1) the need for more scholarship support for students to achieve their cyber security degree and 2) the desperate need of federal, state, and tribal government organizations for more cyber security professionals. Students who receive the scholarship are required to work in a job in one of those settings for the same number of years they received the CyberCorps scholarship. These students are often the "brightest and the best" cyber security majors due to the requirements of the scholarship We consistently hear from government employers that they eagerly recruit these DSU graduates and find them highly qualified and a tremendous asset to their endeavors from the individual's first day on the job.

*Question 3.* Blockchain and AI: Nevada has been a leader in developing various blockchain startups. This kind of activity across the country has led us to include policy in the 2017 defense bill that included a provision to allow the public sector to invest in modernization projects that could include the use of blockchain technology. This development is coming as we see exciting developments in Artificial Intelligence.

Can you speak to the potential of how blockchain and AI technologies may be used to help improve security and efficiency within the public and private sectors?

Answer. Blockchain is, in essence, a technique for keeping track of encrypted records in real time. That makes it perfect for such things as electronic currencies, where, for example, it is important to know whether the particular piece of crypto-

currency has been spent elsewhere already. Therefore, blockchain will be an appropriate strategy to use in certain situations, but it will not solve wide cyber security threats.

Single use applications for blockchain are the easiest and most likely to be most widely implemented, *e.g.,* adding bitcoin as a payment mechanism. Adopting virtual currency will force many aspects of a business, such as finance, accounting and sales, to build blockchain capabilities. Another low-risk approach will be to use blockchain internally as a database for managing assets, recording transactions.

Blockchain technology is also opening the door for new business initiatives. For example, financial services companies are finding private blockchain networks they have set up significantly reduce transaction costs. Government support and funding of this development will encourage open and ethical attributes in these new systems, as well as leveraging the development work to the benefit of a large number of industries and businesses, not just multi-national corporations with extensive resources. In addition, as these new services are developed, oversight and regulatory constraints will have to be developed as well, which may well require legislative intervention to avoid the errors of the past as well as to protect against societal, government, and business vulnerabilities in the future.

Artificial intelligence (AI) is of greater use—but also presents a greater threat. AI can be used to help develop new security techniques, even while it can be used to seek ways to break those security techniques. The development of AI is proceeding rapidly across the world, in some cases driven by those seeking to do good and in others by those seeking to use it as another cyber warrior tool. While the U.S. has been energetic in its military exploration of AI potentials, governmental agencies should also be looking at ways to encourage AI advancement in a wider range of U.S. endeavors. An understanding and knowledge of AI is already one of the required tools in the toolbox of cyber security analysts, and will be even more so over the next 5 to 10 years.

*Question 4.* Elections: What are your recommendations for what we can be doing better to strengthen our election security from potential cyber intrusion?

Answer. This question must be addressed on at least two fronts.

First, the integrity of the actual vote-counting process must be assured. The data thus far do not suggest this has been a problem to date, but it is likely only a matter of time before cyber-sophisticated attackers, especially nation-states or crime-oriented entities with considerable resources to allocate to the challenge, will figure out how to invade and control these systems. While the temptation of technology is always to drop older systems in favor of new efficiencies and systems, this is a situation where it may be wise to continue the processes that ensure that every vote is backed by a paper ballot. All safe technology systems require a backup process, and that backup is not required to also be technology based.

Secondly, everything around the voting process must be hardened. As we saw in 2016, an attacker does not need to actually alter votes in order to have a significant, harmful effect on the process. State election boards, county election commissions, and voter registration databases are all very soft targets. The Federal Government would be wise to invest heavily in securing all of this supporting infrastructure and require states to demonstrate that their voting systems are robust and consistently separated from partisan manipulation.

*Question 5.* How can we effectively engage the global cybersecurity community to respond effectively to this challenge?

Answer. More and more multinational companies operate across numerous governments, each with their own ethics and commitments to their technology systems. Recently we have seen multiple examples where corporations have had to change products or service delivery models internationally to accommodate the requirements of one country or region. We must find ways to encourage collaboration, cooperation and communication among U.S.-based companies, the Federal Government, and cyber security university and research activities. This must include incentives for all to participate. As I stated in my testimony, we must seek to actualize "the potential to develop a nationwide distributed and trusted force (of faculty and students) that could be mobilized on short notice to address initial vulnerabilities and test solutions."

In recent months, the FBI has warned of sophisticated Russian-linked hacking campaigns could be infecting hundreds of thousands of routers and home network devices around the world. As we move to the Internet of things, where nearly everything is connected, it will be even more important to deter data breaches.

*Question 6.* What special considerations should be given as we move towards an economy powered by this technology?

Answer. The adoption of IoT has raised many cybersecurity threats, including challenges in architecture, system, standardization, privacy, etc. While there are no perfect solutions to resolve these challenges, there are also good security principles (*e.g.,* layering, isolation, limiting) to follow to remediate security risks in IoT. While the solutions for securing IoT are still in development and to be matured, there are also steps we can take to help us transition to a more secure interconnected world. In terms of standardization, we need to develop and implement novel ways to conduct security testing on products and audit source code. We need to ensure cybersecurity becomes part of standards for products before they are released to the general public. In terms of culture, there is more work necessary to educate the public in security awareness. Security must become a key factor just like performance and price when a customer purchases an IoT device. Many have suggested that just as food products in the U.S. must carry a label identifying their country of origin and ingredients, or home appliances for sale display the energy efficiency ratings, the development of a federally-based and defined security certificate label system on IoT products would have tremendous impact on educating the general population such that they can make informed technology choices and understand the risks of purchasing and using a non-certified or security-verified IoT product or service.

*Question 7.* Smart Cities: I have been active in the Senate developing bipartisan legislation on expanding the opportunities for local communities to tap Federal funding to build out smart communities. Nevada has been an exciting leader in these kind of emerging opportunities with electric and autonomous buses, traffic management systems, and other new transit options, and that's just in the transportation sector. The possibilities to have technological solutions help address various local concerns communities by communities, or regions by regions, is very exciting and a large undertaking.

How can cities be incentivized to consider cybersecurity when investing in smart technologies?

Answer. The adoption of new technologies such as smart cities and IoT comes with security risks. These security risks need to be constantly assessed. There are known cyber attack vulnerabilities in existing smart technologies, and there will be emerging vulnerabilities and new cyber attacks over time. Financial assistance for risk assessment and security auditing, as well as clearly defined and publicized standards for these technologies can provide incentives for cities to consider cybersecurity when investing in them. As mentioned above, partnerships with cybersecurity research centers such as DSU's Madison Cyber Labs (MadLabs) can provide essential resources for building in security robustness at the point of purchase and implementation of systems.

*Question 8.* What policies do you believe are necessary to preserve privacy in smart cities?

Answer. Policies regarding user-generated data are essential to preserve user privacy. IoT and smart cities applications generate huge amounts of data. Data needing protection are generated from mobile devices, IoT, and cyber physical systems as users access an ever-larger universe of devices and applications. Protecting user-generated data is essential to privacy since the data often includes user personal information and user location/movement, frequently without the user's knowledge.

Clear standards and policies must be established dealing with data ownership (who owns the data?), data use (who can use the data and how?) and user rights (*e.g.,* can a user ask a service provider to delete all the data generated from his/her mobile devices?). Systems that were previously effective in protecting individual privacy by anonymizing data have now been disabled as new methods have been discovered or developed for re-identification of individual users (using principles of reverse engineering). This requires that policies must be defined concerning the use of all data, supposedly anonymized or not.

*Question 9.* Private Sector Investment: Within the private sector, is enough being invested in cybersecurity?

Answer. It seems that security concerns fall behind added functionality (the proficiencies referred to in the written testimony) and safety (such as in vehicles, non-exploding batteries, etc). Thus, it does not appear that there is sufficient investment in security by device designers and manufacturers. This is especially challenging in that so many Internet of Things (IoT) devices are increasingly manufactured and even designed outside of the U.S., where standards and quality requirements may not be the focus of the process. Until the U.S. has clearly defined standards and requirements related to IT projects (*e.g.,* in the direction that the European Union has developed) the problems of poorly secured IoT will continue to proliferate.

*Question 10.* How can companies be incentivized to dedicate sufficient resources to this problem?

Answer. The development of a public-private partnership along the lines of the national standards bodies or the Consumer Products Safety Commission may well be warranted. There is a need for review and prompt, easily accessible communication of reports of failures; support for testing cyber products for reasonable security features and dissemination of results; and perhaps the development and communication of product security ratings.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JON TESTER TO DR. JOSÉ-MARIE GRIFFITHS

*Question 1.* Government Notification: Reports indicate that when Intel discovered the Spectre and Meltdown vulnerabilities, firms first notified Chinese technology companies Lenovo and Alibaba. However, the U.S. Government only found out about these vulnerabilities after the security vulnerabilities became public.

Hiring top cybersecurity talent at DHS is challenging due to Federal hiring logjams—including security clearance delays, salaries, and private sector competition. A) What strategies should we implement to improve the Federal Government's cybersecurity workforce at agencies such as DHS?

Answer. Cyber security professionals most often leave the Federal Government for private industry because of pay differentials. At present, private salaries for cyber security professionals are often as much as five times that of comparable government positions. A significant challenge is that, just as in military-related private companies, a cyber security contractor can charge the U.S. Government far more for a service than the agency has available to pay its own staff. This ensures a constantly-revolving door for government cyber professionals to move into—or start their own company—to do exactly the same work they were doing for the government for a great deal more money.

There are a number of ways the government could address this problem. The Federal Government needs to fundamentally change its relationship to cyber security contractors. Raising wages close to market value would be a first step. However, refusing to purchase commercial off-the-shelf solutions at exorbitant cost must also be considered. The Scholarship for Service model has been highly effective in making it possible for more students to achieve cyber degrees while also ensuring at least some years of government service by its recipients. However, there are far more qualified students than scholarships available.

Another impediment that must be fixed in order to attract talent is the complex, slow, and invasive process of obtaining a security clearance. We fully understand the Federal Government's desire to fully vet every employee, but this process turns away good people in droves.

To work for NSA or CIA, for instance, requires (as communicated to us by graduates):

1. Filling out a 127-page document, disclosing one's deepest personal information, which the submitter must trust will always be kept safe (see: OPM breach);
2. Waiting for an indeterminate amount of time (up to 3 years in some cases) with no communication about the status of the application or ability to find out where in the process an applicant is presently, and how long it will be before the applicant will know whether they have achieved the clearance necessary to be considered for the job;
3. Participating in a battery of intense psychological evaluations with polygraph machine monitoring;
4. Finally accepting a job to work in a highly supervised and often not very pleasant work environment (*e.g.,* a windowless cement building filled with cubicles).
5. Often waiting for a number of years for a decision/opportunity;
6. With compensation and a benefit package that is far below what industry offers, generally about $75k/year.

Alternatively, as an example, to work for Google requires:

1. Submitting an application, a few pages in length, describing talents and work history;
2. Within a few days or at most a couple of weeks being informed about next steps;
3. Completing a phone interview, and then being flown to a Google location for an on-site interview;
4. Accepting a job to work in a spacious, comfortable office with free gourmet meals cooked on site daily;

5. This process might take a month or two, and compensation will be about $150k/year.

Admittedly the above comparison does not fully represent either employer (job security, some benefits, work hours, and sense of "purpose" are all attractive at the agencies for instance). However, increasingly this comparison is reflective of the general perception of cyber security professionals of the job application process and end result. It is no surprise that many talented individuals choose to work as a contractor for the government, or in private industry, over working directly in our government agencies.

We are not suggesting that Federal agencies should follow all corporate hiring practices, but it is the case that meeting the requirements (*e.g.,* for clearances) and the process could be significantly more timely and efficient. Reducing paperwork would be a good first step. For example, it is not clear that a 127-page SF–86 is necessary for an entry-level hire. The lack of communication from the agencies to candidates, leaving candidates "hanging" without information as to their status or timeline, causes many applicants to pursue other positions. There are few students who graduate from university who can afford to, or are willing to, remain unemployed for the length of time (1 to 3 years) that it generally takes Federal agencies to complete a hiring. It may well be that agencies need to allocate more resources to the hiring process or find ways to expedite the hiring of high-demand individuals like cyber security professionals over other positions for which there is a large population of potential candidates.

Many DSU cyber security students are eager to serve their country with their skills but become discouraged and pursue non-government careers due to the impediments described above. Perhaps a centralized streamlined process could be initiated, at least for the short term, for cyber security positions across the Federal Government. Additionally, an earlier pre-screening process for cyber security students in their junior or senior year could help increase the available pool of cleared or partially cleared candidates. This is one area where the U.S. is falling farther and farther behind the rest of the world—we increasingly have a far smaller percentage of cyber professionals working in our government than do other major international powers.

*Question 2.* How do we keep pace with geo-strategic competitors such as Russia and China?

Answer. There are a number of suggested strategies that would assist the U.S. remaining competitive in cyber security. The DoD and Intelligence Community need increased funding to develop and carry out the cyber mission. U.S. Cyber Command would benefit from being a true stand-alone command with its own skilled workforce and defined mission. It would also benefit clear defined national policy on the who/what/when/why/where that U.S. Cyber Command can execute their mission. Because their mission includes both offensive and destructive capabilities it must have different emphases and strategies than much of the rest of the intelligence community. The existing lack of funding, authority, and mission clarity has allowed other superpowers to gain the upper hand over the United States in cyber warfare, an ever more pervasive and threatening dimension of national security.

*Question 3.* Human Element: Software patches are only as good as the person installing them. Most folks aren't nearly as tech savvy or as familiar with cyber-hygiene best practices as the folks on this panel. This whole system of patches and updates seems to break down when the average user is not aware of the problem, does not take the time to install updates or even know how to do so.

How would you recommend U.S. consumers, businesses and government entities—including Congress—better equip ourselves and the American people for the ever-changing cyber vulnerabilities we face?

Answer. There are two significant components to answer these questions: education and simplicity. A basic "cyber hygiene for all" national educational program would be a first step. This could be tailored to multiple audiences based on age, experience, and context. Such a campaign, similar to many of our public health communications programs, warning of cyber vulnerabilities, could be coupled with more responsible "cyber health warnings" related to specific devices and infrastructures.

We must educate all users of technology—which now means citizens of every age—of the importance of good security practices (backing up information, installing upgrades and security patches in a timely manner, and safeguarding passwords) along with the consequences of poor security practices, and how to remediate them. The vast number of consumers have little understanding of the required maintenance of their technology tools, in contrast to their understandings, for example, of the maintenance required to keep their vehicles running. It is not enough to enhance technology education in our school systems, which is critical, we must also

provide public education through communications channels accessed by the non-school age population.

The other major component is for hardware and software companies to be incentivized to build in simpler user interfaces into their systems and applications. It has often been easy and cost-effective for technology companies to push security responsibilities onto largely untrained (and often uninterested) users. Manufacturers and software developers must make security upgrades and mitigations easier for users to install, and must take greater responsibility for building in security protections into systems that will not require frequent and complex procedures to maintain.

*Question 4.* What role should private industry play in making the average consumer aware of cyber vulnerabilities to their software or hardware, whether it on their CPU, smartphone, or car? What role do you believe should the U.S. Government should play?

Answer. In addition to the suggestions in the response to the previous question, the development of a public-private partnership along the lines of the national standards bodies or the Consumer Products Safety Commission may well be warranted. There is a need for review and prompt, easily accessible communication of reports of failures; support for testing cyber products for reasonable security features and dissemination of results; and perhaps the development and communication of product security ratings.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO SRI SRIDHARAN

*Question 1.* I don't think these are new or complex ideas, but at hearing after hearing on this topic, experts put out the call for national coordination to advance these initiatives. According to Department of Homeland Security there were 290 cyber-attacks on our Nation's critical infrastructure in 2016.

I am particularly worried about our energy grid and the integrity of our voting infrastructure in the absence of a robust national strategy. What are the ingredients to an effective national strategy?

Answer. A successful national strategy requires three ingredients: cooperation, communication, and collaboration. Government organizations and private industry must cooperate, communicate, and collaborate *within* and *among* one another to create an emergency response system that follows a clear hierarchy and communication strategy. All stakeholders must be identified and prioritized. We need a clear communication plan that addresses the role of each area and order and method of notification.

As we were preparing our response, the Department of Homeland Security announced the launch of the National Risk Management Center (*https://www.cnbc.com/2018/07/31/dhs-head-cat-5-cyber-hurricane-is-forecast-heres-what-were-doing-a.html*) to address these very issues. Upon initial review, it seems an appropriate and much needed solution, however, coordination among stakeholders will be key. More on this below.

*Question 2.* Where should responsibility for implementing a national strategy lie? Is there a legislative solution that would work here?

Answer. As stated above, the Department of Homeland Security has just announced the launch of the National Risk Management Center. The Florida Center for Cybersecurity agrees that DHS is the appropriate organization to house this responsibility, given their overall mission to protect critical infrastructure. While this is an admirable step, legislation may be required to ensure the necessary cooperation among the various stakeholders in government and industry. First, we need to consider creating duty to report legislation that mandates the circumstances in which private industry and researchers must disclose new findings to the Federal Government and identifies the appropriate reporting mechanism and channel. Second, legislation may be required to outline the chain of command and communication model enacted upon discovery of an incident.

*Question 3.* Can you lay out what you think is necessary to ensure we have the cybersecurity workforce we need to be safe and secure?

Answer. We need to create more awareness of the opportunities in the industry, starting at the earliest ages of schooling, and create more points of access to the industry. The jobs are there, the salary is there, but the infrastructure is not in place to easily move people into those positions. To an industry outsider, the pathway to success is unclear. There are several short-term approaches that I feel

should be leveraged to quickly move people into the field, but a long-term national strategy must be put in place as well.

We at the Florida Center for Cybersecurity have had great success with veterans' training programs, and I believe these programs can provide significant relief for the Federal Government's hiring challenges. Veterans (and their families) are ideal candidates for cybersecurity positions, particularly those in government agencies, for several reasons. First, military training teaches strategic thinking, analytical problem-solving, adaptability, and the value of collaboration. Second, they have been pre-screened and many have held high-level security clearances. Third, they have a demonstrated commitment to country and service that supplants, which often remains with them in new career paths. Lastly, the jobs are portable, have no physical requirement, and can be performed remotely, making cybersecurity an optimal career path for disabled veterans as well as spouses and families of veterans, who may need to move frequently.

Furthermore, many entry-level cybersecurity jobs do not require a four-year degree. Short-term intensive training programs that take only weeks or months provide adequate training for many entry-level technical positions in the field, such as analysts and penetration testers, that provide the first line of defense. These programs are relatively inexpensive to run, portable, and offer veterans a post-service career that is both financially and personally rewarding.

Likewise, the Nation's robust community college system can be leveraged to assist with career changers, such as skilled or semi-skilled workers in regions where traditional economic drivers are waning, as well as underutilized populations such as women and minorities, those who are underemployed, or those simply looking to make a change to a growing and lucrative industry.

Once employed in the industry, these workers can pursue the higher degrees needed for management and leadership positions. Traditional higher education institutions are rising to the challenge as well by adding certificate and degree programs. The implementation of traditional four-year bachelor's degree programs in cybersecurity is an important step to building awareness of the field and providing a smooth path to entry for those pursuing four-year degrees. Likewise, master's degree programs provide education to fill another critical gap in the cybersecurity workforce: mid-career managers. However, these programs are in their infancy and not widely available. The Florida Center for Cybersecurity has worked closely with the State University System of Florida to introduce dozens of cybersecurity-specific programs across the system; this model needs to be adopted by other states and additional funding for students pursuing these degrees added to incentivize colleges and universities to make more cybersecurity programs available.

Part of the problem also lies in the lack of awareness of cybersecurity as a career. It is a relatively new field, and the need has grown so quickly that young people are simply unaware of the options and benefits offered by a cybersecurity career. Integrating better awareness of cybersecurity through the public education system, beginning at the earliest stages of education, will not only dramatically improve the Nation's levels of personal security, but also improve awareness of the field, allowing young people to begin planning and pursuing careers as cybersecurity professionals at a much earlier age. Teachers and guidance counselors in K–12 need to be engaged and trained to incorporate cybersecurity into lesson plans and career events throughout a child's academic journey.

In addition to leveraging the public education system, future cybersecurity professionals can be reached and inspired through gamification. Gamification, the process of applying a competitive scoring system to a training event, is rapidly gaining in popularity within the cybersecurity community not only for professional development, but also for general awareness training. Early programs are showing that employees retain and apply cybersecurity awareness training much better when taught using gamification. Leveraging the average high schooler's love of online gaming is an easy way to introduce them to the cybersecurity and to encourage them to start building their skills from a young age. More government-led, gamified cybersecurity training programs targeting youth could help inspire new practitioners and help the government be the first to identify burgeoning talent in the field.

In summary, funding for widespread availability of short-term, intensive training programs; youth camps and competitions; bachelor's and master's degree programs; and outreach programming are needed to boost awareness and interest in the field and create pathways to success.

The Department of Homeland Security advocates these strategies and discusses them in greater detail in their document, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future, which can be found online at *https://www.dhs.gov/publication/supporting-growth-and-sustainment-nations-cyber*

*security-workforce.* We agree with the strategies and recommendations made in that report, and endeavor to support those recommendations across the state of Florida.

*Question 4.* What else can the government and private sector do to fill this very pressing cybersecurity skills gap?

Answer. As mentioned earlier, a long-term national strategy needs to be implemented. Part of the problem is the lack of awareness of cybersecurity as a career. It is a relatively new field and the need has grown so quickly that young people are simply unaware of the options and benefits offered by a cybersecurity career. Integrating better awareness of cybersecurity through the public education system, beginning at the earliest stages of education, will not only dramatically improve the Nation's levels of individual security, but also improve awareness of the field, allowing young people to begin planning and pursuing careers as cybersecurity professionals at a much earlier age. Teachers and guidance counselors in K–12 need to be engaged and trained to incorporate cybersecurity into lesson plans and career events throughout a child's academic journey.

Funding for widespread availability youth camps and competitions and outreach programming are needed to boost awareness and interest in the field. K–12 education programs need to be encouraged to include cybersecurity education and career awareness, and college-level programs should include basic cybersecurity awareness components as well since all organizations require a cyber-aware workforce.

---

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO TO SRI SRIDHARAN

*Question 1.* Small Business Cybersecurity: We have over 240,000 small businesses in Nevada and they're really worried about cybersecurity, it's something I hear about most often from them. With the inter-connectedness of our economy now a small business can be vulnerable even when they're not directly attacked because their information can be shared with a large company who is more likely to be a victim.

This leaves them very vulnerable and since they often don't have a lot of resources to combat cyber threats, they don't have a lot of options for increasing security.

Can you speak to how viable cyber security type programs, like bug bounties for example, or others, are for small and medium sized businesses?

Answer. While bug bounties have proven to be a valuable and cost-effective method of discovering system vulnerabilities, they only address one side of the problem and could present unforeseen problems for an SMB. The benefits of bug bounties are twofold. First, the business can set reward amounts based on their financial capabilities. Second, the organization receives a customized penetration test unique to their systems, something that most SMBs cannot afford. Bug bounties, however, are intended to test an organization's cybersecurity; they do not rectify vulnerability issues nor provide security. This can pose a potential problem for a small business that can only afford minimal security. The less security in place, the more likely bug hunters are to find vulnerabilities and demand payouts. Small-to-medium businesses that want to take advantage of the bug bounty model should be sure to outline payout restrictions and limitations to ensure their payout liability stays within the approved budget.

An alternative but similar grassroots approach for small businesses with limited resources is to solicit assistance from local colleges and universities. Internships are a crucial part of higher education, and connecting SMBs to cybersecurity degree programs can provide little-to-no-cost cybersecurity services to the SMB and valuable hands-on experience to students under the supervision of faculty professionals. This is a win-win for businesses and colleges. Students can review the business's needs, make recommendations, and implement security measures. Once the business has reached a level of security maturity, then the bug bounty model can be employed to test the system.

Additionally, there are several low-to-no-cost programs to assist SMBs with cybersecurity needs. The Florida Center for Cybersecurity has partnered with several state and national organizations (National Cyber Security Alliance, NICE, U.S. Army, Raymond James Financial, and others) to produce a free resource specifically to address this need in the SMB community. *The Cyber Defense for SMBs Handbook* will be available nationally through digital distribution this fall and will offer a primer on cybersecurity considerations for SMBs. It will review current threats and outline options to helps SMBs prioritize cybersecurity spending and needs. The handbook will be accompanied by statewide workshops as well as a website that will

offer more advice and links to free resources available to SMBs. Many private companies and nonprofit organizations recognize the need to assist SMBs in this challenge, and our goal is to make it easy for SMB owners, managers, and IT specialists to access these resources.

*Question 2.* Cybersecurity Workforce Development: One reported estimate is that the gap in the needed pool of cyber professionals could be as large as 1.8 million by 2022.

What would you recommend we focus on to make progress on this challenging issue?

Answer. We at the Florida Center for Cybersecurity have had great success with veterans' training programs, and I believe these programs can provide significant relief for the Federal Government's hiring challenges. Veterans (and their families) are ideal candidates for cybersecurity positions, particularly those in government agencies, for several reasons. First, military training teaches strategic thinking, analytical problem-solving, adaptability, and the value of collaboration. Second, they have been pre-screened and many have held high-level security clearances. Third, they have a demonstrated commitment to country and service that supplants, which often remains with them in new career paths. Lastly, the jobs are portable, have no physical requirement, and can be performed remotely, making cybersecurity an optimal career path for disabled veterans as well as spouses and families of veterans, who may need to move frequently.

Furthermore, many entry-level cybersecurity jobs do not require a four-year degree. Short-term intensive training programs that take only weeks or months provide adequate training for many entry-level technical positions in the field, such as analysts and penetration testers, that provide the first line of defense. These programs are relatively inexpensive to run, portable, and offer veterans a post-service career that is both financially and personally rewarding.

Likewise, the Nation's robust community college system can be leveraged to assist with career changers, such as skilled or semi-skilled workers in regions where traditional economic drivers are waning, as well as underutilized populations such as women and minorities, those who are underemployed, or those simply looking to make a change to a growing and lucrative industry.

Once employed in the industry, these workers can pursue the higher degrees needed for management and leadership positions. Traditional higher education institutions are rising to the challenge as well by adding certificate and degree programs. The implementation of traditional four-year bachelor's degree programs in cybersecurity is an important step to building awareness of the field and providing a smooth path to entry for those pursuing four-year degrees. Likewise, master's degree programs provide education to fill another critical gap in the cybersecurity workforce: mid-career managers. However, these programs are in their infancy and not widely available. The Florida Center for Cybersecurity has worked closely with the State University System of Florida to introduce dozens of cybersecurity-specific programs across the system; this model needs to be adopted by other states and additional funding for students pursuing these degrees added to incentivize colleges and universities to make more cybersecurity programs available.

Part of the problem also lies in the lack of awareness of cybersecurity as a career. It is a relatively new field, and the need has grown so quickly that young people are simply unaware of the options and benefits offered by a cybersecurity career. Integrating better awareness of cybersecurity through the public education system, beginning at the earliest stages of education, will not only dramatically improve the Nation's levels of personal security, but also improve awareness of the field, allowing young people to begin planning and pursuing careers as cybersecurity professionals at a much earlier age. Teachers and guidance counselors in K–12 need to be engaged and trained to incorporate cybersecurity into lesson plans and career events throughout a child's academic journey.

In addition to leveraging the public education system, future cybersecurity professionals can be reached and inspired through gamification. Gamification, the process of applying a competitive scoring system to a training event, is rapidly gaining in popularity within the cybersecurity community not only for professional development, but also for general awareness training. Early programs are showing that employees retain and apply cybersecurity awareness training much better when taught using gamification. Leveraging the average high schooler's love of online gaming is an easy way to introduce them to the cybersecurity and to encourage them to start building their skills from a young age. More government-led, gamified cybersecurity training programs targeting youth could help inspire new practitioners and help the government be the first to identify burgeoning talent in the field.

In summary, funding for widespread availability of short-term, intensive training programs; youth camps and competitions; bachelor's and master's degree programs;

and outreach programming are needed to boost awareness and interest in the field and create pathways to success.

The Department of Homeland Security advocates these strategies and discusses them in greater detail in their document, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future, which can be found online at *https://www.dhs.gov/publication/supporting-growth-and-sustainment-nations-cyber security-workforce. We agree with the strategies and recommendations made in that report, and endeavor to support those recommendations across the state of Florida.*

*Question 3.* Blockchain and AI: Nevada has been a leader in developing various blockchain startups. This kind of activity across the country has led us to include policy in the 2017 defense bill that included a provision to allow the public sector to invest in modernization projects that could include the use of blockchain technology. This development is coming as we see exciting developments in Artificial Intelligence.

Can you speak to the potential of how blockchain and AI technologies may be used to help improve security and efficiency within the public and private sectors?

Answer. *Note: The following responses regarding blockchain were prepared with the assistance of Sagar Samtani, Ph.D., Assistant Professor, Information Systems and Decision Sciences (ISDS), University of South Florida, and Daniel Conway, instructor for the University of South Florida's Muma College of Business and expert on blockchain and cryptocurrency.*

Artificial Intelligence (AI) technologies hold significant promise to rapidly advance state-of-the-art cybersecurity practices within organizations and across industries. Specifically, AI can aide security analysts with automation. A security analyst (*e.g.,* Security Operations Center member) may have to deal with hundreds of thousands of indicators, alerts, and messages on a daily basis. AI can help provide a valuable mechanism to quickly and automatically (and in some cases, more accurately) sift through this data in a significantly shorter time frame than a traditional human analyst. AI can also help identify underlying patterns within the data, which the security analyst may not have been able to identify manually. As a result, new recommendations, correlations, and discoveries provided to security operations at remarkable speeds. Taken together, these benefits can help enable an organization to save significant amounts of time, labor, and ultimately cost. Moreover, they can provide a highly-scalable and efficient mechanism for an organization as it expands its operations to become more of a market leader.

Blockchain can be used in some facets of cybersecurity but has limitations. Blockchain is a peer-to-peer technology, an append-only database (meaning nothing can be removed or changed from the past) distributed across hundreds of thousands of computers. The security stems from the trust structure inherent in a distributed system where everyone has a copy of every transaction and agrees to it being "the" version of the truth. It is extremely difficult for the database to ever be deleted or held hostage by ransomware. No one can accidentally delete the record, as it is replicated on thousands of computers around the world running vastly different operating systems. This is a clear benefit, though less so with smaller blockchains or blockchains operating within one physical data center. The more widely the network replicates the ledger, the more resilient it is to a section of it (within a particular jurisdiction for example) becoming inaccessible. Thus, if the US, China, Russia, Japan, and Germany all decided to block all bitcoin traffic, Bitcoin would live on happily throughout the rest of the world.

However, blockchain does have a few restrictions. First, blockchain applications are still susceptible to social engineering weaknesses. A user is generally responsible for their own keys, and a loss of the keys means a loss of access to the assets on the blockchain. We expect better applications for key management/recovery in the future, but those applications will have all of the security risks of any web service or database application.

Second, one cannot take an existing application and "blockchain-ify" it. Each new blockchain will have to be written from scratch, with the configuration parameters hard-wired into the first block. There is a shortage of developers with this skill set (in the US), and thus we see leadership in application development coming from countries that are aggressively positioning themselves in this space, such as Estonia, China, South Korea, and Israel. That presents security issues if the source code employed is not freely available to all.

*Question 4.* Election: What are your recommendations for what we can be doing better to strengthen our election security from potential cyber intrusion?

Answer. *Note: The following responses regarding election security are offered by Eman El-Sheik, Ph.D., Professor, Computer Science, University of West Florida.*

Elections security is of utmost importance to our national security. There are several strategies that can help strengthen our elections security. I recommend coordinating efforts at national, state and county levels to share information and resources and stay ahead of the evolving threat landscape. There are several helpful initiatives that would be even more helpful if we can bring them together, *e.g.,* Department of Homeland Security vulnerability assessments, EI–ISAC and MS–ISAC information sharing centers and UWF Center for Cybersecurity training for elections officials. We need to coordinate these initiatives and develop effective strategies for helping every county and every election official to take advantage of these resources.

In addition, up-to-date cybersecurity training is crucial for everyone involved in elections processes, from the elections directors and supervisors to the volunteers. Many breaches are caused by user access, and employees can be an organization's greatest risk, regardless of how secure its networks and systems are. I recommend developing and coordinating a training program that integrates best practices and hands-on training and provides appropriate levels of training based on each person's role in the elections process.

We recommend planning a working meeting that brings together the Department of Homeland Security (DHS), National Association of State Election Directors (NASED), Election Assistance Commission (EAC) and other organizations to develop and implement a more coordinated strategy that can reach every county.

It is worth noting that The University of West Florida Center for Cybersecurity recently partnered with the Florida Department of State to provide cybersecurity training for elections supervisors and personnel across the state (see recent news).

*Question 5.* How can we effectively engage the global cybersecurity community to respond effectively to this challenge?

Answer. I recommend coordinating efforts to share information and resources among cybersecurity experts and allies more effectively and expeditiously. The cybersecurity threat landscape continues to evolve rapidly. Our efforts to secure our elections depend greatly on keeping up with the evolving landscape and on responding expeditiously.

*Question 6.* IoT: In recent months, the FBI has warned sophisticated Russian-linked hacking campaigns could be infecting hundreds of thousands of routers and home network devices around the world. As we move to the Internet of things, where nearly everything is connected, it will be even more important to deter data breaches.

What special considerations should be given as we move towards an economy powered by this technology?

Answer. Special consideration should be placed on risk awareness. In lieu of security standards and industry security guidelines, consumers, business and manufactures need to be aware of the risks associated with connected devices. Many are unaware of the risks associated with connecting IoT devices to the Internet. The Mirai Botnet is only one example of how connected devices can be exploited. We can expect to see even more disruptive exploits, exploits that cause significant or even physical damage to equipment. These attacks tend to rely on weaknesses in configuration and lax system administration. Ensuring general users, not just IT and cybersecurity staff, are aware of the risks and mitigation steps would help reduce the risk.

An analogy for our current situation can be found in the automotive industry. For decades, people drove and rode in cars without seatbelts. In the early 1980s, after thousands of preventable deaths, the auto industry and the government made a concerted effort to educate the public about the benefits of seatbelts. While that included legislation mandating seatbelt use, the awareness campaign is what truly created a culture shift where the public went from seeing seatbelts as an unnecessary inconvenience to a basic, easy win for safety that today we all engage in without giving it second thought. As a digital society, we face the same challenge. We've been using devices without seatbelts. The industry and government need to work together in a concerted effort to create an educated, mindful consumer population that engages basic security measures without giving it a second thought. For many, passwords, patches, and updates are seen as an unnecessary inconvenience. We need to shift the culture toward an understanding that these are basic, easy steps to protect one's digital wellbeing. The outreach and education for IoT should include a product rating system that alerts users to the device's default level of privacy and security features enabled and available on the device.

*Question 7.* Smart Cities: I have been active in the Senate developing bipartisan legislation on expanding the opportunities for local communities to tap Federal funding to build out smart communities. Nevada has been an exciting leader in

these kind of emerging opportunities with electric and autonomous buses, traffic management systems, and other new transit options, and that's just in the transportation sector. The possibilities to have technological solutions help address various local concerns communities by communities, or regions by regions, is very exciting and a large undertaking.

How can cities be incentivized to consider cybersecurity when investing in smart technologies?

Answer. *Note: The following responses regarding Smart Cities are offered by Kemal Akkaya, Ph.D., Professor of Electrical & Computer Engineer, Florida International University, a nationally recognized expert on Smart Cities and privacy.*

Cities have limited resources, so they are unwilling to do risky investments in smart technologies before they see the benefits. Therefore, they often ignore the cybersecurity investments due to its additional costs.

- One solution is to give priority to cities when federal/state government is funding infrastructure projects if the built infrastructure will implement smart technologies in a secure manner. In other words, smart infrastructure proposals with comprehensive security measures should be given priority in state/federal budgets.
- Another option is to create/increase the number of state/federal level research and development funding programs on smart city security and privacy and require city governments to be part of the research proposals. For instance, last year NSF started Smart and Connected Communities program, which encouraged local governments to be part of the proposals for increased funding chances. Other federal/state agencies can start similar programs, which may accelerate development and deployment of secure smart technologies that can also be adapted by other cities once they are successful.
- Finally, in the same lines, Federal or state governments could fund cooperative research/innovation regional cybersecurity centers, which can help and consult on implementing security solutions for cities. In this way, the costs for implementing security measures can be reduced.

*Question 8.* What policies do you believe are necessary to preserve privacy in smart cities?

Answer. Smart Cities typically work with third parties to use their services or apps that collect information from the citizens. Therefore, there are numerous stakeholders that can be involved. For instance, a parking app might include a city government, telecommunication company, financial institution, etc. that will be collecting information about the user. This is a special challenge that raises several issues regarding user data privacy as this data can be reused, combined with other relevant data for forecasting, and partially shared with other third parties. Plus, if the data is not securely communicated and stored, it can be compromised to steal Personally Identifiable Information (PII). Therefore, the following policies are recommended to preserve user privacy through various policies:

- Before launching any Smart City service or app, the stakeholders involved in that service should come together to agree on how to inform the user, how to store data without repetition, how to minimize/delete PII data after the service is provided, how to anonymize data, etc. Without such an agreement policy, the app/service should not be allowed to launch.
- There should be audit/policy enforcement mechanisms that can be imposed to these stakeholders by the state/federal government to check their apps and track the data stored in their servers if any. There are many emerging technologies that can certify certain apps to see if the data being sent is only sent to the proper stakeholders. They should agree to such audits when they are involved in any Smart City application.
- Once the data is stored, there needs to be proper encryption and access control mechanisms to access this data by the stakeholders so that not everyone from the stakeholders will have access to it. Again, there are various technologies to achieve this. It should be noted that the ultimate solution is to give the citizens' the ability to control this stored data (*i.e.,* to remove it, keep it or modify it) but this may take some time as the user awareness and abilities to do this are not currently at the desired levels.

*Question 9.* Private Sector Investment: Within the private sector, is enough being invested in cybersecurity?

Answer. The cybersecurity industry is benefitting from significant private investment. Momentum Cyber reports that $5.1 billion in financing was funneled into cybersecurity enterprises in 2017, with $2 billion funneled so far for 2018 and $3.8

billion in merges and acquisitions. Fintech Global reports that global cybersecurity investments increased more than 25 percent year-over-year for Q1 2018, and the ten most active investors in cybersecurity are headquartered in the US. The tremendous need for cybersecurity services across the Nation and around the world is driving healthy market growth in this sector and attracting hefty investment from private equity and venture capital firms.

*Question 10.* How can companies be incentivized to dedicate sufficient resources to this problem?

Answer. Between 2016 and 2017, we have seen a major shift among corporate leadership in attitudes toward cybersecurity investment. The 2018 Thales Data Threat Report showed that 73 percent of companies increased cybersecurity spending in 2017, up from 58 percent in 2016. A similar study done specifically for financial institutions showed 86 percent percent of financial services firms planned to increase cybersecurity spending in 2018, an increase from 60 percent in the previous year (*https://www.esecurityplanet.com/network-security/86-percent-of-financial-services-firms-to-increase-cyber-security-spend-in-2017.html*). Both studies reveal that corporate leadership is finally facing the reality of data breaches and the financial and reputation consequences that follow. Lawsuits, loss of reputational trust, hefty fines imposed by new legislation such as the European Union's General Data Protection Regulation have made the risk of a data breach a greater financial concern than ever before, forcing corporate leadership to engage in due diligence in this area.

---

## RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JON TESTER TO SRI SRIDHARAN

*Question 1.* Government Notification: Reports indicate that when Intel discovered the Spectre and Meltdown vulnerabilities, firms first notified Chinese technology companies Lenovo and Alibaba. However, the U.S. Government only found out about these vulnerabilities after the security vulnerabilities became public.

Hiring top cybersecurity talent at DHS is challenging due to Federal hiring logjams—including security clearance delays, salaries, and private sector competition. A) What strategies should we implement to improve the Federal Government's cybersecurity workforce at agencies such as DHS? B) How do we keep pace with geo-strategic competitors such as Russia and China?

Answer. *Response (A):* We at the Florida Center for Cybersecurity have had great success with veterans' training programs, and I believe these programs can provide significant relief for the Federal Government's hiring challenges. Veterans (and their families) are ideal candidates for cybersecurity positions, particularly those in government agencies, for several reasons. First, military training teaches strategic thinking, analytical problem-solving, adaptability, and the value of collaboration. Second, they have been pre-screened and many have held high-level security clearances. Third, they have a demonstrated commitment to country and service that supplants, which often remains with them in new career paths. Lastly, the jobs are portable, have no physical requirement, and can be performed remotely, making cybersecurity an optimal career path for disabled veterans as well as spouses and families of veterans, who may need to move frequently.

Furthermore, many entry-level cybersecurity jobs do not require a four-year degree. Short-term intensive training programs that take only weeks or months provide adequate training for many entry-level technical positions in the field, such as analysts and penetration testers, that provide the first line of defense. These programs are relatively inexpensive to run, portable, and offer veterans a post-service career that is both financially and personally rewarding.

Likewise, the Nation's robust community college system can be leveraged to assist with career changers, such as skilled or semi-skilled workers in regions where traditional economic drivers are waning, as well as underutilized populations such as women and minorities, those who are underemployed, or those simply looking to make a change to a growing and lucrative industry.

Once employed in the industry, these workers can pursue the higher degrees needed for management and leadership positions. Traditional higher education institutions are rising to the challenge as well by adding certificate and degree programs. The implementation of traditional four-year bachelor's degree programs in cybersecurity is an important step to building awareness of the field and providing a smooth path to entry for those pursuing four-year degrees. Likewise, master's degree programs provide education to fill another critical gap in the cybersecurity workforce: mid-career managers. However, these programs are in their infancy and not widely available. The Florida Center for Cybersecurity has worked closely with

the State University System of Florida to introduce dozens of cybersecurity-specific programs across the system; this model needs to be adopted by other states and additional funding for students pursuing these degrees added to incentivize colleges and universities to make more cybersecurity programs available.

Part of the problem also lies in the lack of awareness of cybersecurity as a career. It is a relatively new field, and the need has grown so quickly that young people are simply unaware of the options and benefits offered by a cybersecurity career. Integrating better awareness of cybersecurity through the public education system, beginning at the earliest stages of education, will not only dramatically improve the Nation's levels of personal security, but also improve awareness of the field, allowing young people to begin planning and pursuing careers as cybersecurity professionals at a much earlier age. Teachers and guidance counselors in K–12 need to be engaged and trained to incorporate cybersecurity into lesson plans and career events throughout a child's academic journey.

In addition to leveraging the public education system, future cybersecurity professionals can be reached and inspired through gamification. Gamification, the process of applying a competitive scoring system to a training event, is rapidly gaining in popularity within the cybersecurity community not only for professional development, but also for general awareness training. Early programs are showing that employees retain and apply cybersecurity awareness training much better when taught using gamification. Leveraging the average high schooler's love of online gaming is an easy way to introduce them to the cybersecurity and to encourage them to start building their skills from a young age. More government-led, gamified cybersecurity training programs targeting youth could help inspire new practitioners and help the government be the first to identify burgeoning talent in the field.

In summary, funding for widespread availability of short-term, intensive training programs; youth camps and competitions; bachelor's and master's degree programs; and outreach programming are needed to boost awareness and interest in the field and create pathways to success.

The Department of Homeland Security advocates these strategies and discusses them in greater detail in their document, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future, which can be found online at *https://www.dhs.gov/publication/supporting-growth-and-sustainment-nations-cybersecurity-workforce.* We agree with the strategies and recommendations made in that report, and endeavor to support those recommendations across the state of Florida.

*Response (B):* While the Russian and Chinese governments were prescient in their investment in cybersecurity forces, the United States remains a global superpower in this realm thanks to the outstanding intellect and dedication of the men and women employed in the Intelligence Community and Armed Forces. To stay ahead of our competition, we must act on two fronts. First, we must invest the resources necessary to attract more workers to the field, as outlined in response (A). Second, the United States must remain innovative and attractive to the best and brightest scientific minds from around the world. By maintaining a high standard of living, an inviting scientific community, and an immigration policy with clear paths of entry for thoroughly vetted industry contributors, we can continue to supplement our existing talent pool with the world's leading practitioners and researchers.

*Question 2.* Human Element: Software patches are only as good as the person installing them. Most folks out there aren't nearly as tech savvy or as familiar with cyber-hygiene best practices as the folks on this panel. This whole system of patches and updates seems to break down when the average user is not aware of the problem, does not take the time to install updates or even know how to do so.

How would you recommend U.S. consumers, businesses and government entities—including Congress—better equip ourselves and the American people for the ever-changing cyber vulnerabilities we face?

Answer. Vigilance in maintaining awareness is required by individuals, businesses, and government entities, and this vigilance must become the cultural norm across the country. For decades, people drove and rode in cars without seatbelts. In the early 1980s, after thousands of preventable deaths, the auto industry and the government made a concerted effort to educate the public about the benefits of seatbelts. While that included legislation mandating seatbelt use, the awareness campaign is what truly created a culture shift where the public went from seeing seatbelts as an unnecessary inconvenience to a basic, easy win for safety that today we all engage in without giving it second thought. As a digital society, we face the same challenge. We've been using devices without seatbelts. The industry and government need to work together in a concerted effort to create an educated, mindful consumer population that engages basic security measures without giving it a second thought. For many, passwords, patches, and updates are seen as an unnecessary inconven-

ience. We need to shift the culture toward an understanding that these are basic, easy steps to protect one's digital wellbeing.

*Question 3.* What role should private industry play in making the average consumer aware of cyber vulnerabilities to their software or hardware, whether it on their CPU, smartphone, or car? What role do you believe should the U.S. Government should play?

Answer. As discussed in the previous question, connected devices have become so ubiquitous that most people, especially young people who have grown up with this technology in place, often don't even think about how or why their device connected . . . the connection process is merely an inconvenience they must suffer through to "get it to work." Each device has a different level of connectivity and different data capturing and transmission abilities. The industry must adopt a common lexicon when describing device capabilities that consumers can recognize and understand and label devices accordingly so that consumers are aware of the level of connectivity and potential vulnerability for each device they use, from thermostats and baby monitors to laptop and smartphones. Does it connect? Do you enter information, or does the device automatically gather information? Where does that information go? Does it record audio and video? Any connected device that sends or receives a signal—even wireless radio signals—has the potential to be hacked or breached. For example, take the case of free USB charging stations now available at most airports as a convenience for travelers. If one connects a USB charging cable that is only capable of charging—not data transmission—using a public USB station is not a threat. However, most USB charging cables are also used for transmitting data. Plug one of those into a public USB port, and one could easily transfer malware to their device as it charges. Most consumers do not know which type of charging cable they have because this information is not clearly presented on packaging or in instruction manuals.

Manufacturers have an obligation to inform consumers about the potential risks of their products, and cyberattacks and data breaches should be treated the same as any other risk since the potential for personal and financial damage is just as significant. In addition to alerting consumers to the device's level of connectivity and ability to gather and transmit data, manufacturers should make it easy for users to engage basic security features and encourage them to do so. For example, last Christmas a popular children's toy offered Internet connectivity with virtually no safety protocols in place. Researchers found that anyone within 100 feet of the doll could easily hijack the signal and speak to children through the doll's built-in microphone and speaker system. More recently, a disturbing story came to light in which a mother discovered that someone had hacked into her video baby monitor and was using the camera to spy on her. When she attempted to change the password through the device's smartphone app, the hacker locked her out (*https://www.wtsp.com/article/news/investigations/investigators/sc-mom-says-stranger-hacked-baby-monitor-to-spy-on-her-family/275-561796417*). Any device that connects should come with a clear description of the potential dangers and clear instructions for engaging safety features right out of the box.

○