

THE STATUS AND OUTLOOK FOR CYBERSECURITY
EFFORTS IN THE ENERGY INDUSTRY

HEARING
BEFORE THE
COMMITTEE ON
ENERGY AND NATURAL RESOURCES
UNITED STATES SENATE
ONE HUNDRED SIXTEENTH CONGRESS
FIRST SESSION

FEBRUARY 14, 2019



Printed for the use of the
Committee on Energy and Natural Resources

Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

JOHN BARRASSO, Wyoming

JAMES E. RISCH, Idaho

MIKE LEE, Utah

STEVE DAINES, Montana

BILL CASSIDY, Louisiana

CORY GARDNER, Colorado

CINDY HYDE-SMITH, Mississippi

MARTHA MCSALLY, Arizona

LAMAR ALEXANDER, Tennessee

JOHN HOEVEN, North Dakota

JOE MANCHIN III, West Virginia

RON WYDEN, Oregon

MARIA CANTWELL, Washington

BERNARD SANDERS, Vermont

DEBBIE STABENOW, Michigan

MARTIN HEINRICH, New Mexico

MAZIE K. HIRONO, Hawaii

ANGUS S. KING, JR., Maine

CATHERINE CORTEZ MASTO, Nevada

BRIAN HUGHES, *Staff Director*

KELLIE DONNELLY, *Chief Counsel*

JED DEARBORN, *Senior Counsel*

ROBERT IVANAUSKAS, *FERC Detailee*

SARAH VENUTO, *Democratic Staff Director*

SAM E. FOWLER, *Democratic Chief Counsel*

DAVID GILLERS, *Democratic Senior Counsel*

BRIE VAN CLEVE, *Democratic Professional Staff Member*

CONTENTS

OPENING STATEMENTS

	Page
Murkowski, Hon. Lisa, Chairman and a U.S. Senator from Alaska	1
Manchin III, Hon. Joe, Ranking Member and a U.S. Senator from West Virginia	3

WITNESSES

Chatterjee, Hon. Neil, Chairman, Federal Energy Regulatory Commission	5
Evans, Hon. Karen S., Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy	9
Keber, Major William J., Executive Officer, West Virginia National Guard's Critical Infrastructure Protection Battalion	19
Robb, James B., President and Chief Executive Officer, North American Electric Reliability Corporation	24
Whitehead, David Edward, Chief Operating Officer, Schweitzer Engineering Laboratories, Inc.	34

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

Chatterjee, Hon. Neil:	
Opening Statement	5
Written Testimony	7
Responses to Questions for the Record	68
Evans, Hon. Karen S.:	
Opening Statement	9
Written Testimony	11
Responses to Questions for the Record	75
Keber, Major William J.:	
Opening Statement	19
Written Testimony	21
Responses to Questions for the Record	99
Manchin III, Hon. Joe:	
Opening Statement	3
Murkowski, Hon. Lisa:	
Opening Statement	1
Robb, James B.:	
Opening Statement	24
Written Testimony	26
Responses to Questions for the Record	164
Whitehead, David E.:	
Opening Statement	34
Written Testimony	36
Responses to Questions for the Record	170

THE STATUS AND OUTLOOK FOR CYBERSECURITY EFFORTS IN THE ENERGY INDUSTRY

THURSDAY, FEBRUARY 14, 2019

U.S. SENATE,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The Committee met, pursuant to notice, at 10:09 a.m. in Room SD-366, Dirksen Senate Office Building, Hon. Lisa Murkowski, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. LISA MURKOWSKI, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Good morning. The Committee will come to order.

I will just note for the record that today is Valentine's Day.

Senator MANCHIN. Happy Valentine's.

The CHAIRMAN. Thank you.

Some people celebrate it with flowers and chocolate. It is actually my son's birthday, so we observe it as a birthday rather than flowers and chocolate today.

But here at the Energy Committee what we prefer to do is take a deep dive into the very real cyber threats that face our electric grid system. Here is the punchline everyone, hold on. After all, nothing says love like ensuring the security of our critical energy infrastructure. So that is our Valentine's statement for the morning from the Energy and Natural Resources Committee. You have to love the script writers back here.

[Laughter.]

Last week we had a chance to examine the state of energy markets and the promise of clean energy innovation. Both of these hearings, great hearings by the way, highlighted the increased automation and the digitalization of energy technologies. While advances in technology are always welcome and can help us run things more efficiently, each new digital connection opens a potential pathway for bad actors to disrupt our energy delivery.

We know that the threat of cyberattacks by our foreign adversaries and other sophisticated entities is real and it is growing. Last month's 2019 Worldwide Threat Assessment detailed how China, Russia and other foreign adversaries are using cyber operations to target our military and our critical infrastructure. The assessment notes that our electric grid and natural gas pipelines are particularly vulnerable to attack and that Russia is mapping

our infrastructure with the long-term goal of causing substantial damage.

Unfortunately, we have already seen the real-world ramifications of cyberattacks on energy infrastructure. Back in December 2015, Russian hackers cut off power to nearly a quarter-million people in Ukraine. And in the summer of 2017, Russian hackers infiltrated the industrial control system of a Saudi Arabian petrochemical plant and disabled the plant's safety systems.

We cannot let a similar attack happen in the United States. Our grid system is 'uniquely critical' and the consequences of a successful cyber incursion would be widespread and devastating. The resulting loss of power could impact hospitals, banks, cell phone service, gas pumps, traffic lights, you name it.

The government's focus on cybersecurity, in partnership with industry, is a major reason that the United States has not experienced an attack like Ukraine's. In the 2005 Energy Policy Act, Congress created the Electric Reliability Organization. We have since certified it as NERC and mandated reliability standards to be developed through an industry stakeholder process. Protecting our nation's critical assets is a shared responsibility, with federal, state, and private sector partners working together to improve cyber defenses and coordinate responses to cyberattacks.

The 2015 FAST Act enacted provisions authored by this Committee to codify the Department of Energy (DOE) as the sector-specific agency for energy sector cybersecurity and provide the Secretary with authority to address grid-related emergencies. We also enacted provisions to facilitate greater information sharing by protecting sensitive information from disclosure.

The Administration is taking steps to address emerging cyber threats. Last year, DOE established the new Office of Cybersecurity, Energy Security, and Emergency Response, known as "CESER." I look forward to learning more about the work that is being done by this office. Assistant Secretary Evans has been on the job for about six months, so gaining her perspective this morning is going to be very useful for us.

The Department is also partnering with FERC to find solutions to energy infrastructure threats. Next month the agencies will co-host a technical conference to discuss current and emerging cyber and physical security threats, as well as ways to incentivize cybersecurity investments. It is important that we are seeing these agencies prioritize cybersecurity and plan this conference very closely together.

I am pleased to welcome a very distinguished panel this morning. We have Chairman Neil Chatterjee from the Federal Energy Regulatory Commission (FERC). We appreciate your leadership at the Commission and look forward to your comments this morning. I have already mentioned Karen Evans, the Assistant Secretary at the Department of Energy working in CESER. From the North American Electric Reliability Corporation, or NERC, we have Mr. James Robb. We have David Whitehead from Schweitzer Engineering Labs (SEL), and we have Major William Keber from the West Virginia National Guard Critical Infrastructure Protection Battalion.

I think it is well recognized that the panel we have in front of us represents those who are on the frontlines of the effort to protect our energy infrastructure from cyber threats.

Thank you all for being here. I look forward to your testimony and comments.

I will now turn to my Ranking Member, Senator Manchin.

**STATEMENT OF HON. JOE MANCHIN III,
U.S. SENATOR FROM WEST VIRGINIA**

Senator MANCHIN. Well, thank you, Madam Chairman, and Happy Valentine's Day to you and everybody else out there, men and women, mostly the women.

The CHAIRMAN. Men too.

Senator MANCHIN. True, it is mostly women.

[Laughter.]

A tidbit I read this morning, it was really interesting and fitting for today about how we got the name of Saint Valentine's Day, or Valentine's Day.

Saint Valentine, in the second century of the Roman Empire, basically, the Roman Emperor, Roman rulers, forbade their soldiers from getting married. They thought they were better fighters if they did not marry. Saint Valentine, basically, was performing marriages because he was a devout Christian, and he would say after he would perform the marriage, Happy Valentine. And so, it came from Saint Valentine. That is how we got Valentine's Day. It was very interesting to hear that, and I thought I would share that with you. I don't know if it is factual or not, but it sounds good.

[Laughter.]

Chairman Murkowski, I want to thank you for convening the Committee today to talk about cybersecurity efforts in the energy industry. This hearing is particularly timely because just a few weeks ago, our Director of National Intelligence, Dan Coats, publicly warned of two potential energy cybersecurity attack scenarios: a Russian cyberattack that could disrupt an electrical network for a few hours and a Chinese cyberattack that could disrupt a natural gas pipeline for weeks. These threats are not just theoretical.

We know that in 2015 and 2016, Ukraine suffered two devastating power outages as a result of cyberattacks. And according to the New York Times, a petrochemical plant in Saudi Arabia was hit with an even more serious type of cyberattack in 2017. That attack was not designed to shut down the plant, like the Ukraine power outages. It was meant to "sabotage the firm's operations and trigger an explosion." In other words, the attack could have taken human lives, but luckily it did not.

I cannot overstate how serious this threat is, and I am pleased that Secretary Perry has given this the attention it deserves by elevating cybersecurity to an office of its own, the Office of Cybersecurity, Energy Security, and Emergency Response, or CEEER, for short.

On a personal note, I am also pleased that the first Assistant Secretary to run this office is Karen Evans, who has not one but two degrees from WVU, a very smart lady.

I am also especially pleased to have Major Keber of the West Virginia National Guard here to share the great work the Guard has done for West Virginia in the cybersecurity space.

My current position as the Ranking Member of the Senate Armed Services Subcommittee on Cybersecurity and my time serving on the Intelligence Committee further convinced me that we need to look at this as a national security priority.

Energy cybersecurity is national security. Period. Absolutely. In fact, there are two items I raised in the Armed Services Committee in our first cybersecurity hearing that are equally relevant in the energy space.

First, supply chain security has emerged as a significant focus in both spaces. We have to make sure the companies that build components for our grid are secure. We have to protect against vendors' remote access of the grid being exploited, and we have to make sure that attackers do not insert malware into a vendor software update.

Second, our cyber workforce is in crisis. We simply do not have enough cyber workers to fill the positions. Forbes reports that by 2021, there will be as many as 3.5 million, I repeat, 3.5 million unfilled positions. Yes, a big part of this is about getting training, but let's not put the cart before the horse. It is also about bringing these jobs to the areas that need them.

I think that is where there is an opportunity here for states like West Virginia and Alaska to fill the gap. I know that Major Keber will speak to this a bit more, but the West Virginia National Guard is one of the few National Guard units with access to a decommissioned power plant for workforce training, and they are increasing their workforce development efforts.

I look forward to hearing from our witnesses about how the nation can rise to this challenge while strengthening the economies of places like West Virginia and Alaska. I look forward to hearing from our witnesses about how the nation can rise to this challenge while strengthening the economies in places like Southern West Virginia and rural Alaska. And I think it will require collaboration between all entities, including those represented by our witnesses here today, to get where we need to go.

My little State of West Virginia has been a leader on energy supply and reliability for this country. But unless cybersecurity challenges are addressed head on, it won't matter how much supply we have. We must do everything we can to protect and ensure the security of our infrastructure. As we kick off that conversation in this new Congress, I am glad to have this great panel here today to share their outlook for cybersecurity in the energy industry.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Manchin.

We will now turn to our witnesses. I introduced everybody, so we will just go ahead and proceed.

We will begin with you, Chairman Chatterjee. We would ask that you all try to keep your comments to about five minutes. Your full statements will be incorporated as part of the record. Again, we appreciate the level of expertise that you bring to this very, very important discussion.

Chairman Chatterjee.

**STATEMENT OF HON. NEIL CHATTERJEE, CHAIRMAN,
FEDERAL ENERGY REGULATORY COMMISSION**

Mr. CHATTERJEE. Chair Murkowski, Ranking Member Manchin, and Members of the Committee, thank you for inviting me to appear before you today to discuss the cybersecurity in the energy sector. I appreciate the Committee's attention to this crucial subject and the role that the Federal Energy Regulatory Commission plays in securing our nation's critical infrastructure.

I'd like to take this opportunity to highlight three major issues for the Committee. First, the evolution of mandatory reliability standards; second, the voluntary partnerships FERC has established with industry and other agencies; and third, the interdependency of the electric and natural gas systems.

Turning first to the topic of Mandatory Reliability Standards. As part of the Energy Policy Act of 2005, Congress gave the Commission the authority to approve and enforce mandatory reliability standards for the nation's bulk power system, including for cybersecurity.

As I'm sure Jim Robb will discuss in greater detail, EPACT '05 established a joint responsibility between the Commission and NERC as the designated electric reliability organization for developing and enforcing the reliability standards. Because of the unique relationship between our organizations, maintaining an open and collaborative relationship between NERC and the Commission has been a top priority during my tenure. I'd like to thank Jim and the rest of the team at NERC for their dedicated efforts, and I look forward to continuing our important work together.

NERC's standards for cybersecurity, known as the Critical Infrastructure Protection, or CIP, standards became mandatory and enforceable in 2009. Since 2009, the CIP standards have matured considerably and now form an effective framework for protections against cyber threats. The evolution of these standards has reduced the need for constant revisions to address discreet issues and instead has allowed both FERC and NERC to focus on tackling emerging threats. In particular, I'd like to call the Committee's attention to two important actions that the Commission has recently taken on this front.

First, at our Commission meeting last October, FERC approved reliability standards to address supply chain threats. By exploiting vulnerabilities in the electric utility supply chain, adversaries can seize on a variety of opportunities to compromise critical systems. While supply chain vulnerabilities are some of the most important to address, they're also some of the most difficult to mitigate. This is because today's utilities rely on a highly integrated, global supply chain to meet their business needs. Leveraging this modern network of vendors can provide utilities with significant benefits but it also presents difficulties in comprehensively identifying risks. While there is no silver bullet to mitigate supply chain risks, I believe this standard is a significant step in the right direction.

Second, at our meeting last July, the Commission approved a final rule directing NERC to expand reporting requirements for critical systems. That rule directed NERC to develop a standard requiring registered entities to report both successful and attempted intrusions into critical systems to NERC's Electricity Information

Sharing and Analysis Center, as well as to the Department of Homeland Security. This final rule represents another important step toward mitigating risks by enhancing the collection and distribution of information on rapidly evolving threats.

While the NERC CIP standards form an important baseline, compliance alone is not enough to achieve cybersecurity excellence. That's why the Commission has adopted a two-prong approach to address threats to energy infrastructure, mandatory reliability standards overseen by our Office of Electric Reliability and voluntary initiatives overseen by our Office of Energy Infrastructure Security, also known as OEIS.

OEIS engages with partners in industry, states, and other federal agencies to develop and promote best practices for critical infrastructure security. These initiatives include, among other things, voluntary architecture assessments, classified briefings for state and industry officials, and joint security programs with other government agencies in the private sector. Because the responsibility for securing critical infrastructure is shared across the public and private sector, I am a strong supporter of our efforts to continue strengthening these partnerships.

As part of that objective, the Commission continues to work collaboratively in this area and will be hosting a joint technical conference on March 28th with the Department of Energy to discuss investments for cyber and physical security. The conference will explore current threats against energy infrastructure, best practices for mitigation, incentives for investing in physical and cybersecurity protections and cost recovery practices at both the state and federal level. And there's one final area where I believe continued partnership across industry and government will be essential. Because of our nation's growing use of natural gas for power generation, I'm increasingly concerned about the security of our natural gas pipeline system.

Last year I joined my colleague, Commissioner Rich Glick, in an op-ed, detailing how a successful cyberattack on the system could have a significant impact on the electric grid. Given this vulnerability, Commissioner Glick and I expressed our view that more must be done to ensure robust oversight for natural gas pipeline cybersecurity. Since the publication of that op-ed, I've been pleased to hear from many members of the natural gas pipeline community who have expressed their appreciation for these concerns and a willingness to continue taking steps to improve their security posture. I also recently met with TSA Administrator David Pekoske and was impressed by his focus on this vital issue as well as his pledge to further improve TSA's oversight of pipeline security.

While I think both industry and government have made significant strides, I believe more work still needs to be done. The Commission stands ready to assist in these efforts wherever we can.

Now before I conclude my opening statement, I want to thank each of you, again, for your efforts in this space and your time to engage in this conversation today. These are complex issues and they won't be solved easily, but I appreciate the opportunity to come before you today, and look forward to continuing this essential dialogue.

[The prepared statement of Mr. Chatterjee follows:]

**Testimony of Neil Chatterjee
Chairman, Federal Energy Regulatory Commission
Before the Committee on Energy and Natural Resources
United States Senate
February 14, 2019**

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee:

Thank you for inviting me to appear before you today to discuss the important issue of cybersecurity in the energy sector. I appreciate the Committee's attention to this crucial issue and the role that the Federal Energy Regulatory Commission (FERC) plays in securing our nation's critical infrastructure.

I'd like to take this opportunity to highlight three major issues for the Committee: first, the evolution of mandatory reliability standards; second, the voluntary partnerships FERC has established with industry and other agencies; and third, the interdependency of the electric and natural gas systems.

Mandatory Reliability Standards

Under Section 215 of the Federal Power Act, the Commission has authority to approve mandatory reliability standards developed by the North American Electric Reliability Corporation (NERC). Once approved by the Commission, the standards are mandatory and enforceable either by NERC or independently by the Commission. The Commission also has the authority to direct that NERC develop a mandatory standard to address reliability concerns identified by the Commission. NERC's standards for cybersecurity, known as the Critical Infrastructure Protection (CIP) standards, became mandatory and enforceable in 2009.

Since then, the CIP standards have matured considerably and now form an effective framework for protections against cyber threats. The maturation of the CIP standards regime has reduced the need for constant revisions to address discrete issues and, instead, has allowed both FERC and NERC to focus on tackling emerging threats. In particular, I'd like to call the Committee's attention to two important actions that the Commission has recently taken on this front. First, at our October 2018 Commission Meeting, FERC approved NERC's proposed reliability standards to address supply chain threats. This action is particularly significant given that these specific threats to the energy sector continue to grow. Second, at our July 2018 Commission Meeting, FERC approved a final rule directing NERC to expand reporting requirements for critical systems. That final rule directed NERC to develop a standard that requires registered entities to report successful and attempted intrusions into critical systems to NERC's Electricity Information Sharing and Analysis Center, as well as to the Department of Homeland Security (DHS). I believe this final rule represents an important step toward enhancing the collection and distribution of information on rapidly evolving threats.

Voluntary Partnerships

While the NERC CIP standards form an important baseline for cybersecurity practices,

compliance alone is not enough to achieve cybersecurity excellence. Therefore, the Commission has adopted a two-prong approach to address threats to energy infrastructure: mandatory reliability standards overseen by our Office of Electric Reliability, and voluntary initiatives overseen by our Office of Energy Infrastructure Security (OEIS). OEIS engages with partners in industry, states, and other federal agencies to develop and promote best practices for critical infrastructure security. These initiatives include, among other things, voluntary architecture assessments of interested entities, classified briefings for state and industry officials, and joint security programs with other government agencies and industry.

Because the responsibility for securing critical infrastructure is shared across industry, federal, and state governments, I believe it's imperative that we continue to strengthen these partnerships. To this end, the Commission continues to work collaboratively in this area and will be hosting a joint technical conference on March 28, 2019 with the Department of Energy, state, and industry officials, to discuss investments for cyber and physical security. The conference will explore current threats against energy infrastructure, best practices for mitigation, current incentives for investing in physical and cybersecurity protections, and cost recovery practices at both the state and federal level.

I'd also like to take a moment to highlight OEIS's joint efforts with the DHS National Risk Management Center and the Transportation Security Administration (TSA) to develop better approaches for managing cybersecurity risks to natural gas pipelines. As I discuss further below, I believe securing our natural gas infrastructure is critical to safeguarding the reliability of the electric system.

Interdependency of Electric and Natural Gas Systems

As I discussed in a joint op-ed with my colleague Commissioner Glick last year, I am concerned that, because of our nation's growing use of natural gas for power generation, a successful cyber-attack on the natural gas pipeline system could have a significant impact on the electric grid. Given this increasing vulnerability, Commissioner Glick and I expressed our view that more must be done to ensure robust oversight for natural gas pipeline cybersecurity. Since the publication of that op-ed, I've been pleased to hear from many members of the natural gas pipeline community who have expressed their appreciation for these concerns and willingness to continue taking steps to improve their security posture. In addition, I recently met with TSA Administrator David Pekoske to discuss pipeline cybersecurity and was impressed by his focus on this vital issue as well as his pledge to taking further action to improve TSA's oversight of pipeline security. While I think both industry and government have made significant strides toward addressing this issue, I believe more work still needs to be done, and the Commission stands ready to assist in these efforts.

Conclusion

Protecting the energy sector from cyber threats will require each of us to do our part, and I assure you that we at the Commission are ready and willing to continue working together with each of you on the Committee, the full Congress and other agencies to bolster our nation's cybersecurity posture. Again, I appreciate the opportunity to come before you today, and I look forward to continuing this essential dialogue.

The CHAIRMAN. Thank you, Chairman Chatterjee.
Welcome, Assistant Secretary Evans.

STATEMENT OF HON. KAREN S. EVANS, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, U.S. DEPARTMENT OF ENERGY

Ms. EVANS. Chairman Murkowski, Ranking Member Manchin and members of the Committee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure. Focusing on cybersecurity, energy security and the resilience of the nation's energy systems is one of Secretary Perry's top priorities.

By the Secretary proposing and Congress affirming the Office of Cybersecurity, Energy Security, and Emergency Response, also known as CESER, the Secretary clearly demonstrated his commitment to achieving the Administration's goal of energy security and, more broadly, national security.

Our nation's energy infrastructure has become a primary target for hostile cyber actors, both state sponsored and non-state sponsored. The frequency, scale and sophistication of cyber threats have increased. Our cyber incidences have the potential to disrupt energy services, damage highly specialized equipment and even threaten human health and safety.

The Director of National Intelligence along with several heads of the Administration's Intelligence agencies recently stated in written testimony that China has the ability to launch cyberattacks that cause localized, temporary, disruptive effects on critical infrastructure such as the disruption of a natural gas pipelines for days to weeks. Russia also has similar abilities with the capability to disrupt an electrical distribution network for at least a few hours, similar to those demonstrated in the Ukraine in 2015 and 2016.

The release of the President's National Cyber Strategy, also known as NCS, in September, reflects the Administration's commitment to protecting America from cyber threats. The Department of Energy plays an active role in supporting the security of our nation's critical energy infrastructure in implementing the NCS.

As a result, energy cybersecurity and resilience has emerged as one of the nation's most important security challenges and fostering partnerships with public and private stakeholders is of the utmost importance for me, as the Assistant Secretary of CESER.

CESER and its predecessor organization have demonstrated the emergency response function through multiple weather events, including hurricanes, by activating our emergency response organization. In 2018, CESER responded to over a wide range of incidences, including six hurricanes, three wildfires, two typhoons, a cyclone, an earthquake and a volcano eruption. Recently we worked closely with the federal industry and state partners to monitor the impact to the energy sector in the January 2019 Arctic Blast that affected central and eastern portions of the nation.

However, today I would like to focus my testimony primarily on the cybersecurity function of the office and how CESER will meet the priorities of the Administration and work in conjunction with our federal agencies, state, local, tribal, territorial governments, industry and our national lab partners. The Secretary has conveyed

that he has no higher priority than to support the security of our nation's critical energy infrastructure.

CESER has the Department's lead to secure our nation's energy infrastructure against all hazards, reduce risks of and impacts from cyber events and disruptive events and assist with restoration activities. The office enhances the Department's ability to dedicate and focus attention on DOE sector-specific agency responsibilities and will provide greater visibility, accountability and flexibility to better protect our nation's energy infrastructure and support asset owners as well as the overall critical infrastructure response framework, as overseen by DHS.

Establishing CESER is the result of the Administration's commitment to and prioritization of energy security and national security. Our long-term approach strengthens our national security and positively impacts our economy. As CESER moves forward, we are taking the first steps in transformational change to achieve the Secretary's priority of emergency preparedness and rapid, coordinated response to disruptions in the energy sector.

I appreciate the opportunity to appear before this Committee to discuss cybersecurity in the energy sector and I applaud your leadership. I look forward to working with you and your respective staffs to continue to address cyber and physical security challenges.

[The prepared statement of Ms. Evans follows:]

Testimony of Assistant Secretary Karen S. Evans
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
Before the
Committee on Energy & Natural Resources
United States Senate
February 14, 2019

Introduction

Chairman Murkowski, Ranking Member Manchin, and Members of the Committee, thank you for the opportunity to discuss the continuing threats facing our national energy infrastructure. Focusing on cybersecurity, energy security, and the resilience of the Nation's energy systems is one of Secretary Rick Perry's top priorities. By the Secretary proposing and Congress affirming the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the Secretary clearly demonstrated his commitment to achieving the Administration's goal of energy security and, more broadly, national security.

Our Nation's energy infrastructure has become a primary target for hostile cyber actors, both state-sponsored and non-state sponsored. The frequency, scale, and sophistication of cyber threats have increased. Cyber incidents have the potential to disrupt energy services, damage highly specialized equipment, and even threaten human health and safety.

The Director of National Intelligence, along with several heads of the Administration's Intelligence Community agencies, recently stated in written testimony that "China has the ability to launch cyberattacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks." Russia has similar abilities with the capability to disrupt "an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016."

The release of the President's National Cyber Strategy (NCS) in September reflects the Administration's commitment to protecting America from cyber threats. The Department of Energy (DOE) plays an active role in supporting the security of our Nation's critical energy infrastructure in implementing the NCS. As a result, energy cybersecurity and resilience has emerged as one of the Nation's most important security challenges and fostering partnerships with public and private stakeholders is of utmost importance as the Assistant Secretary of CESER.

CESER and its predecessor organization have demonstrated the Emergency Response function through multiple weather events, including hurricanes, activating our Emergency Response Organization. In 2018, CESER responded to a wide range of incidents, including

six hurricanes, three wildfires, two typhoons, a cyclone, an earthquake, and a volcanic eruption. Recently, we worked closely with Federal, industry, and State partners to monitor the impacts to the energy sector from the January 2019 “arctic blast” that affected the central and eastern portions of the Nation.

However, today, I would like to focus my testimony primarily on the cybersecurity function of the office and how CESER will meet the priorities of the Administration and work in conjunction with our Federal agency, State, local, tribal and territorial government (SLTT), industry, and National Laboratory partners.

DOE FAST Act Authority

DOE’s role in energy sector cybersecurity is established in statute and executive action. In 2015, Congress passed the Fixing America’s Surface Transportation (FAST) Act (P.L. 114-94), codifying DOE as the Sector-Specific Agency (SSA) for cybersecurity for the energy sector, consistent with existing policy. Defined in Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, “the term ‘Sector- Specific Agency’ (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.” PPD-21 states that the Department of Homeland Security (DHS) will “provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation’s critical infrastructure.” Specific to cybersecurity, DHS has authorities that support cybersecurity assistance by the federal government to all critical infrastructure sectors, including information sharing and technical assistance. The FAST Act further mandates that the Secretary of Energy coordinates “with the Department of Homeland Security and other relevant Federal departments and agencies” and collaborates with them on, among other things, “providing, supporting, or facilitating technical assistance and consultations for the energy sector to identify vulnerabilities and help mitigate incidents, as appropriate.” With the formation of CESER, the Department’s role as the SSA is strengthened and has undertaken the responsibilities with the highest degree of dedication and commitment.

The FAST Act also amended the Federal Power Act to give the Secretary of Energy new authority, upon declaration of a Grid Security Emergency by the President, to issue emergency orders to protect or restore critical electric infrastructure or defense critical electric infrastructure. This authority allows DOE to support energy sector preparations for, and responses to, events.

CESER

The Secretary has conveyed that he has no higher priority than to support the security of our Nation’s critical energy infrastructure. CESER leads the Department’s efforts to secure our Nation’s energy infrastructure against all hazards, reduce the risks of and impacts from cyber events and other disruptive events, and assist with restoration activities. This office works closely with the private sector, as well as Federal and SLTT government partners, to enable more coordinated preparedness and response to cyber and physical threats and natural disasters. The office enhances the Department’s ability to dedicate and focus attention on DOE’s SSA

responsibilities and will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners, as well as the overall critical infrastructure response framework overseen by DHS.

The CESER office plays an active role in coordinating government and industry efforts to address energy sector threats. The office is currently composed of two divisions: Infrastructure Security and Energy Restoration and Cybersecurity for Energy Delivery Systems.

DOE's Roles and Responsibilities for Energy Sector Cybersecurity

In preparation for, and in response to, cybersecurity incidents, the Federal Government's operational framework is provided by Presidential Policy Directive-41 (PPD-41). A primary purpose of PPD-41 is to clarify the roles and responsibilities of the Federal Government during a "significant cyber incident," which is described as one that is "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."

Under the PPD-41 framework, DOE works in collaboration with other agencies and private sector organizations, including the Federal Government's designated lead agencies for coordinating the response to significant cyber incidents: the DHS, acting through the National Cybersecurity and Communications Integration Center (NCCIC), and the Department of Justice (DOJ), acting through the Federal Bureau of Investigation (FBI) and its National Cyber Investigative Joint Task Force, as well as other agencies and private sector organizations. In the event of a significant cyber incident in the energy sector, DHS and DOJ coordinates with DOE to ensure its deep expertise with the sector is appropriately leveraged.

DOE is also working with the Tri-Sector Executive Working Group (TEWG) in conjunction with Department of Treasury and DHS along with our industry partners in order to address and manage risks across the energy, telecommunications, and financial sectors. The formation of the TEWG was recommended by the President's National Infrastructure Advisory Council (NIAC) in their August 2017 report titled, "Securing Cyber Assets: Addressing Urgent Cyber to Critical Infrastructure."

In the energy sector, the core of critical infrastructure partners are represented by the Electricity Subsector Coordinating Council (ESCC), the Oil and Natural Gas Subsector Coordinating Council (ONG SCC), and the Energy Government Coordinating Council (EGCC). The ESCC and ONG SCC represent the interests of their respective industries. The EGCC, led by DOE and DHS, is where the interagency partners, States, and international partners come together to discuss the important security and resilience issues for the energy sector. This forum ensures we are working together in a whole-of-government response.

The SCCs, EGCC, and associated working groups operate under DHS's Critical Infrastructure Partnership Advisory Council (CIPAC) framework, which provides a mechanism for industry and government coordination. The public-private critical infrastructure community engages in open dialogue to mitigate critical infrastructure vulnerabilities and to help reduce impacts from threats.

DOE's Cybersecurity Activities for the Energy Sector

DOE plays a critical role in supporting energy sector cybersecurity by enhancing the security and resilience of the Nation's critical energy infrastructure. To address these challenges, it is critical for us to be proactive and cultivate a secure energy network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover.

The Department is focusing cyber support efforts to strengthen energy sector cybersecurity preparedness, coordinate cyber incident response and recovery, and accelerate game-changing research, development, and deployment (RD&D) of resilient energy delivery systems.

Strengthening Energy Cybersecurity Preparedness

It is necessary for partners in the energy sector and the government to share meaningful and timely emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyberattacks more rapidly. An example of this type of collaboration is the Cybersecurity Risk Information Sharing Program (CRISP), a voluntary public-private partnership that is primarily funded by industry, administered by the Electricity Information Sharing and Analysis Center (E-ISAC), and enhanced by DOE through intelligence analysis by DOE's Office of Intelligence and Counterintelligence, as well as the broader U.S. intelligence community.

Current CRISP participants provide power to more than 75 percent of continental United States electricity customers. CRISP has clearly demonstrated that continuous monitoring of critical networks and shared situational awareness is of utmost importance in protecting against malicious cyber activities. Programs such as CRISP are critical for facilitating the identification of, and response to, advanced persistent threats targeting the energy sector.

The CRISP program is an example of how DOE, as the Sector-Specific Agency for energy, integrates additional efforts, including information from other public-private cybersecurity programs, such as DHS's Automated Indicator Sharing (AIS). The AIS program also allows for the bidirectional sharing of observed cyber threat indicators amongst DHS and participating companies. Those cyber threat indicators are incorporated into the CRISP analytics.

Advancing the ability to improve situational awareness of Operational Technology (OT) networks is a key focus of DOE's current activities. The Department is currently taking the lessons learned from CRISP and developing an analogous capability to monitor traffic on OT networks via the Cybersecurity for the Operational Technology Environment (CyOTE) pilot project. Observing anomalous traffic on networks can be the first step in stopping an attack in its early stages.

Cybersecurity vulnerabilities of key control systems and operational technology are an increasing concern for the Nation's critical energy infrastructure owners and operators. The Cyber Testing for Resilience of the Industrial Control Systems (CyTRICS) program will serve as a central capability for DOE's efforts to increase energy sector cybersecurity and reliability through testing and enumeration of critical electrical components. Further, analysis of test results will identify both systemic and supply chain risks and vulnerabilities to the sector by

correlating collected test data and enriching it with other data sources and methods. Through CyTRICS, DOE will collaborate with government, National Laboratories, and industry to identify key energy sector industrial control systems components and apply a targeted, prioritized, and collaborative approach to these efforts.

DOE is also establishing the Clean Energy Manufacturing Innovation Institute: Cybersecurity in Energy Efficient Manufacturing, led by the Office of Energy Efficiency and Renewable Energy in collaboration with CESER, to enhance the cybersecurity of energy-efficient manufacturing processes and accelerate the adoption of these technologies in the marketplace. The Institute will focus on cybersecurity in manufacturing, including understanding the evolving cybersecurity threats to greater energy efficiency in manufacturing industries, developing new cybersecurity technologies and methods, and sharing information and expertise with the broader community of U.S. manufacturers. The initiative will develop and leverage innovative solutions in two technical areas, securing automation and securing the supply chain, in order to address current and future challenges.

Facilitating Cyber Incident Response and Recovery

As the Energy SSA, DOE works at many levels of the electricity, petroleum, and natural gas industries. We interact with numerous stakeholders and industry partners to share both classified and unclassified information, discuss coordination mechanisms, and promote scientific and technological innovation to support energy security and reliability. By partnering through working groups between government and industry at the national, regional, state, and local levels, DOE facilitates enhanced cybersecurity preparedness.

Last year, DOE and the National Association of Regulatory Utility Commissioners (NARUC) released the third edition of a cybersecurity primer for regulatory utility commissioners. The updated primer provides best practices, access to industry and national standards, and clearly written reference materials for state commissions in their engagements with utilities to ensure their systems are secure from cyber threats. This document is publicly available on the NARUC website, benefitting not only regulators, but other State officials as well.

We are continuing to work with NARUC to support regional trainings on cybersecurity, with the goal of building commission expertise on cybersecurity, so they ensure cyber investments are both secure and economically viable.

DOE also continues to work closely with our public and private partners with the goal of fully supporting and bolstering the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the Sector Coordinating Councils (SCCs) to synchronize government and industry cyber incident response playbooks.

CESER engages directly with our government and industry partners to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. The 2018 iteration of DOE's cybersecurity-focused exercise, Liberty Eclipse, included two phases. Phase I was a tabletop exercise focusing on the roles, responsibilities, and authorities, of Federal, State, and energy industry partners in response to a significant cyberattack on energy infrastructure. Phase II included a seven-day operations-based exercise conducted on Plum Island in New York.

During Phase II, DOE worked with the Defense Advanced Research Projects Agency (DARPA), who tested and evaluated technologies that could enable the blackstart recovery of the power grid during a cyberattack in an isolated and controlled environment with first responders and power engineers on hand.

In 2017, DOE participated in Clear Path V, an annual exercise led by the North American Electric Reliability Corporation (NERC) that was designed to simulate a cyber and physical attack on electric and other critical infrastructures across North America. Clear Path V, which took place in Houston, Texas, focused on the cross-sector response to a hurricane impacting the Gulf Coast, with particular attention to the interdependencies of the electricity, oil and natural gas, and communications sectors. This exercise was cited by participants from multiple sectors as crucial to preparing for a nearly-identical real-world event only a few months later Hurricane Harvey. This and other similar large scale exercises continue to highlight the interdependencies between our Nation's energy infrastructure and other sectors.

DOE's most recent exercise, Clear Path VI, took place near Washington, D.C., in May 2018. Clear Path VI built on the successful implementation of the regionally-focused Clear Path IV exercise, and addressed the desire to conduct more issue-focused exercises that explore coordination between industry, State, and Federal partners in managing interdependencies within and between infrastructure sectors. This iteration focused on the challenges that the sector may face during a major hurricane impacting the mid-Atlantic region.

Clear Path VII, scheduled for May 2019, will return to examining the impacts of a catastrophic earthquake, this time focusing on the New Madrid Seismic Zone. As a result of the lessons-learned identified from Clear Path IV, improvements have been implemented regarding the Department's response communications and coordination structures.

It is critical that the results of the exercises inform our response plans on a continuous basis to close identified gaps in coordination with our industry and government partners through the associated coordinating councils. Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinating various efforts showcased in the exercise, including unity of messaging required to recover from a real-life version of the exercise scenario.

In preparation for any future grid security emergency, it is critical that we continue working with our government and industry partners to further shape the types of orders that may be executed under current authorities, while also clarifying how we communicate and coordinate the operational implementation of these orders. Continued coordination with Federal, SLTT, and industry partners and participation in preparedness activities like Liberty Eclipse enable DOE to identify gaps and develop capabilities to support cyber response.

Accelerating Breakthrough RD&D of Resilient Energy Delivery Systems

Cybersecurity for energy control and OT systems is vastly different from typical IT systems. OT power systems must operate continuously with high reliability and availability. Upgrades and patches can be difficult and time consuming, with components dispersed over wide geographic regions. Further, many assets are in publicly accessible areas where they can be subject to

physical tampering. Real-time operations are imperative and latency is unacceptable for many applications. Immediate emergency response capability is mandatory and active scanning of the network can often be difficult.

CESER's Cybersecurity for Energy Delivery Systems (CEDs) R&D program is designed to assist energy sector asset owners by developing cybersecurity solutions for energy delivery systems through a focused, early-stage research and development effort. CESER co-funds industry-led, National Laboratory-led, and university-led projects with SLTT and industry partners to make advances in cybersecurity capabilities for energy delivery systems. These research partnerships are helping to detect, prevent, and mitigate the consequences of a cyber incident for our present and future energy delivery systems. In a demonstration of our coordination with other federal agencies, two of the university-led collaborations are funded in partnership with DHS Science and Technology.

To select cybersecurity R&D projects, DOE constantly examines the threat landscape and coordinates with partners, like DHS, to provide the most value to the energy sector while minimizing overlap with existing projects. For example, the Artificial Diversity and Defense Security (ADDSec) project will develop solutions to protect control system networks by constantly changing a network's virtual configuration, much like military communications systems that rapidly change frequencies to avoid interception and jamming. As a result, ADDSec can harden networks against the mapping and reconnaissance activities that are the typical precursors to a cyberattack.

Another project, the Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks (CODEF), is designed to anticipate the impact a command will have on a control system environment. If any commands would result in damage to the system or have other negative consequences, CODEF will have the ability to prevent their execution. This type of solution is especially intriguing as it can detect malicious activity regardless of the source, be it an insider threat or an external actor.

The Energy Sector Security Appliances in a System for Intelligent Learning Network Configuration Management and Monitoring project, otherwise known as *Essence*, is a CEDs-funded endeavor involving the National Rural Electric Cooperative Association (NRECA). *Essence* started as a concept to build a system that passively monitors all network traffic within an electric utility, and to use machine learning to develop a model of what "normal" is, so that deviations indicative of cyber compromise could be detected instantly and acted on quickly. The envisioned system was built and successfully demonstrated in the first project. Work since then has focused on extending a solid technical prototype into commercially deployable products with solid, committed technical partners with an established presence in the utility market. To date, NRECA has engaged with four partners to offer commercial products based on *Essence*.

DOE is also working in conjunction with NRECA and the American Public Power Association (APPA) to help further enhance the culture of security within their utility members' organizations. With more than a quarter of the Nation's electricity customers served by municipal public power providers and rural electric cooperatives, it is critical that they have the tools and resources needed to address security challenges. To address risks and manage the risks to an acceptable level, APPA and NRECA are developing security tools, educational resources,

updated guidelines, and training on common strategies that can be used by their members to improve their cyber and physical security postures. Exercises, utility site assessments, and a comprehensive range of information sharing with their members will all be used to bolster their security capabilities.

Strengthening our Workforce Development

The final area I would like to highlight is one that is truly foundational in nature, cybersecurity workforce development. It is also a national priority outlined in the President's National Cyber Strategy. Through our SLTT workforce development efforts with state organizations like the National Association of State Energy Officials (NASEO), we are developing a multifaceted approach including online trainings, playbooks, workshops, and guidance to build capacity throughout the sector and guarantee that the State energy officials that we engage with regularly have the necessary and current skills and resources needed to prepare for and respond to energy disruptions of significance, including cyber emergencies.

DOE is also continuing and expanding our annual collegiate-level cyber defense competition. In 2018, DOE held two competitions to help develop the next generation of cybersecurity professionals to help secure our Nation's critical energy infrastructure. DOE's third Cyber Defense Competition (CDC) took place in April, with 25 college and university teams competing at three National Laboratories. DOE's 2018 CyberForce Competition™ followed in late November-December, with 64 college and university teams from 24 states and Puerto Rico competing at seven National Laboratories across the Nation.

Conclusion

Establishing CESER is the result of the Administration's commitment to and prioritization of energy security and national security. Our long-term approach strengthens our national security and positively impacts our economy. As CESER moves forward, we are taking the first steps in the transformational change necessary to achieve the Secretary's priority of emergency preparedness and rapid, coordinated response to disruptions in the energy sector.

I appreciate the opportunity to appear before this Committee to discuss cybersecurity in the energy sector, and I applaud your leadership. I look forward to working with you and your respective staffs to continue to address cyber and physical security challenges.

The CHAIRMAN. Thank you, Assistant Secretary.
Major Keber, welcome to the Committee.

STATEMENT OF MAJOR WILLIAM J. KEBER, EXECUTIVE OFFICER, WEST VIRGINIA NATIONAL GUARD'S CRITICAL INFRASTRUCTURE PROTECTION BATTALION

Major KEBER. Good morning, Chairman Murkowski, Ranking Member Manchin, and members of the Committee. Thank you for the invitation and opportunity to participate in today's hearing on the Status and Outlook for Cybersecurity Efforts in the Energy Industry.

My name is Major William Keber. I'm the Executive Officer for the West Virginia National Guard's Critical Infrastructure Protection Battalion, currently serving in a Title 32 status. Our organization is a distinctive one that conducts assessments and training to improve the security and operation of our nation's critical infrastructure.

Since 2005, we have conducted infrastructure protection assessments and training events for the Department of Energy, Department of Transportation, Defense Industrial Base, the Department of Homeland Security and the Department of Defense. To date, our teams have conducted over 3,500 assessments and 2,600 training events, educating over 59,000 individuals. We have conducted assessments in support of national events such as the State of the Union, Republican and Democratic National Conventions, the National and World Scout Jamborees and the Superbowl.

The West Virginia National Guard CIP Battalion has a diversified portfolio that currently supports DHS, Department of the Army and the United States Coast Guard. We support DHS' cybersecurity infrastructure security agency with training, assessment support and infrastructure image captures. We support the U.S. Coast Guard by conducting their port security and resiliency assessments and the Department of Army by conducting mission assurance assessments and training.

The CIP Battalion has always assessed networks and communication architectures against cybersecurity concepts and principles but never had the authorities to conduct deep analysis on the network. Assessment teams were relegated to questioning site representatives through interviews and annotating their physical observations. Recent Congressional legislation has opened the doors to evaluate cybersecurity and thereby allowing us to expand our capabilities and methodologies.

The West Virginia National Guard has developed a relationship with the cybersecurity branch at NASA's Independent Verification and Validation Office. Members of this team have years of experience conducting blue and red team cyber assessments against some of our nation's most complex technical architectures. The collaborative sharing of best practices has significantly enhanced our organization's assessment teams.

We are currently working in conjunction with a cybersecurity community of interest that includes Army cyber, NASA, Idaho National Labs, the National Security Agency, the Threat Systems Management Office, the Navy and the U.S. Army Corps of Engi-

neers to formalize our approach and bring together the best practices from each of these organizations.

We are working to develop a comprehensive approach and methodology for our cyber assessments. We will cover key cyber infrastructure areas such as the perimeter, networks and points applications, control systems and especially the policies and procedures to govern them. We plan to conduct network architecture reviews, traffic analysis, policy and procedure document review, access control evaluation and wireless vulnerability assessments.

Most importantly, we are striving to replicate these systems in a lab environment to research potential vulnerabilities, determine possible attack vectors, test resiliency, identify systemic concerns and evaluate impacts in a safe manner. We will document our findings and incorporate risk mitigation recommendations into the Army's preexisting remediation processes.

The West Virginia National Guard and the regular Army have contributed to enhancing workforce development by sending team members to specialized training. The West Virginia National Guard has organized cybersecurity training in partnership with the University of Charleston.

Additionally, we have utilized our access to a decommissioned power plant in West Virginia. We utilize this facility to give trainees the opportunities to see firsthand the vast systems involved with industrial systems and power generation.

Our Army partners have organized training at Idaho National Labs, SANS and other Army training opportunities. The CIP Battalion team's citizen soldiers have unique professional experiences providing distinct benefits. We have engineers, master electricians and network administrators that have decades of industrial experience. They can serve on an active status with us or in traditional reserve status, later returning to industry providing valuable skills and knowledge.

To summarize, the West Virginia National Guard CIP Battalion is uniquely positioned to provide the Department of Defense and other related sectors insight and assistance pertaining to infrastructure protection and cybersecurity. We will continue to move forward with our efforts to expand our cybersecurity activities and help more organizations secure this great nation of ours.

Thank you again for this opportunity to discuss our efforts to enhance cybersecurity within the West Virginia National Guard at today's hearing.

[The prepared statement of Major Keber follows:]

**United States Senate Committee on Energy and Natural Resources
Hearing to Consider the Status and Outlook for Cybersecurity Efforts in the Energy Industry**

February 14, 2019

**Testimony of Major William J. Keber
Executive Officer, West Virginia National Guard's Critical Infrastructure Protection Battalion**

Good morning, Chairman Murkowski, Ranking Member Manchin, and members of the Committee on Energy and Natural Resources, thank you for the invitation and opportunity to participate in today's hearing on the Status and Outlook for Cybersecurity Efforts in the Energy Industry.

My name is Major William Keber, and I am the Executive Officer for the West Virginia National Guard's Critical Infrastructure Protection (CIP) Battalion. Our organization is a distinctive one that conducts assessments and training to improve the security and operation of our nation's critical infrastructure. Our unit started in 2005 when Major General James A. Hoyer, then a Lieutenant Colonel, presented a concept to West Virginia National Guard leadership proposing assessment activities to support homeland defense. Over the past fourteen years we have conducted infrastructure protection assessments and training events for the Department of Energy, Department of Transportation, the Defense Industrial Base, the Department of Homeland Security, and the Department of Defense. Since inception, our teams have conducted 3,583 assessments and 2,662 training events, educating 59,237 individuals as of January 2019. We have conducted assessments in support of national events such as the State of the Union, Republican and Democratic National Conventions, the National and World Scout Jamborees, Presidential visits, and the Superbowl, just to name a few.

In this testimony I will address three topics. First, I will cover how our organization historically contributed to protecting our nation's infrastructure and assessed cybersecurity. Second, I will describe the current steps we are taking to further enhance cybersecurity assessment practices. Third, I will discuss how we are contributing to workforce development and contributing to the broader defense industry along with other interdependent industries.

I. History of WVNG's Critical Infrastructure Protection Assessments

The West Virginia National Guard's CIP Battalion has a diversified portfolio that currently supports the Department of Homeland Security, Department of the Army, and United States Coast Guard. Additionally, we are in discussions with the Department of the Navy and the Nuclear Regulatory Commission to collaborate on future physical security and cybersecurity projects.

We support DHS's Cybersecurity Infrastructure Security Agency by creating Infrastructure Visualization Platform products, assisting facilities self-assess utilizing DHS's Infrastructure Survey Tool, conducting training for the Office for Bombing Prevention, and assisting its Regional Resiliency Assessment Program by assessing natural gas and petroleum pipelines. We support the U.S. Coast Guard by conducting Port Security and Resiliency Assessments and the Department of the Army by conducting Mission Assurance Assessments and training. Both Coast Guard and Army teams reference DoD Mission Assurance Benchmarks and assess risk with an all threats, all hazards approach.

Our teams have always assessed networks and communications architectures against cybersecurity concepts and principles, but never had the authorities to conduct deep analysis on the network to validate the information given. Assessment team members were relegated to questioning site representatives through interviews and annotating their physical observations. Recent Congressional legislation has opened the doors to evaluate cybersecurity, thereby allowing us to expand our capabilities and methodologies.

Testimony of Major William J. Keber
Executive Officer, West Virginia National Guard's Critical Infrastructure Protection Battalion

II. Current Status to Evolve Assessments and enhance Cybersecurity

The National Defense Authorization Act of 2017, Section 1650 directed the Department of Defense to evaluate cyber vulnerabilities within its critical infrastructure. Integrating upon other efforts, the Office of the Secretary of Defense decided to include this within its preexisting Mission Assurance construct. This was a natural fit because cybersecurity is one of the 17 programs that Mission Assurance Assessments evaluate.

The West Virginia National Guard has developed a relationship with the Cybersecurity Branch at the National Aeronautics and Space Administration's (NASA) Independent Verification and Validation (IV&V) in Fairmont, West Virginia. Members of this team have years of experience conducting blue and red team cyber assessments against some of our nation's most complex and sensitive technological architectures. Both organizations have a common objective and that is to ensure mission success for our respective organizations. The collaborative sharing of best practices has significantly enhanced both organizations' assessment teams.

We are currently working in conjunction with a cybersecurity community of interest that includes Army Cyber, NASA, Idaho National Labs, the National Security Agency, the Threat Systems Management Office, the Navy, and the U.S. Army Corps of Engineers to formalize our approach and bring together the best practices from each of these organizations.

We are working to develop a comprehensive approach and methodology for our cyber assessments. We will cover key cyber infrastructure areas such as the perimeter, networks, endpoints, applications, control systems, and the policies and procedures that govern them. We plan to conduct network architecture reviews, traffic analysis either live or offline, policy and procedure document review, access control evaluation, and wireless vulnerability assessments. Most importantly, we are striving to replicate these systems in a lab environment to research potential vulnerabilities, determine possible attack vectors, test resiliency, identify systemic concerns, and evaluate the impacts in a safe manner. We will document and report our findings and incorporate recommendations for risk mitigation into the Army's preexisting remediation processes.

III. Workforce Development and Benefits for the Cybersecurity and Energy Communities

In the last six months Army Cyber and the West Virginia National Guard have contributed to enhancing workforce development by sending team members to specialized training. The West Virginia National Guard has organized cybersecurity training in partnership with the University of Charleston in Charleston, West Virginia conducting Certified Ethical Hacker and Certified Incident Handler courses. Additionally, the WVNG has access to a decommissioned coal power plant. We use this facility to give trainees the opportunity to see firsthand the vast systems involved with Industrial Control Systems and power generation.

Our partners at Army Cyber have organized training at Idaho National Labs, SANS, and through internal training organizations. Courses include Industrial Control System training, Army Penetration Testing Course; Communications Security Course, and SANS courses such as ICS/SCADA Security Essentials, Essentials for NERC CIP, and ICS Active Defense and Incident Response.

Our teams have the unique experience not found in other organizations and can provide future benefits to the Defense and Energy industries. For instance, we have Engineers, Master Electricians, and Network Administrators that have been working in the energy and industrial sectors for decades. These unique

Testimony of Major William J. Keber
Executive Officer, West Virginia National Guard's Critical Infrastructure Protection Battalion

citizen soldiers can actively serve in uniform for a period of time and later return to industry providing valuable skills and knowledge they acquired.

To summarize, the West Virginia National Guard's Critical Infrastructure Protection Battalion is uniquely positioned to provide the Department of Defense and other related sectors insight and assistance pertaining to infrastructure protection and cybersecurity for industrial and interconnected systems. We will continue to move forward in our efforts to expand our cybersecurity activities and help more organizations secure this great nation of ours.

Thank you again for the opportunity to discuss our efforts to enhance cybersecurity within the West Virginia National Guard at today's hearing.

The CHAIRMAN. Thank you, Major.
Welcome, Mr. Robb.

**STATEMENT OF JAMES B. ROBB, PRESIDENT AND CHIEF
EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELI-
ABILITY CORPORATION**

Mr. ROBB. Good morning, Chairman Murkowski, Ranking Member Manchin and members of the Committee. This is my first appearance before the Committee as NERC's CEO, and I appreciate the invitation very much to discuss the status and outlook for cybersecurity in the electricity sector.

As you pointed out in your opening comments, Chairman, electricity supports every aspect of our way of life and well-being. While to date there's been no successful cyberattack that's resulted in any loss of load in the United States, the threats are very real and the potential consequences severe.

While all sectors of the economy are increasingly targets for data theft, ransomware and other criminal activity, the electricity sector, in particular, has taken the cyber threat very seriously and has put in place a robust system to provide protection for critical infrastructure. We find that boards and executive leadership provide very strong support and focus and set cybersecurity as a top priority for their organizations.

In recent years we've seen an increase in the sophistication and frequency of cyber threats. The major threats include phishing, malware, physical attacks and theft. Spear phishing, in particular, with credential harvesting objectives is one of the most common attacks because it's proven to be so effective and relatively easy to execute.

Nation states and terrorist groups are persistent threats, a reminder that security requires constant vigilance.

NERC and our work employs a three-pronged approach to support the security of the bulk power system. Our approach includes mandatory and enforceable standards, as Chairman Chatterjee mentioned earlier, information sharing and partnerships. Together they form a solid foundation of best practices and strategies necessary to effectively confront this ever-evolving threat.

NERC's mandatory critical infrastructure protection standards provide a common foundation for security. Our standards are developed using subject matter expertise from industry through a FERC-approved process and then reviewed and approved by NERC's independent board of trustees and then by the FERC.

The CIP standards require companies to establish plans, protocols and controls that protect their critical systems against cyberattack, ensure the personnel are adequately trained on cyber hygiene, timely report security incidents to us and then be able to recover from events.

Electricity is the only critical infrastructure with mandatory cyber standards. Compliance with those standards is routinely audited and non-compliance is subject to financial penalty.

However, while critical to the security equation, standards alone are clearly insufficient. The emerging dynamic nature of malicious cyber threats requires constant situational awareness, real-time communications that are effective and prompt emergency response

capabilities. That's where information sharing comes in. NERC's Electricity Information Sharing and Analysis Center, or the E-ISAC, provides these services and supports industry cyber defense. Operated by NERC, but working in collaboration with DOE and the Electricity Subsector Coordinating Council, the E-ISAC is the central hub for the sharing of security information within the electricity sector. The E-ISAC communicates with over 1,000 electric industry organizations via a secure portal with critical security information that is provided both by industry and government. We conduct periodic webinars and critical broadcast calls to rapidly communicate key insights and threats to industry.

For the most serious of threats, NERC alerts are used to provide concise, actionable security information and mitigation strategies to industry. NERC alerts are divided into three levels and can require companies to positively affirm back to us that they have successfully mitigated the threat. Since 2009, we've issued 46 security-related alerts, 41 of those were cyber-related.

Partnerships, however, form the third plank for security and the preeminent partnership in the electricity sector is something we call the CRISP Program, the Cyber Risk Information Sharing Program. Conceived by the DOE and managed by the E-ISAC, CRISP uses innovative technology developed by the Department of Energy and the national laboratory system to monitor cyber activity on company systems.

CRISP companies currently cover approximately 75 percent of the meters in the United States and we are working to further expand that program. Indicators and threat actor information captured by CRISP is then shared to the entire E-ISAC membership base. So it's shared beyond the direct participants in CRISP so that everyone can benefit from those insights.

Another key partnership is NERC's GridEx exercise. GridEx is the largest geographically distributed security exercise for the electricity sector. It's conducted every other year and simulates a widespread, coordinated physical and cyberattack designed to overwhelm even the most prepared of organizations. In 2017, 6,500 individuals and 450 organizations participated in GridEx IV, and we'll be launching GridEx V this November on November 13th and 14th.

Looking ahead, however, there are many challenges for us to address and those include strengthening cross sector partnerships to facilitate better information sharing and coordination between critical infrastructure segments, developing more advanced and nimble tools to stay ahead of adversaries, securing electronic devices that are connected behind the meter, expanding the declassification and dissemination of critical information and developing a strong cyber-aware and cyber-capable workforce.

Thank you again for the opportunity to discuss NERC's responsibilities for cybersecurity, and I look forward to questions.

[The prepared statement of Mr. Robb follows:]

**Testimony of James B. Robb, President and Chief Executive Officer
North American Electric Reliability Corporation**

**Before the Senate Committee on Energy and Natural Resources
“Status and Outlook for Cybersecurity Efforts in the Energy Industry”**

February 14, 2019

Introduction

Good morning Chairman Murkowski, Ranking Member Manchin, members of the committee and fellow panelists. My name is Jim Robb and I am the President and CEO of the North American Electric Reliability Corporation (NERC). NERC’s mission, as the Electric Reliability Organization (ERO) certified by the Federal Energy Regulatory Commission (FERC), is to assure the reliability and security of the bulk power system (BPS) in North America. The threat of cyber attacks by nation states, terrorist groups, and criminals is at an all-time high. Now more than ever, grid security is inextricably linked to reliability. The North American BPS is among the nation’s most critical infrastructures. Virtually every critical sector depends upon electricity. The BPS is also one of the largest, most complex systems ever created. It is robust and highly reliable. Nevertheless, conventional and non-conventional factors do present risks to the BPS.

I have been at NERC for nine months and prior to NERC served as the CEO of WECC, the Western Electricity Coordinating Council, one of seven regions in the reliability enterprise. I have more than 30 years of experience working with the electricity industry and am pleased to speak with you today about NERC’s responsibilities for grid security.

Summary

The security landscape is dynamic, requiring constant vigilance and agility. NERC assures grid security through a comprehensive series of complementary strategies involving mandatory standards, information sharing, and partnerships. NERC’s mandatory critical infrastructure protection standards (CIP standards) are a foundation for security practices. They provide universal, baseline protections. Due to the ever-evolving nature of cyber threats, security cannot be achieved through standards alone. Vigilance also requires the agility to respond to new and rapidly changing events. Accordingly, NERC’s Electricity Information Sharing and Analysis Center (E-ISAC) serves as the information sharing conduit both within the North American electricity industry and between the electricity industry and government for cyber and physical security threats. The E-ISAC facilitates communication of important or actionable information, and strives to determine and maintain “ground truth” during rapidly evolving security events. The E-ISAC also plays a key role in cross-sector coordination, focusing on sectors with which electricity has interdependencies, such as natural gas, water, and other critical infrastructure. Mandatory standards, coupled with effective mechanisms to share information, provide robust and flexible tools to protect the BPS. NERC works closely with the Department of Energy (DOE), Department of Homeland Security (DHS), FERC, and the Electricity Subsector Coordinating Council (ESCC) to further the public-private partnership so important to addressing security. NERC’s biennial GridEx exercise is the largest of its kind in the sector and helps industry and government exercise their emergency response plans, and drive new and innovative approaches to reduce security risk to the electric grid.

About NERC

NERC is a private non-profit corporation that was founded in 1968 to develop voluntary operating and planning standards for the users, owners and operators of the North American BPS. Pursuant to Section 215 of the Federal Power Act (FPA) (16 U.S.C. §824o) and the criteria included in Order No. 672 for designating an Electric Reliability Organization (ERO), FERC certified NERC as the ERO for the United States on July 20, 2006. On March 16, 2007, FERC issued Order No. 693 which approved the initial set of reliability standards. These reliability standards became mandatory in the United States on June 18, 2007.

NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC performs a critical role in real-time situational awareness and information sharing to protect the electricity industry's critical infrastructure against threats to the BPS. NERC's area of responsibility spans the continental United States, Canada, and Mexico. Our jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

Critical Infrastructure Protection Standards

With oversight from FERC, NERC is responsible for developing and enforcing mandatory reliability standards for the BPS. The CIP standards provide a common, universal foundation for security. They are robust and comprehensive, covering a wide range of priorities and threat vectors.

More than a decade ago, Congress had the foresight to anticipate the emerging risk posed by cyber security threats to the BPS by defining reliability standards to include "cybersecurity protection." NERC's CIP standards are developed by registered entities through an open, transparent stakeholder process, subject to approval by NERC's Board of Trustees and FERC. In addition, FERC can order NERC to develop a standard and has done so on topics such as geomagnetic disturbances, physical security, and supply chain cyber security risk management.

The CIP standards group includes the following 12 topics addressing cyber and physical security:¹

CIP-002 – Cyber System Identification and Categorization requires entities to identify their cyber systems that perform reliability functions and must be protected under the CIP standards. Using bright-line criteria, this standard also requires entities to categorize these systems as "high," "medium," or "low" impact based on the risk to the BPS if the system were compromised. This categorization forms the basis for determining the level of controls applied to those systems under the applicable CIP standards.

CIP-003 – Security Management Controls and Requirements for Lower Risk Cyber Systems requires entities to adopt and maintain cyber security policies to establish responsibility and accountability for protecting critical cyber systems. This standard also identifies the security controls for those systems identified as low impact focusing on: cyber security awareness;

¹ To view NERC CIP standards, see <http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United%20States>.

physical access controls; electronic access controls; cyber security incident response; and protections for transient electronic devices (e.g., thumb drives, laptop computers).

CIP-004 – Personnel and Training establishes rules for authorizing personnel, including contractors and service vendors, for electronic or unescorted physical access to high- and medium-impact cyber systems. It also establishes rules for ensuring these personnel have the appropriate level of training and security awareness.

CIP-005 – Electronic Security Perimeters establishes rules for managing electronic access to high and medium impact cyber systems through use of electronic security perimeters that delineate a “trust zone.” This standard also establishes rules for remote access to these cyber systems.

CIP-006 – Physical Security of Cyber Systems establishes rules for managing physical access to high- and medium-impact cyber systems.

CIP-007 – Systems Security Management addresses system security by specifying technical, operational, and procedural requirements in support of protecting high- and medium-impact cyber systems.

CIP-008 – Incident Reporting and Response Planning specifies incident reporting and response requirements.

CIP-009 – Recovery Plans specifies recovery plan requirements to help ensure that reliability functions are recovered following a cyber security incident.

CIP-010 – Change Management and Vulnerability Assessments specifies system configuration management and vulnerability assessment requirements to help prevent and detect unauthorized changes to high- and medium-impact cyber systems.

CIP-011 – Information Protection establishes rules to prevent unauthorized access to cyber system information by specifying information protection requirements.

CIP-013 – Cyber Security Supply Chain Management will require entities to develop and implement a plan to address supply chain cyber security risks during the planning and procurement of industrial control system hardware, software, and services. This standard was approved by FERC on October 18, 2018, and will become effective on July 1, 2020. This standard was approved by FERC on October 18, 2018, and will become effective on July 1, 2020.

CIP-014 – Physical Security of Critical Transmission Substations and Associated Control Centers that pose the greatest risk to reliability if they are damaged or rendered inoperable due to physical attack. The standard requires entities to determine what facilities are critical, assess the physical security threats to and vulnerability of those critical facilities, and implement a plan to mitigate those threats and vulnerabilities.

As experience and technology continue to grow, NERC, with FERC oversight, continues to refine and improve the CIP standards to help ensure their effectiveness and timeliness. For example, pending before FERC is a new CIP standard, CIP-012, that would require enhanced protections of sensitive data transmitted between critical control centers. Additionally, at its February 2019 meeting, the NERC Board of Trustees adopted revisions to CIP-008 to enhance reporting of cybersecurity incidents. This revised standard will be filed for FERC approval in the near future. NERC is also currently working with industry experts to consider modifications to the CIP standards to better account for technological innovation.

Electricity Information Sharing and Analysis Center

NERC's CIP standards provide a universal foundation for security practices. Yet security cannot be achieved through these standards alone. Because of the emerging and dynamic nature of malicious cyber threats, reliability assurance also requires constant situational awareness, real time communication, and prompt emergency response capabilities. The E-ISAC provides these services and supports these industry capabilities.

The mission of the E-ISAC is to reduce cyber and physical security risk to the electricity industry across North America by providing unique insights, leadership, and collaboration. It accomplishes this mission by sharing trusted information and analysis in a timely, credible, actionable manner with asset owners and operators across the continent.

Operated by NERC, and working in collaboration with the DOE and the ESCC, the E-ISAC is the central information sharing hub for the electricity sector. The E-ISAC uses a secure portal as the primary means for communicating with its more than 1,025 electricity industry member organizations, and the number continues to grow. The portal was revamped in 2017 and is constantly undergoing further upgrades to enhance the user experience. The new portal functions, plus greater outreach with key industry stakeholder groups through our Industry Engagement Program (IEP), has improved bi-directional information sharing and allows members greater access to more information.

E-ISAC services enable industry to defend against and respond to cyber and physical security threats, vulnerabilities, and incidents through the exchange of timely, actionable information. In addition to coordination with DOE and FERC's Office of Infrastructure Security, the E-ISAC promotes cross-sector coordination through work with the DHS and other agencies and ISACs. In particular, to further enhance cross-sector collaboration in light of electric and natural gas interdependencies, the E-ISAC continues to expand its partnership with the Downstream Natural Gas ISAC (DNG-ISAC). In the past year, the E-ISAC added additional partnerships with other interdependent sectors, including the Water-ISAC and the Multi-State ISAC with the goal providing electricity sector context to water and waste-water operators, as well as state and local governments. Security is a global priority, and because NERC is an international organization, the E-ISAC works with Natural Resources Canada, Public Safety Canada, and the recently established Canadian Centre for Cyber Security to provide cross-border outreach and collaboration. In October 2018, NERC announced a trilateral memorandum of understanding among the E-ISAC, the Japan Electricity ISAC and the European Energy ISAC with the intention of expanding sources of information and opportunities for analysis with partners who face similar adversarial threats. As the E-ISAC moves to 24/7 watch operations, these international

partnerships will provide valuable context and awareness of emerging threats for overnight analysts to share with North American grid operators

Cybersecurity Risk Information Sharing Program (CRISP)

Managed by the E-ISAC and in partnership with DOE, CRISP uses innovative technology and leverages DOE and its National Laboratory System's analytical capability. CRISP provides timely bi-directional sharing of unclassified and classified threat information and develops situational awareness tools to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure. CRISP companies cover more than 75 percent of U.S. customers. CRISP information is shared in a secure fashion through the E-ISAC portal, and allows non-CRISP member companies to benefit from the shared indicators and threat actor activity captured by the program. CRISP information also supports the development of situational awareness to enhance the industry's ability to identify, prioritize, and coordinate the protection of its critical infrastructure and key resources. In addition to CRISP, the E-ISAC is pursuing cyber automated information sharing systems as well as a malware analysis repository and threat information exchange to provide for more advanced information sharing capabilities.

NERC Alerts, Critical Broadcasts, and Briefings

In addition to the secure portal, the E-ISAC shares information through a number of forums to increase awareness of threats, and to recommend mitigation. When there is a significant security concern, NERC and the E-ISAC communicate with the electricity industry via two distinct platforms.

NERC alerts provide concise, actionable security information to the electricity industry. Security alerts communicate unclassified sensitive information and mitigation measures. Alerts are divided into three levels:

- **Level One – Industry Advisory:** Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- **Level Two – Recommendation to Industry:** Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the alert.
- **Level Three – Essential Action:** Identifies actions deemed to be "essential" to BPS reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the alert.

NERC determines the appropriate alert notification based on risk to the BPS. Generally, NERC distributes alerts broadly to users, owners, and operators of the North American BPS using its compliance registry. Entities registered with NERC are required to provide and maintain updated compliance and cyber security contacts. NERC also distributes the alerts beyond BPS users, owners, and operators to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g., balancing authorities, transmission operators, generation owners, etc.). Alerts are developed with the strong partnership of federal technical organizations, including FERC, DOE National Laboratories, DHS, and BPS subject matter experts. Since 2009, NERC has

issued 46 security-related alerts, 41 of which were cyber-related (41 Industry Advisories and 5 Recommendations to Industry). Those alerts covered items such as sabotage events, pandemic, Aurora, Night Dragon, and heightened awareness and reporting guidance of suspicious activity. In 2016, NERC issued two Level Two alerts – the first related to the 2015 cyber-attack in Ukraine and another concerning distributed denial of service attacks leveraging compromised Internet of Things² devices. Responses to alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders.

In addition to NERC alerts, the E-ISAC uses the Critical Broadcast Program (CBP). This program launched in 2018 to rapidly share information with members. The CBP capability is designed to rapidly disseminate critical security information to the electricity industry. The CBP leverages E-ISAC staff and stakeholder expertise to obtain and share the best available information and potential mitigation strategies to address developing security threats and events in a timely manner. The information is shared through the E-ISAC portal and other means, as necessary. The E-ISAC used this capability four times in 2018: on February 7, where 1,208 individuals joined the call; February with 2,960 individuals; November 29, with 524 participants; and December 20, where more than 1,284 individuals from the electricity and oil and natural gas subsectors joined the call.

The E-ISAC also hosts regular monthly threat briefings, unclassified threat workshops, classified forums for its members, and allows asset owners and operators to interact with our analysts and each other to share trend analysis and context on common threats to the electricity sector. In addition to the regularly hosted events, the E-ISAC conducted seven sessions of IEP in 2018, a three-day session where industry members visit the E-ISAC to see firsthand how the E-ISAC operates on a daily basis. These activities allow members to discuss emerging threats, learn from security experts, and provide feedback directly to the E-ISAC—which help improve E-ISAC's products and services.

GridEx

Consistent with our mission to promote a strong learning environment, NERC hosts an every other year grid security exercise – GridEx – which simulates widespread, coordinated cyber and physical attacks on critical electric infrastructure designed to overwhelm even the most prepared organizations. GridEx is the largest geographically distributed grid security exercise for the electricity sector. It consists of a two-day distributed play exercise and a separate executive tabletop session. GridEx allows participants to:

- Exercise crisis response and recovery;
- Improve communication;
- Identify lessons learned; and
- Engage senior leadership.

² The Internet of Things (IoT) refers to devices and sensors connected to the Internet such as security cameras, alarm systems, printers, or light switches. IoT devices typically use default passwords and are highly vulnerable to subversion by threat actors.

In 2017, 6,500 individuals and 450 organizations participated in GridEx IV, including industry, law enforcement, and government agencies. The executive tabletop included 42 participants from a cross-section of industry executives and senior officials from federal and state governments. Participating organizations are encouraged to identify their own lessons learned and share them with NERC. NERC uses this input to develop observations and propose recommendations to help the electricity industry enhance the security and reliability of North America's BPS. We are deep into planning for GridEx V which will be conducted on November 13-14, 2019.

GridSecCon

Consistent with promoting a learning environment and information exchange, NERC hosts the annual Grid Security Conference (GridSecCon). This widely attended conference brings together cyber and physical security experts from industry and government to share emerging security trends, policy advancements, and lessons learned related to the electricity industry. While the specific agenda varies from year to year, general objectives include:

- Promoting reliability of the BPS through training and industry education;
- Delivering cutting-edge discussions on security threats, vulnerabilities, and lessons learned from senior industry and government leaders; and
- Informing industry with discussions on security best practices, reliability concerns, risk mitigation, and cyber and physical security threat awareness.

Cyber Threats and Trends

These engagements and analytical capabilities have increased the E-ISAC's insight into threats to the grid. This greater insight has translated into more security products for industry, as well as more member-originated information submitted to the E-ISAC and more sharing. In 2018, more than 300 cyber bulletins and more than 200 physical bulletins were posted to the portal. The E-ISAC also posts bulletins based on information obtained from government partners and trusted open source partners, and we thank our government partners at DOE, DHS, and FBI for continuing to produce these valuable products.

Looking at the trend analysis of those bulletins, the major cyber and physical security trends of 2018 included: cryptojacking, phishing, malware, gunfire at electric infrastructure, and theft. From a cyber perspective, the threat constantly changes, and members must be vigilant, staying informed about adversaries' latest tactics, techniques, and procedures. While many physical security threats remain similar from year-to-year, the threat from activist groups continue to evolve as they become more capable.

In 2018, many familiar malware families such as Shamoon and GreyEnergy—the successor to BlackEnergy—saw new variants, while other frameworks like VPNFilter first appeared. In the case of VPNFilter, the E-ISAC leveraged its partnership with an industrial control system vendor to quickly dispel concerns regarding the Modbus module's capabilities. The threat, however, is clear: advanced attackers continue to develop highly modular tools with the ability to greatly impact a targeted system.

Cyber Security Threat Outlook

As the E-ISAC looks to the future, we anticipate certain trends:

Credential harvesting: Tactics to acquire legitimate user credentials to gain initial access to targeted networks and establish persistence mechanisms will continue to be popular because it helps evade detection. Sophisticated spear phishing activity to harvest credentials is the most common technique observed by members.

Exploitation of the trust relationship between targeted organizations and their business partners: Recent incidents have demonstrated that nation-state adversaries are targeting the electric sector and other industries by compromising the networks of third parties with which the intended targets have established business relationships. This tactic is a type of supply chain attack, and increases the success rate of tactics used to initially compromise the intended target.

Network device targeting: From the high profile reports on VPNFilter to the state-sponsored actors targeting network devices discussed in United States, switches and routes located on the edge of networks are a prime target for threat actors capable of intercepting and processing a large amount of information. Because these devices are placed at the boundary between internal networks and the internet, and exist to allow controlled access to the internal network, they will most likely continue to be a target of reconnaissance.

Use of native tools: Adversaries will likely continue to use tools and capabilities already present on a compromised network – such as PowerShell or Windows Management Infrastructure (WMI) – to conduct reconnaissance, lateral movement, and privilege escalation. The presence or use of these tools on a targeted network is unlikely to raise alarm, so their inappropriate use helps evade detection.

Conclusion

Reliability is NERC's mission, and grid security is inextricably linked to reliability. To date, there has not been any loss of load in North America that can be attributed to a cyber attack. At the same time, the security landscape is dynamic, requiring constant vigilance and agility. NERC addresses cyber threats through a comprehensive range of complementary strategies. Our partnership with DOE is critical to the electricity subsector's priority for security. Mandatory CIP standards provide a universal foundation for security and is a shared priority with FERC and industry. Through the E-ISAC, NERC provides situational awareness, and sharing of timely, actionable intelligence with industry and government. Strong public private partnerships are key to successful information sharing within the electricity sector and across sectors. NERC remains keenly focused on our mission to assure reliability of the BPS.

The CHAIRMAN. Thank you, Mr. Robb.
Mr. Whitehead, welcome.

STATEMENT OF DAVID EDWARD WHITEHEAD, CHIEF OPERATING OFFICER, SCHWEITZER ENGINEERING LABORATORIES, INC.

Mr. WHITEHEAD. Chair Murkowski, Ranking Member Manchin, and members of the Committee, thank you for the opportunity to share the views of Schweitzer Engineering Laboratories on the important topic of securing our critical infrastructure from cyber threats.

SEL is an employee-owned U.S. manufacturer and provider of products, systems and services for the protection, monitoring, control, automation and metering of utility and industrial electric power systems worldwide. Our mission is to make electric power safer, more reliable and more economical. We are headquartered in Pullman, Washington, and employ 3,700 folks in the United States with a total of 5,200 employees worldwide.

As highlighted by today's hearing, cybersecurity is a critical component for the secure and reliable operation of electric power systems. For 35 years, SEL has emphasized the importance of security in the products and solutions we create.

Whether it's regulatory compliance, securing power system assets or protecting operational network technologies, SEL offers security-focused solutions to help utilities protect electric networks and help vital industries protect their assets.

Today, I'd like to highlight three topics that I believe are critical to the cybersecurity challenges we face in the energy industry and our nation. First, I will review what we see as an essential role of government, "teaching the threat"; second, I will discuss the difficult task of balancing regulation and innovation; and third, I will provide a few examples of how industry is actively addressing cybersecurity threats.

My point one, teaching the threat. We read in the news weekly, sometimes daily, about advanced, persistent threats from nation-states. Clearly, our adversaries are becoming more sophisticated in the way they target our critical infrastructure. We are constantly having to evolve our thinking and innovate against these threats.

At SEL and other like-minded companies, we have some of the best engineers in the world doing just that. What we do not have is the access to the vast and sophisticated intelligence and information gathering that exists in our country. The U.S. Government has the capability to identify, classify and communicate these threats. At SEL, we take cybersecurity threats very seriously, and we act immediately when we receive information.

Building out a more robust system of communication where government agencies move quickly and efficiently to share important information, to teach us about the potential or actual threats, will not only make our systems or will make our systems more secure.

Point two, balancing regulation and innovation. SEL is a company built on the foundation of innovation. At the entrance of our research and development building in Pullman, Washington, these words are boldly displayed, "The best way to predict the future is to invent it."

Innovation and regulation do not have to be at odds with each other. Regulations, however, are often implemented as a reaction to an undesired event. As soon as a regulation is enacted to address a specific issue or event, bad actors are already looking for other avenues of exploitation.

Regulations have the capacity to limit how an institution may go about solving a problem. And further, regulations will never be able to anticipate new or innovative solutions. There are clear and obvious needs for standards and regulations and we are always ready to work together to create solutions, but we would encourage or we should be encouraged to work together in finding ways to continue fostering critical innovation that outpaces our adversaries. We cannot allow bad actors, who are unconstrained by regulations, to outpace us.

And point three, industry is actively addressing cybersecurity threats. There is so much cutting-edge work being done in our industry to keep ahead of cyber threats. During the past 35 years since the development of our first product, SEL has continued to advance cybersecurity solutions. As systems become more integrated, we have moved from a, or we moved to a, security-in-depth approach, building layers of security so that systems are not dependent on one security feature, but instead consist of many layers. And solutions range from simple to very sophisticated.

I remind folks never to connect critical infrastructure to the internet and to audit this which is certainly a very simple solution and then there's new technologies evolving like Software-Defined Networking which I'm convinced is the solution for engineered and cyber-secured industrial networks which is certainly a more sophisticated and technically advanced solution.

The Federal Government is not the only entity paying attention to cybersecurity, industry is addressing cybersecurity too. Last week, I had the opportunity to attend DistribuTECH, a very large, electric power industry conference in New Orleans. It was exciting to see cutting-edge cyber solutions being offered by both new startups and well-established suppliers. There are many brilliant minds working diligently to solve cybersecurity challenges.

As new threats emerge, and they will, industry and government must work together and learn from each other to effectively secure our critical infrastructure. And I know we can.

Thank you for the opportunity to testify, and I look forward to the questions you may have.

[The prepared statement of Mr. Whitehead follows:]



SCHWEITZER ENGINEERING LABORATORIES, INC.

2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

February 14, 2019

STATEMENT FOR THE RECORD FROM
DAVID EDWARD WHITEHEAD, CHIEF OPERATING OFFICER
SCHWEITZER ENGINEERING LABORATORIES, INC.
SUBMITTED TO THE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
U.S. SENATE
HEARING TO
“CONSIDER THE STATUS AND OUTLOOK FOR CYBERSECURITY
EFFORTS IN THE ENERGY INDUSTRY”

Chairman Murkowski, Ranking Member Manchin, and members of the Committee, thank you for the opportunity to share the views of Schweitzer Engineering Laboratories (SEL) on the important topic of securing our critical electric infrastructure from cyber threats.

SEL is an employee-owned U.S. manufacturer and provider of products, systems and services for the protection, monitoring, control, automation and metering of utility and industrial electric power systems worldwide. Our mission is to make electric power safer, more reliable and more economical. We are headquartered in Pullman, Washington, and employ 3,700 in the United States with a total of 5,200 employees around the world.

As is highlighted by today's hearing, cybersecurity is a critical component for secure and reliable operation of electric power systems. For 35 years, SEL has emphasized the importance of security in the products and solutions we create. When our first product was released in 1984, we had the foresight to incorporate multiple levels of password protection as well as physical alarms to signal unauthorized access attempts to equipment—something no one else in the industry was doing at the time. Today, whether it's regulatory compliance, securing power system assets or protecting operational technology networks, SEL offers security-focused solutions to help utilities protect electric networks and help vital industries protect their assets.

For most of its history, the bulk power system operated reliably and securely without communications. While the benefits of communications technologies have greatly enhanced the monitoring, automation and control capabilities of electric power systems, it is necessary to ensure communications systems are secure. I do not believe our security challenges are insurmountable.

Today, I would like to highlight three topics that I believe are critical to the cybersecurity challenges we face in the energy industry and our nation. First, I will review what we see as an essential role of government—“teaching the threat.” Second, I will discuss

the difficult act of balancing regulation and innovation. Third, I will provide a few examples of how industry is actively addressing cybersecurity threats.

Point #1: Teaching the threat. We read in the news weekly, sometimes daily, about advanced, persistent threats from nation-states. Clearly, our adversaries are becoming more sophisticated in the way they target our critical infrastructure. We are constantly having to evolve our thinking and innovate against these threats. At SEL and other like-companies, we have some of the best engineers in the world doing just that. What we do not possess is access to the vast and sophisticated intelligence and information gathering that exists in our country. The U.S. government has the capabilities to identify, classify and communicate these threats. Sharing information with asset owners and equipment manufacturers through a just-in-time approach is critical to keeping our systems and electrical infrastructure safe. It has been my experience that asset owners take cybersecurity seriously and will act if they understand the threat. At SEL, we take cybersecurity threats very seriously and we act immediately when we receive information. Many in our industry already have positive working relationships with various government agencies. Building out a more robust system of communication where government agencies move quickly and efficiently to share important information—to teach us about potential or actual threats—will only make our systems more secure.

Point #2: Balancing regulation and innovation. SEL is a company built on the foundation of innovation. At the entrance of our research and development building in Pullman, Washington, these words are boldly displayed: "The best way to predict the future is to invent it." Our R&D researchers and inventors pass by this quote daily. Interestingly, our practice of building cybersecurity into everything we make was a concept learned by our founder early in his career while working for the Department of Defense.

Innovation and regulation do not have to be at odds with each other. Regulations, however, are often implemented as a reaction to an undesired event. Developing a regulation may be fine to address static situations, but cyber is a dynamically changing environment. As soon as a regulation is enacted to address a specific issue or event, bad actors are already looking for other avenues of exploitation.

Regulations have the capacity to limit how an institution may go about solving a problem. For example, if a new and innovative solution does not conform to regulations but is the best way to address a security element at a company, the company may choose not to employ the solution, or worse, be fined for noncompliance if they chose to use that solution. Further, regulations will never be able to anticipate new and innovative solutions. For example, NERC CIP-005-5 requires multifactor authentication for all Interactive Remote Access sessions. What happens when new and potentially more effective authentication methods are developed?

As you are aware, a great deal of time is being spent discussing, debating, demonstrating and proving compliance. I believe this time could be better spent on creating and deploying innovative solutions that will keep us in front of threats.

There are clear and obvious needs for standards and regulation, and we are always ready to work together to create solutions, but we should be encouraged to work together in finding ways to continue fostering critical innovation that outpaces our adversaries. We cannot allow bad actors, who are unconstrained by regulations, to outpace us.

Point #3. *Industry is actively addressing cybersecurity threats.* There is so much cutting-edge work being done in our industry to keep ahead of cyber threats. During the past 35 years since the development of our first product, SEL has continuously advanced our cyber security solutions. As systems became more integrated, we moved to a security-in-depth approach—building layers of security so that systems are not dependent on one security feature, but instead consist of many layers. And solutions range from simple to very sophisticated. I remind folks to never connect critical infrastructure to the internet; audit this—a simple solution. Software-Defined Networking is emerging as the solution for engineered and cyber-secured industrial networking.

SEL is partnering with universities, including Washington State University, University of Idaho, Montana Tech and Purdue, to develop new ways to secure industrial networks. We have participated in the U.S. Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) program. Under the CEDS program, SEL has partnered with utilities and national laboratories across the country to identify, design and test new solutions for protecting critical infrastructure from cyber-attacks.

The federal government is not the only entity paying attention to cybersecurity; industry is addressing cybersecurity too. Last week, I had the opportunity to attend DistribuTECH, an electric power industry conference. It was exciting to see cutting-edge cyber solutions being offered by both new startups and well-established suppliers. There are many brilliant minds working diligently to solve cybersecurity challenges.

As new threats emerge—and they will—industry and government must work together and learn from each other to effectively secure our critical infrastructure. And I know we can.

Thank you for the opportunity to testify, and I look forward to any questions you may have.

The CHAIRMAN. Thank you, Mr. Whitehead.

I think your comments really sum it up neatly. Specifically, how do we stay ahead of the bad actors? To use your words, the best way to predict the future is to invent it, but that requires us to be nimble and flexible, to be quick. You mentioned that it would be helpful if government agencies moved more quickly to share information.

One of the things that we are not really adept at here in the Federal Government is moving quickly and sharing things readily. It speaks to the reality of this problem that we are reckoning with, not just here in the Energy Committee but across all of these Committees, whether you are on SASC or you are on Commerce or Homeland, this is impacting all of us.

You have suggested, Mr. Whitehead, that some regulations can inhibit the process of invention. We would like to think that some regulation can actually help incentivize more investment, which I hope is the purpose of the joint conference that FERC and DOE are going to be hosting, called Security Investments for Energy Infrastructure.

So, just a quick conversation this morning with you, Mr. Chairman, Assistant Secretary, and Mr. Whitehead. Exactly what options are out there to help facilitate this ability, this innovation, so that we have the investment that will line up behind it because you cannot have one without the other.

Do you want to start off, Mr. Chairman?

Mr. CHATTERJEE. Thank you for the question, Chair Murkowski.

As I mentioned in my opening remarks, the Commission takes a two-pronged approach to address much of what you and Mr. Whitehead just laid out.

We have mandatory reliability standards overseen by our Office of Electric Reliability but I firmly believe that those standards are the floor, not the ceiling. And that is why the second prong of our approach through our Office of Energy Infrastructure Security on focusing on voluntary best practices. Coordinating with other agencies is so critical to keep up with these, with the required information sharing that is necessary and these fast-evolving threats that we're dealing with.

The CHAIRMAN. Do you think we share information quickly enough and adequately enough?

Mr. CHATTERJEE. I think the efforts that Secretary Perry and Deputy Secretary Brouillette have led through the Electric Sector Coordinating Council have been effective. We've got the appropriate agencies and industry and stakeholders at the table, but we need to be smarter and better. We can always be better.

I'm looking forward to the joint technical conference to make sure that as we look at cyber and physical protections that we have the right incentives policy in place. And that's really an important role that FERC can play in ensuring that those incentives to take on those risks are there so that we attract the right kind of investment focused on these physical and cyber threats.

The CHAIRMAN. I appreciate that.

Under Secretary?

Ms. EVANS. So I'd like to approach it a couple different ways based on what we've talked about today.

The CESER office is actually looking at this challenge in concurrent paths, not sequential paths. There are specific things that we have to be able to do in order to respond and understand what's going on, and I think a lot of that deals with the information sharing.

It's clear with what Chairman Chatterjee has said and the leadership and the partnership that we have with the E-ISAC and our electricity subsector coordinating council as well as the oil and natural gas coordinating council. So a lot of that information is being shared.

A specific example I would like to share is that this Administration and we have been very forward leaning with attribution and then doing a full, multi-pronged approach with indictments as well as sanctions and then putting context around the information as to what is the threat and then how do you manage that. And then we share it out through the E-ISACs.

But the other thing that we most recently have done on February the 6th, the Department has sent out a notice of intent, and you're going to hear me reference this a lot, which is the "Clean Energy Manufacturing Innovation Institute: Cybersecurity in Energy Efficient Manufacturing" because to me, that is how we get to the innovative leap ahead types of things.

Everything that everyone has talked about, about building it into software, being able to manage ahead, taking care of innovation, that is the vision of what this manufacturing institute will do. And looking at a lot of the things that we have learned as an industry across the board and building it in so that we can take advantage of the technology.

The CHAIRMAN. Thank you.

Mr. Whitehead, is this going to help?

Mr. WHITEHEAD. What I think the biggest help we see right now is having forums this like where I had the opportunity to meet with Mr. Robb this morning for lunch and the information sharing that is set up right now with members and government is really the asset owner, so the Baltimore Gas and Electric, the PEPCOs and so on and so forth.

Where I think, for my request, is we're off one derivative though because I'm the manufacturer of these devices that are getting installed by the asset owners. And so, if there is a cyber threat or one of these activities going on, I think we're the most skilled in ascertaining what is the impact of a particular cyber threat because we're the ones writing the code, developing the hardware. So getting us looped in as quickly as possible if there's an attack out there and setting up mechanisms so it's, we refer to it as a JITE type of information exchange, I think it would really move us forward in terms of being able to secure our critical infrastructure.

The CHAIRMAN. Thank you.

Senator Manchin.

Senator MANCHIN. Thank you, Madam Chairman. I thank all of you for your appearance today.

Many in this room, myself included, spent time at substations and know how physically vulnerable they used to be. In April 2013, attackers with rifles shot 17 transformers at a Metcalf, California

substation. Before the attackers opened fire on the transformers, fiber optic lines running nearby were cut.

Since then, NERC has proposed standards requiring transmission owners to address physical security risk and vulnerabilities that could impact the reliable operation of the grid.

Mr. Robb and Chairman Chatterjee, I want to ask quickly, how has the physical security of the grid, specifically at substations, improved since those attacks? Very quickly, if you will.

Mr. ROBB. Now that the physical security standard you referenced has been put in place, all of the utilities in the country have had to identify critical assets within their jurisdiction and when we have to verify that they did the assessment of what's critical correctly and then they have to have a credible hardening plan against them. So not every substation in the country is subject to that protection standard, but the critical ones are and those actions have been put in place.

Mr. CHATTERJEE. I agree with what Mr. Robb has said. You know, the important part is identifying, you know, where those critical substations are and where those key interconnections are and we have to remain, you know, vigilant on this.

Senator MANCHIN. Let me go into this then.

Just a week and a half ago, NERC issued the largest ever fine for 127 violations of physical and cybersecurity standards. As a general matter, many in the electrical sector have viewed the NERC standards as effective at establishing a baseline for cybersecurity.

It is also my understanding large utilities often have more resources available to them than the smaller utilities to make the necessary security investments.

So, again, my question would be as the entity responsible, Mr. Robb, for enforcement and imposing fines, what is your view of the current state of compliance across the country?

Mr. ROBB. So, in general, the industry has taken security very, very seriously and I think one of the important things to note about the CIP standards is one, they're relatively new to the industry. And most all of the violations that we process, including many in the enforcement action you referenced, Senator, are voluntarily reported, detected through detective controls within the entities. And I think that, in and of itself, shows the level of diligence and seriousness with which industry approaches this.

I think your question about the resources of large versus small entities is a very insightful question. One of the things that we have done with our substandards is try to take a very thoughtful, risk-based approach to make sure that those entities, those assets, those functions, if you will, elements that propose the highest risk to reliability are more thoroughly protected and for lower risk entities and so forth, that they are, they have a baseline—

Senator MANCHIN. Are there resources available to the smaller utilities so that they can maintain the security they need?

Mr. ROBB. I can't speak, obviously, for every utility in the country.

One of the—

Senator MANCHIN. No, I am saying do we have programs in place, government programs, because of the necessity of security,

to make sure that smaller utilities are still meeting the highest security standards we have?

Mr. ROBB. The small utilities are required to be compliant for those functions that they are responsible for.

One of the other initiatives that the industry has put in place though is something called Cyber Mutual Assistance.

Senator MANCHIN. Okay.

Mr. ROBB. So that if an entity that is resource constrained suffers a cyber event or a physical event, that in the same way that the industry will muster resources to help in storm recovery and so forth, will also deploy resources to help in cyber recovery.

Senator MANCHIN. Every two years, the North American Electric Reliability Corporation Grid Security Exercise, called GridEx, challenges utilities and state and local governments to respond to realistic cyber or physical security threat scenarios.

Major KEBER, from our little State of West Virginia, are you all participating? Do you participate in GridEx?

Major KEBER. Sir, to date, I have not personally, but yes, we do send other members that are working in our cybersecurity.

Senator MANCHIN. Are all states represented? Do we know who is participating in GridEx so we can basically evaluate their proficiency?

Mr. ROBB. I can't affirm that every state does, but I'm pretty sure they all do.

Senator MANCHIN. And?

Major KEBER. Yes, sir, I have heard that there is good representation from other states to include West Virginia's participation in the national GridEx exercise.

Senator MANCHIN. Thank you, Madam Chairman.

Thank you, all, I appreciate it.

The CHAIRMAN. Senator Risch.

Senator RISCH. Thank you, Madam Chairman.

First of all, I want to welcome Mr. Whitehead here. We are honored to have a good chunk of Schweitzer Engineering Laboratories in Idaho. Mr. Whitehead, I think, was very modest in his description of what the company does. You indicate you have 5,200 employees around the world. How many countries do you operate in, Mr. Whitehead?

Mr. WHITEHEAD. We have product in about 146 different countries, so we certainly have a global presence.

Senator RISCH. Yes.

Schweitzer Engineering was founded by a genius of a man, Edward Schweitzer, who is a former NSA employee, interestingly enough. And he is the driving force right now behind the establishment of an NSA museum here in Washington, DC.

The products that they put out are legendary around the world, and we are glad to have you.

You and I have talked a little bit about this but when I started about ten years ago on this, well, on this Committee and the Intelligence Committee, the cyber thing was becoming obviously a big issue. At that point the private industry was very, very reluctant to engage the United States Government in its activities and particularly to disclose to them what kinds of things they were doing, what they had, et cetera, et cetera.

After a couple of few incidents the private sector and, by the way I understand where they were coming from on this, but after a couple of few incidents the private sector had a rude awakening and now that whole situation has changed dramatically.

Do you agree with that assessment, that the private sector has realized that they are not big enough to individually take on this cyber threat?

Mr. WHITEHEAD. I think there's certainly a lot of talent within the private sector to go about solving problems. Certainly, the challenge we have in the private sector is knowing all of the threats that may be coming at our critical infrastructure.

And I think, again, that's where the government plays a great role. They have a lot of resources to understand, attack vectors and who may be the threat actors challenging our systems. So the ability to work with the government to quickly exchange information, tell us what's going on, by us being the individual manufacturers or the asset owners, being able to tell us what the threat is or teach us what the threat is. We have a lot of brilliant minds that then can figure out how to mitigate those threats and come up with new solutions to protect our critical infrastructure.

Senator RISCH. It has become a much more robust partnership then, would you agree with that, between the private sector—

Mr. WHITEHEAD. Yeah, I think, yeah. After the last ten years or so we're getting, you know, great relationships with NERC and other regulating bodies.

I feel that the pace with which information gets disseminated could—it would help us all if it was sped up.

Senator RISCH. As I listen to the threats through the Intelligence Committee, I am always amazed that we do not have more trouble than we do with the number of people that are levying a tax against us, the number of attacks that they are levying against us and the sophistication with which they are operating.

It is things that you make at your company that stop that and, for that, I think everyone should be grateful, although most people have no idea what, that those devices are out there between them and between the device they are holding and where they are communicating with.

Mr. WHITEHEAD. Thank you.

And it's not like, well certainly from SEL's perspective which we woke up say, five years ago, and thought cybersecurity would be a challenge. And as you pointed out, Ed, Dr. Schweitzer, had a career at DoD and took cybersecurity very seriously. So even back in 1984 when he created the first product, there were two levels of passwords and other means for signaling control systems, that there was, you know, at least an attempted access to one of our devices.

So, this is, we've always, I think, taken cybersecurity very, very seriously from day one, certainly at SEL, and I think our industry also appreciates the need for cybersecurity.

Senator RISCH. Well, we appreciate that.

Major Keber, very briefly.

I understand that you recently had some training at the Idaho National Laboratory (INL) on cybersecurity. Is that correct?

Major KEBER. Yes, sir, that is.

Senator RISCH. Realizing you cannot tell us everything about it, for those of you who do not know, the Idaho National Laboratory has been the flagship nuclear energy laboratory in America and is quickly becoming the cybersecurity flagship laboratory in America which we are glad to have. It has some unique things going on there, some unique assets, that they have that make it such.

Could you tell us a little bit, briefly, about your training there and what you can tell us about it?

Major KEBER. Yes, sir.

It was, the training was a very good, comprehensive look at industrial control system cybersecurity. We looked at specialized, sort of, devices that are unique to industrial control system and kind of looked at the holistic approach of how to access those particular networks and infrastructures developed.

They did take us, we did take a look at the tour of the lab that they have there. It was a very interesting and unique, one of a kind, site to see.

Senator RISCH. Did you meet with any of the strike teams that they have there that are ready to deploy?

Major KEBER. Yes, sir.

We met with some of their assessment teams. They came in and we had an engagement with them and it was very informative. We shared and cross-leveled best practices and took a lot from what they had to offer in a way of experiences and things that they're seeing out during their assessments.

Senator RISCH. Well, we are proud of the INL, and glad to hear that it worked well for you.

So thank you very much. My time is up. Thank you very much, Madam Chairman.

The CHAIRMAN. Thank you, Senator Risch.

Senator Stabenow.

Senator STABENOW. Thank you, Madam Chair.

First to you and the Ranking Member, congratulations again on a very important lands bill being passed. I know it was an incredible amount of hard work for a long time. So congratulations.

This is an incredibly important hearing. It touches every part of our economy, our way of life, and our national security. So thank you to all of you for being here.

The last polar vortex a few weeks ago produced, as we know, freezing temperatures and snow and rain across the Midwest. We certainly felt that in Michigan. We had a gas compressor station in Southeastern Michigan that suffered an unexpected fire, and there were a lot of questions about how that happened and what was going on, as you know. It resulted in Michigan families being asked to lower their thermostats, and businesses, including our auto manufacturers, suspended operations.

It was a real sobering reminder of the vulnerabilities, both because of climate change and what is happening around carbon pollution, and cyberattacks from foreign companies or others and the increasing interdependence of our critical infrastructure. And I know that is why we are having this discussion.

I want to stress one area in transportation coming from Michigan, because we know that the new cybersecurity threats are emerging as transportation becomes more electrified and autono-

mous. This is another important piece because we know that by next year, 90 percent of new cars are projected to be connected to the internet and what comes with that. And we know that within 20 years, 55 percent of all new car sales are projected to be electric, in addition to other kinds of fuels.

We currently have mandatory federal cybersecurity standards for bulk power in electric systems, but not for interstate natural gas pipelines and electric distribution that directly services homes, businesses and transportation.

I know that Chairman Chatterjee, you mentioned that gas infrastructure, but to you and Mr. Robb, isn't it time we had mandatory cybersecurity standards for this critical electric and gas infrastructure?

Mr. CHATTERJEE. Thank you, Senator Stabenow, for the question.

And yes, the point you raise is spot on. The increased interdependence that we are seeing, particularly between gas and our electricity mix in our power system makes ensuring the security of that infrastructure so important and so significant. And it's something that I've been particularly concerned about.

I partnered with my colleague on the Commission, Rich Glick, early on after we both joined the Commission, to highlight the fact that due to this increased interdependence focusing on the security of this infrastructure was essential. We raced and looked at the fact that while FERC was responsible for permitting the approval of the pipeline, the responsibility for securing the pipelines, you know, against physical and cyberattacks fell to the TSA. So, the agency which is responsible for 800 some odd million aviation passengers, the highways, our rail system, also responsible for this massive network of pipelines. We had concerns about the resources and the personnel and the expertise at TSA to do this as well as the fact that TSA relied upon voluntary standards.

One thing that I will say is that in the past year since Commissioner Glick and I, sort of, elevated the profile of this discussion and folks like Senator Heinrich and others have introduced legislation on it, I have been impressed by the response I've seen from both industry and TSA. Industry has really moved forward to take ownership of this and take steps to demonstrate their seriousness and focus on investing in the security. And as I mentioned in my opening remarks, in meeting with the TSA Administrator, it was clear that they were putting a greater focus on this. That said, the recently published GAO report showed that there is still much, much more work to do.

And so, while I'm pleased with the progress we've seen since we elevated the profile of this issue, I'm going to remain vigilant on it because there's a lot more that needs to be—

Senator STABENOW. Well, we have been talking about this for a long time, frankly, and not moving as fast as the technology. Those that wish to use the technology to do us harm are moving. I did not hear yes or no on mandatory cybersecurity standards.

Mr. CHATTERJEE. Again, I think it's an ongoing dialogue that we'll have to see.

Senator STABENOW. Alright.

Mr. CHATTERJEE. I've been encouraged by the voluntary, by the improvement in the voluntary steps that industry has taken and

by the attention that TSA is putting to this. I want to continue to work toward that.

Senator STABENOW. I understand. We need to be moving a lot faster.

Mr. Robb, did you have thoughts on that?

Mr. ROBB. Well, I'll agree with the Chairman that the interdependency between natural gas and electric, the electric sector, has become fundamental now to the reliability of the system. Without fuel, power plants can't run.

And while I can't comment authoritatively on the state of cybersecurity on the pipelines and the effectiveness of the voluntary standards that are in place there, I think it is incumbent upon the natural gas industry to be as secure as the industry that they are supporting.

Senator STABENOW. Okay. We have a lot of work to do in all of this.

My time is up, so I will not ask another question, but I am going to ask in writing about the vulnerabilities in our energy supply chain and whether our growing dependence on foreign made energy components presents a potential national security threat, as we are hearing from our own intelligence community when they say technology supply chain attacks are a key threat. I know in the auto industry they are deeply concerned about that.

So thank you, Madam Chair.

The CHAIRMAN. Yes, it is a good question.

Senator Cassidy.

Senator CASSIDY. Mr. Whitehead, I think it was you who mentioned the necessity for increased information sharing between the Federal Government and folks such as you. I totally agree. Why is it not occurring?

Mr. WHITEHEAD. I think that's better left up to Mr. Robb or the Chairman.

When we had to have conversations to make great conversations with them, I think that we're just at a point now where we've established between say, the government and the asset owners. I think that the next step in the evolution of how we share information that will certainly include the equipment suppliers to the asset owner.

Senator CASSIDY. So let me kick it over to you, Mr. Chatterjee, because if we have voluntary standards and as Senator Stabenow said, okay, it's very important, but everybody's testimony says it is dynamic. How can you voluntarily comply with a dynamic situation when you are not given the information about the dynamism? Does that make sense?

Mr. CHATTERJEE. It makes complete sense.

I think there are a number of elements to this. The topic of workforce has come up. You know, cybersecurity talent is hard to find.

Senator CASSIDY. Now, that seems separate though, if I may, because obviously you have somebody coding but you have somebody else saying, uh oh, we never thought of this one but they are coming at us this way. That is not workforce, that is information sharing.

Mr. CHATTERJEE. Information sharing is a component of it as well. There's also issues, quite frankly, that are taking place with getting the sufficient clearances.

FERC has been trying to do our part to do one day read ins so that our colleagues at the state level and industry have access to—

Senator CASSIDY. Now, we have heard testimony, not to interrupt, but I have limited time.

Mr. CHATTERJEE. Yes, sir.

Senator CASSIDY. We have heard testimony, because I think Madam Chair has a fixation on this topic. So last time we had several hearings on this, and it was that the big energy producers have that clearance. There is someone there who has that clearance. But still I am hearing from Mr. Whitehead, who is being very diplomatic over there, that the information is not being shared. Now you sense my frustration.

Mr. CHATTERJEE. Absolutely, sir.

Senator CASSIDY. So, digame, porqué?

[Laughter.]

Why is that?

Mr. CHATTERJEE. So again, there are challenges that occur in terms of sharing the information in a classified setting. We are doing everything we can to make sure that the information that we gather in a closed setting or an open setting is shared with industry partners—

Senator CASSIDY. What I am hearing from Mr. Whitehead—my eyes are not good enough, is it doctor or mister?—that is not the case. Ms. Evans, did you have some comment on that?

Ms. EVANS. Yes, sir, I appreciate the opportunity to discuss this with you.

This is exactly why Secretary Perry established the CESER office is to address the frustration that you're experiencing right now and that you're expressing.

So the activities in the programs in our office are to help bridge that gap with our partners because we're looking at it from a national security perspective. So the threats, the things that you're talking about, how do you declassify that and then how do you get it out to the asset owners as well as to the people that are delivering services and also software and manufacturers, those types of things?

Senator CASSIDY. So none of that is aspirational.

Ms. EVANS. Well, no, I was going to get into—we were doing things. We actually have—

Senator CASSIDY. Okay, because I have a minute and 40 seconds left.

Ms. EVANS. Okay.

So we have several programs underway and the most recent example under my tenure is the APT10 threat where we worked to declassify, with the intel community, declassified those indicators, then shared those out with the community through the E-ISACs and then continuously communicate that back out. We work with the national labs and it's—

Senator CASSIDY. Why would Mr. Whitehead say that there is still an issue here?

Ms. EVANS. Because the Administration and Secretary Perry and this office has been established for four months.

Senator CASSIDY. Got it.

Ms. EVANS. And so, I would give you, I would ask you to give me the opportunity to increase that because he does work with our research and development program and there are several programs that we are actually working in conjunction with him to improve that.

Senator CASSIDY. Got it.

Now let me ask you one more thing. Everybody mentions this dynamic you don't want regulations but there was a malware incident with Entergy about a year ago and it was on the corporate side, not on the grid side. I think it is MISO—I never know if it is “meeso” or “miso”—but the concern was that it might infect the transmission. It did not because it was in corporate.

That just seems like a best practice that you would have a firewall between somebody opening an attachment from his son which turns out to be malware versus that which is sending electrons from Indiana to Louisiana.

Knowing that we do not want to regulate this to death but are there best practices that are expected to be complied with because, for example, in a previous hearing we heard that in some situations they have an analog switch as a best practice because it doesn't allow the cyber to go all the way through because there's one little flip that a human being has to do that otherwise protects one side from the other. Are there best practices that we are, kind of, mandating?

Ms. EVANS. Well, we're not mandating best practices. What DOE does is share the information out with our respective partners that are represented here as well as into the community. So that specific incident that you are describing really says, okay, if you're going to gain efficiencies, don't connect your IT systems to your OT systems. Yes, that is a best practice that is stressed throughout the community that is talked about over and over again. I know that the E-ISACs have shared that information out in the community. But this is some of those things where you have to over communicate to make sure that best practices and the exercises—you know, we have done joint exercises with FERC. We do the exercises, we participate because exercises highlight what you think the best practices are, give you opportunities to really demonstrate those and then to continuously close the gap. So everybody has been talking about that, that is important.

Senator CASSIDY. I have a question for the record regarding compliance with those best practices because once you have everybody putting their electrons on the same grid, you want to make sure that they are not just thinking about it but they are actually doing it.

Ms. EVANS. Yes, sir.

Senator CASSIDY. So we would like to know about compliance.

Madam Chair, thank you for indulging.

The CHAIRMAN. Thank you.

Senator King.

Senator KING. Thank you, Madam Chair.

First, I would like to hopefully suggest that we can move quickly on S. 174, which is the bill of Senator Risch and me. Last year it was S. 79. It passed the Senate and came within a whisker of passing the House at the very end of the session. I hope we can. We have had a hearing. We have had a markup. I hope we can move that bill out because it addresses this question exactly.

There is a weird calmness about this hearing.

[Laughter.]

This is not calm. The Russians are already in the grid, are they not, Mr. Robb?

Mr. ROBB [off mic]. I can't—

Senator KING. Well, there were news reports from a year ago of the Department of Homeland Security releasing screenshots of Russian hackers in the SCADA system. Is that not true?

Mr. ROBB. Again, I'm not in a position to talk—

Senator KING. Well, can you comment on the public story that was something released by the Department of Homeland Security?

Mr. ROBB. No.

Senator KING. Okay, let me ask another question.

Do any of our utilities have Kaspersky, Huawei or ZTE equipment in their systems?

Mr. ROBB. We issued a NERC alert.

Senator KING. I did not ask you if you issued an alert. I am asking you, do any of our utilities have ZTE, Huawei or Kaspersky equipment or software in their systems?

Mr. ROBB. Not to my knowledge.

Senator KING. Not to your knowledge.

Mr. ROBB. Not to my knowledge.

Senator KING. Have you surveyed the utilities to determine that?

Mr. ROBB. I don't believe we have.

Senator KING. I think that would be a good idea, don't you?

Mr. ROBB. I'll take that on.

Senator KING. Thank you.

Of course there should be mandatory standards for gas pipelines. They are part of the electric system. 60 percent of the energy of the electric industry supply in New England is natural gas, not to mention heating.

It seems to me we have already passed this, an effective system for the electric utilities, and Mr. Chairman, I am with you 100 percent, but I just don't want you to hedge about it. I think you should come right out and say, we have to do this.

Mr. CHATTERJEE. I think mandatory standards are one way to do this, but I just would caveat that they are not necessarily the only way and the only—the point that I was making was that I've been heartened by the significant support I've seen from industry since I raised the subject matter, and I want to continue that productive dialogue.

Senator KING. Do they support mandatory standards?

Mr. CHATTERJEE. Right now, again—

Senator KING. Let me guess, they don't.

Mr. CHATTERJEE. At this stage I have to commend them for the steps that they have taken since I raised this issue, and I want to give them the opportunity to work in good faith going forward.

Senator KING. Well, I appreciate working in good faith, but it seems to me we made a realization some years ago that mandatory standards made sense in the electric side. If the natural gas pipeline system is now essentially a part of the electric system, I see no reason why that should not be the case in that industry.

Mr. CHATTERJEE. I think there's no question that Congress continuing to shine a light on this will help move forward on this issue.

Senator KING. Major, do we red team the utilities?

Major KEBER. Sir, not at this time, I do not. My teams do not red team utilities and private sector. We are focused on government-only entities.

Senator KING. Mr. Robb, does anybody red team the utilities?

Mr. ROBB. I'm not aware of, sir.

Senator KING. Don't you think that would be a good idea? You can't really tell if you are safe until somebody smart comes in and tries to attack you.

Mr. ROBB. I'll take that, sir.

Senator KING. Thank you.

Again, I just think we are entirely too calm about this. This is not a threat. This is happening now. We are under attack.

This is not something that may happen next year or two years from now, and I am not revealing anything classified in the sense of quoting news articles and presentations by the Department of Homeland Security.

We are in a very dangerous place and I just think this has to be an emergency, an urgent situation and that's—I just, I hope I have conveyed that here this morning.

Madam Chair, I really commend you and the Ranking Member for doing this hearing, because I do not think there are many more serious threats facing this country than this one.

And I thank all of you. I don't mean to come off as negative. I love what you are doing at the Department of Energy. You have the office set up. It is the right structure.

But I just think this has to be addressed with a real sense of crisis because I do not want to go home to Maine and say, well, we knew what was going on but you know, we had four committees here that had jurisdiction and we really could not quite get it done. We have got to get it done.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator King.

I am reminded that when it comes to pipelines that, oddly, it is not our Committee's jurisdiction, it is the Commerce Committee. But you are right, cybersecurity is not limited to this Committee or to Commerce or to Homeland or to SASC, it is cross-jurisdictional. We need to address it as such.

How we are able to do that and do that quickly gets back to the issue that it is not only agencies being nimble. It has to be amongst us and our committees and how we are talking with one another, because right now we all know that we have our own silos inherent within this. But you have good cause to be frustrated.

Let's go to Senator McSally.

Senator MCSALLY. Thank you, Madam Chair.

I want to pick up where my colleague left off, because I agree this is a very real threat and the threat is with us.

I am thinking back if I close my eyes, I worked for Senator Kyl back in 1999 when I was a major in the Air Force as a Legislative Fellow. As he was the Chair of Technology Terrorism and Government Information Subcommittee on Judiciary, this is what we focused on. The majority of my portfolio was cybersecurity related to critical infrastructure and at that point the potential threat of state actors and non-state actors to hold us hostage and to take down grids and the potential attacks there. If I close my eyes this would sound like a hearing from 19 years ago in many ways.

I do not want to take away from some of the things that have been done but what has changed in 19 years, more rapidly than us figuring out how to defend, protect, share information and do whatever it takes, is the threat is real and it is happening. And that includes China and Russia, Iran, other non-state actors that have just taken leaps and bounds investing in looking at how they could go after us in asymmetrical capabilities, to go after us where we might be vulnerable.

I appreciate you, Madam Chairman, for doing this hearing. I appreciate the discussion today.

I am deeply concerned about the threat, the information sharing, the silos, both up here and out there.

One is related to information sharing to rural communities. So, the CRISP program, Ms. Evans. I want to talk a little bit about some of the major utilities. A lot of them are involved in it and that is great, but in Arizona the vast majority of our communities are rural and so the smaller companies or the co-ops and others—how is that program going to be able to or how is more information sharing going to be able to get out to small utility companies so that they are equally informed and protected?

Ms. EVANS. So I appreciate the opportunity to answer that question, and I want to share although we are calm, I would say that the Administration shares your sense of urgency in addressing this issue because we know the threat is real and we know that we have to deal with the energy sector accordingly.

And it is a multi-pronged approach to the question about is there red teaming that is happening in the utilities. DHS does have that capability and does offer it when it is asked for. It is a voluntary type of activity.

As it relates specifically to the municipalities and co-ops, we are embracing and taking that and leaping forward because CRISP is an evolution of several lessons learned that we have from the energy sector. And the one thing that I want to highlight is that trust relationship that is key to information sharing.

If you have this long history, as you have said, then you know if there's no trust in the sector then the information isn't going to be shared. And so, CRISP and the E-ISAC and the leadership from the energy sector, across the board, both with pipelines as well as oil and natural gas and the electric sector have really built the trust. That's how we share the information. They have an oil and natural gas. We have the E-ISAC. And also because of what happened with the FAST Act of 2015, this Committee clearly estab-

lished that DOE had to say what is the critical defense, critical infrastructure and what are the energy assets associated with that.

When we did that, Assistant Secretary Walker has done that. We, as DOE, because of the critical nature paid to make sure that those municipalities that were identified in that could be part of the CRISP program as we continue to evolve how we're going to do information sharing in a dynamic bidirectional way.

Senator MCSALLY. Great, thanks.

I do want to follow up also on the clearances issue. I was on the Homeland Security Committee in the House and this, for all sorts of threats that we are talking about, whether it is terrorist threats to, you know, massive sports gatherings or retail industry, the constant issue that came up is the lack of ability for individuals that are out there, day in and day out, that are having to deal with the threat, knowing what is going on.

We have done a good job since 9/11 in general of breaking down barriers among federal agencies, but now this vertical information sharing amongst governments and with the private sector is just something that is lacking. So the clearance issues, the opportunity to do tear lines so that the information can be shared out there is really important. Where are we in breaking down some of those barriers? We have to protect, obviously, information, but there are ways to do this by reading in more people with clearances and using tear lines.

Ms. EVANS. Well, the clearance process, as you know, is an amorphous process that everyone participates in but I would say that the intelligence community is very forward leaning because the worldwide threat assessment document that was just released on January 29th really clearly outlines what the current state of affairs is. And that's an open-sourced document that everyone can read.

Now what we have done from our perspective is those with clearances, we're giving them more specific information associated with that. But I don't know how much clearer you can be if you don't read that document about what the threats are, the sense of urgency, what our adversaries, our nation-states are capable of doing and what we need to do as a nation in order to be able to secure the energy infrastructure.

Senator MCSALLY. Great.

I am out of time, but I think I am also talking about specific threats as they are arising. I realize we have to protect sources and methods but then getting that information out quickly.

Thank you.

Thank you, Madam Chair.

The CHAIRMAN. Senator McSally, I appreciate you raising the issue of security clearances because we have heard that time and time and time again. I understand that it is still an issue even though we addressed it through the FAST Act but we continue to have holdups through the FBI.

Those who need it—

Senator KING. Madam Chair, last time we checked in the Intelligence Committee, there was a backlog of something like 750,000 security clearances.

The CHAIRMAN. Yes.

Senator KING. It is a huge problem.

The CHAIRMAN. Yes.

You say you are working to get the clearances, but you still have folks on hold. So you cannot get the information that you need to share because you do not have the clearances.

Mr. WHITEHEAD. Just a point of clarification, and I'm sure our company is not unique, but at SEL we have folks with clearances, including myself up to the TS/SCI level so we can sit in classified briefings and get to understand the details of what those threats might be.

The CHAIRMAN. I should hear from our folks. You speak about the rural application and there is a need to know here.

Senator Heinrich, you are probably going to carry on this conversation, so it is your turn.

Senator HEINRICH. I will do my best, and thank you for having this hearing.

I continue to hear from utilities that it is a real challenge, the backlog, and that it is a huge bottleneck. In fact, we heard from a former member last year, if you remember, who used to be on the House Intelligence Committee, that he could not get his clearance. If he can't get his clearance, then who can?

Let me switch gears here and, Mr. Robb, you mentioned spear phishing. I agree that is an incredibly important point of entry that we need to do a better job on, and it is a hard one because it is human-based.

Secretary Evans mentioned separating IT systems and OT systems. When I think about this—and I grew up in a utility family, my dad was a lineman then he went on to manage both gas and electric distribution systems—there is a bias in utilities and it is, oftentimes, a very positive bias toward reliability. But sometimes that can manifest itself in ways that do not help us update systems.

Specifically, I think about SCADA systems and I think about programmable logic controllers. I think about the openings there with regard to being able to control those systems using radio communication due to the fact that they are hard to air gap, especially the older ones. And I worry that we are not moving fast enough, especially in a world where it is often viewed that if it works, just leave it alone. Sometimes that causes utilities, or the person whose job it is to actually update the software or change out an outdated component, to not do that. And so, those challenges continue to exist well beyond their normal life span.

Are we doing enough in terms of securing and updating those kinds of components across the entirety of the utility system, Mr. Robb?

Mr. ROBB. Yes, so a couple comments to your point directly.

The CIP standards do require critical systems to be patched and to be kept at up to date with the latest releases.

You're right that it is a challenge in many cases to reconfigure systems without studying all the derivative ramifications of those. It's a very complex machine but the standards do require ongoing patching and modernization.

Senator HEINRICH. Do we spot check or have any way to just make sure that it is actually happening?

Mr. ROBB. Subject to spot check and thorough audit.

Senator HEINRICH. Great.

Mr. ROBB. Routinely.

One other point I wanted to make, if I could, just a second.

Senator HEINRICH. Sure.

Mr. ROBB. The Senator's question from Arizona because it's applicable here.

The CRISP program insights are not confined to just the CRISP participants. When we work through the insights that come out of that program, although they originated from a handful of utilities, they're disseminated broadly across the—

Senator HEINRICH. So, rural electric co-ops, for example.

Mr. ROBB. So, the rural electric companies, the municipalities and so forth are the beneficiaries of that information.

I am sorry.

Senator HEINRICH. No.

Chairman Chatterjee, I wanted to ask you, is TSA the right place—and I appreciate that they are putting more focus on this and they seem to have a pretty big job at the airports, I have noticed—is it the right place for that to live?

Mr. CHATTERJEE. When I recently raised this issue, that was the question that I asked. Is the entity responsible for aviation, for railroads, for highways, you know, also responsible for this, particularly when reports indicated that they had as few as, I think, four or six people responsible for overseeing this really critical task?

I've been impressed with how they've responded to the call for action but the GAO report clearly showed that there was much more work to do and, I think, particularly stressed having the expertise and the resources in place. I think FERC is making a commitment through our Office of Energy Infrastructure Security to work with TSA to provide that expertise.

Senator HEINRICH. Sure.

Mr. CHATTERJEE. My final point I want to make because it addressed a point Senator King was pressing me on as well, and I just wanted to be clear on this. The authority to impose mandatory standards does currently lie with TSA, and it would take Congress to make that change. I just want to be clear, I wasn't dodging the question but—

Senator HEINRICH. I think we should all be thinking about that question, where the right place is to do this and making sure it is adequately resourced.

Before I let you go, Chairman, I want to get your update on FERC Order 841. What kind of a timeline are we looking at?

Mr. CHATTERJEE. So we've heard from a number of stakeholders that they're waiting for our action on rehearing. We had a comment or a deadline for filings of December the 3rd. These are very, very complex issues. We understand that people want that clarity going forward. My colleagues and I are committed to doing it right and we understand the agita and the desire to get it done. Better to do it right than rushed, but we're working diligently.

Senator HEINRICH. I agree. We do need to get this right, but it is also a pretty urgent matter. It certainly opens up an enormous

amount of economic activity and a resiliency that we need to be supportive of.

I would just, once again, emphasize what an urgently important order that is.

Mr. CHATTERJEE. Yes, sir.

Senator HEINRICH. Thank you, Chairman.

The CHAIRMAN. Thank you, Senator Heinrich.

Senator Hyde-Smith.

Senator HYDE-SMITH. Thank you, Madam Chairman, and thank you so much to the panel and the experts that we have here that is so helpful to this Committee.

I do have a question, Ms. Evans, kind of continuing on the conversation.

We all understand the nature of the infrastructure in the energy sector, and it makes it extremely difficult to deploy cybersecurity protocols that fit every single niche, but are the checklist standards that are applied so broadly to cybersecurity in the energy sector enough to ensure security in mainstream and custom energy applications? And if so, what are the proactive security approaches that are being taken to require more thorough testing in research by qualified agencies or institutions to improve that cybersecurity in the energy section?

Ms. EVANS. Well, I believe based on what my colleagues have talked about here is, is that when we look at what standards are that they are the floor and that that would be the minimum of what you have to do.

If you take a risk-based approach, and you're really looking at what are the consequences for the activities that you have, you'll get to either complying with the checklist or complying with the standard, really understanding what your environment is.

We have cybersecurity research and development which is cybersecurity for energy delivery systems which is our research and development group which is underneath us which is actually taking that question but also leaping ahead and saying how do we skate to the puck, not necessarily think about where we are today but where we want to be in the future.

And then, how do we then test supply chain risk management? How do we then embrace these types of things that have been highlighted today by the members dealing with cars that have computers in them so that you can go and do a lot of different things with your cars, but that's another attack vector.

So I think a lot of the things that we've been talking about in the sense of urgency is how do you raise the cost to our adversaries? Anyone who is in this space, using any type, to your point, there's not going to be a silver bullet here. There's going to be multiple ways but what we really have to do is raise the cost of what everybody is doing because it's too easy for our adversaries to exploit several things.

We've talked briefly about phishing, but that's really a cheap way to get in. That is what our research and development is doing. Then, as the results of that, where we partner with industry, people that are participating in this sector, how do we then share the information out to the right stakeholders because this is all owned by private sector.

The government doesn't own this infrastructure. What we have to do from a national security perspective is share the information so that it can facilitate whether there needs to be a regulation or whether there needs to be a resiliency standard. But they need to benefit from the research and development that the Department is doing.

Senator HYDE-SMITH. Absolutely.

And one other question, if I may, Madam Chairman?

How would you decide what types of non-federal infrastructure should be defined as critical for these purposes?

Ms. EVANS. This is a specific thing that we really are looking at and researching now, to your point.

What we are looking at is through our program called Citrix which is really dealing with supply chain risk management. And this is something that I'm sure my colleague from SEL would also talk about is where has industry gone because you want to stimulate a market economy, right? And you want to have competition and you want to be able to have all those things. So where is the greatest bang for the buck to be able to address what we have today? Where are people investing? But then, how do we then take the information and this is again what we're going to do for the manufacturing institute, is take the knowledge that we get from our labs where they are doing incredible work, and then being able to transfer that out into industry so that industry can incorporate it into their product road maps.

So we do work very closely with the Office of Technology Transfer within the Department so that we can take these things that we are learning here and what is the best way to transfer it back out into the industry so that as people are entering into the energy sector, we know that they are incorporating these types of things so that as our industry partners are buying solutions, they could then say, okay, these things have gone through these types of analysis. If I buy this over this, I'm reducing the risk in my enterprise. That—we are accelerating that and working through that with the national labs to get it out to the industry.

Senator HYDE-SMITH. Based on the critical areas?

Ms. EVANS. In multiple areas because there's current ones that they have to comply with.

So, for example, we're working with Pacific Northwest Lab on a risk-based model because one question that always gets asked by industry is for every dollar I invest, how much risk am I going to reduce?

They have to comply with the CIP standards. So, the risk model is saying, okay, let's look at these attack trees associated with the CIP standards. We should be able to answer that question so that a CEO of a board or a utility or a municipality can say if I do this investment, this is how I can reduce risk.

The national labs have a lot of modeling that's going on, and what I'm trying to do is take that knowledge that they have and use it in a way that the energy sector then has the tools that they need to make those decisions. So that's where we started.

Senator HYDE-SMITH. Great. Thank you so much.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you.

Senator Cantwell.

Senator CANTWELL. Thank you, Madam Chair and Ranking Member Manchin. This has been a great hearing so far. I thought I was just going to come down and say the words, Chairman Chatterjee, and get a little focus there on your new leadership. But, good to see you.

Our colleagues have just been so excellent on illuminating this problem. I could not be more supportive of the concept. I think that we need to do something very, very aggressive here. It is good to see that, from various aspects, people understand that.

Just for clarification, our National Guard is doing red teaming in the State of Washington on utilities. So, it does exist somewhere in this.

But I wanted to get to this question about regulation versus innovation and get your thoughts, Mr. Whitehead. I understand my colleague, Senator Risch, was here earlier claiming that the CEO of your company was a genius and that definitely puts you into a high atmosphere of challenges.

But you understand how important it is, and you mentioned your security clearance. How can we work with everybody here to create that system so that we are not just making up a bunch of things that we want all the utilities to do, and then five months from now, we see a new threat and they are doing this little list that we asked them to do and now there is a new list?

The changing nature of the attacks is really the game, right? It is like the path of least resistance. They are just going to start and as we keep advancing, they are just going to continue.

How do we get this system in place where we are getting the data and information shared and seeing real-time effects of these attacks? Because I feel like that is what everybody on this Committee wants. I think that is why you are hearing the urgency from everybody and now the opportunity is here. How do we really define how to get that communication system?

Mr. WHITEHEAD. Well, thank you, Senator, for the question.

I think there's two parts. There was the innovation versus regulation and from my perspective as a supplier of equipment for the critical infrastructure is there's a lot of reporting up that happens to various agencies but what we don't see then is a lot of reporting back down to us. So, there seems to be a diode or a one-way communication.

I think working with Mr. Robb and other folks, we had a great conversation at breakfast this morning is how do we integrate what we're doing, as a supplier we're not, you know, part of the members of the various information sharing committees. How do we get on to those committees?

I don't think it's hard. And I think we're at a point in the evolution of these information sharing committees where we, as suppliers, critical suppliers, certainly to the U.S. infrastructure, that we have a seat at the table for being able to share that information.

I'd make an argument and I've joked with our folks is I'll stand up a team that's ready to talk, have a phone call at eight o'clock every single morning, 7 days a week, 365 days a year, even if it's a 15 minute phone call that says, hey there's nothing going on or

vice versa, hey, you know, asset owners and suppliers of equipment, this is what you should be looking out for today.

You know, it doesn't have to be a long conversation. I mean, that's one idea that I thought of. I don't think it takes a lot of effort. Certainly, you need to—how you classify your information and who can be on those phone calls. I'm sure there's words or ways to work out those particular scenarios.

But I think it's setting up organizations that can be very quick, very nimble disseminating information. And it can be both ways. I could get on that phone call and say, hey you know what? I had a customer call me up. They saw this weird thing and that could be reported up and shared amongst the community at that level.

Senator CANTWELL. What level of security clearance do you think that is?

Mr. WHITEHEAD. I think it can be all the way from unclassified where it's just hey, look out for this kind of data packet coming where you don't have to attribute to sources or methods of how that came out, just be looking for this kind of traffic, all the way to if you're in this particular area and based on, you know, sources and methods. Maybe some people do need to know that level. But I think it can go scale from all different levels of classification.

Senator CANTWELL. Assistant Secretary Evans or Chairman Chatterjee, what about this other way of looking at this, which is: do we have anything where we are assessing the technology as it exists and focusing more on creating a security standard that we think should be deployed?

For example, I am a big fan of Schweitzer Electronics because they are doing a lot of great work in this area and, I believe, are on some cutting-edge technology. But let's say it's somebody else, some other company, do we have any operation within the Federal Government now, either from the Department or from FERC's perspective, that says we highly recommend the deployment of this technology?

It is almost like the constant hygiene aspect of this problem. And is there a function within our government where we are making the recommendations that these things be deployed more rapidly or is somebody just making the judgment call that this is where we need to be?

Ms. EVANS. So, the heart of the issue of what you're talking about is the innovation while you're maintaining the existing environment. And so, yes, that environment exists. And we've talked about it briefly, but it is with the Electricity Subsector Coordinating Council, the Government Coordinating Council which is all of the whole of government approach as well as the Oil and Natural Gas Subsector Coordinating Council.

So we specifically, as the Department of Energy, my research and development program underneath me looks into the future, like evaluating equipment. That's what we're doing from a supply chain risk management.

The Department itself, our OCIO function looks at this as well because we have the PMAs also in there.

When we take a risk-based approach as a Department based on, for example, we had to do Kaspersky but there are other things that we know based on the current environment and the IT world.

We share that out with the sector and say, look, the Department has taken this approach based on these types of things. We do it at a classified level. We also attempt to do it at an unclassified level.

I will share one thing that, maybe, the Committee would want to think about this going forward is as we have shared what the Department is doing one of the issues that has been raised up from the sector as a whole is, is that as they look at it to take an action as a collective against this to not, say for example, they did not do something with a specific company that is in this sector, one of the issues that they have raised is the potential of an anti-trust type of issue that would come against the sector as a whole because they were taking a risk-based approach.

Senator CANTWELL. This is why I am interested in whether we have the function within the Federal Government because look, we all travel, and guess what we do if we are going to travel somewhere? We look online and say, well, what are the threat assessments of traveling to that region of the world—and it is posted there.

So what I am interested in is the issue about the regulatory side taking a long time, and the challenge here is that it is constant and evolving.

What we want though is some part of the Federal Government that says, oh, yes, these software-defined network (SDN) solutions should be deployed. We are not even saying whose, just that these are five solutions we think all utilities should be deploying if they want the hygiene of their networks to be state-of-the-art or—

Again, I know that gets a little tricky, but at the same time, I just feel like this is what we are trying to do in the State of Washington. We are trying to use the National Guard and a coalition of people to define what the state-of-the-art hygiene is to make people's systems secure.

I would just think if we are going to stay out of whatever we think is the—I am where my colleague from Maine is and that is that with the evidence as clear as it is, we need to do a lot more.

But one thing we need to do a lot more on is to start having the Federal Government define what is the state-of-the-art technology that they think utilities should be deploying, even if it is a recommendation and not mandated.

Ms. EVANS. Absolutely.

Senator CANTWELL. But I think we are over here researching and exploring and I just feel like we should be upgrading the checklist of things that people should be doing at least every six months.

Ms. EVANS. I would say that we, that the Department and the Secretary's viewpoint is in line with what you are suggesting, that is what we view for the long-term play with the Advanced Manufacturing Institute.

But in the short run of what we are doing is how my office is going to do that evaluation, work through the programs that we have and the intent is for us to publicize from a voluntary perspective, looking at everything that has been envisioned up on this Hill is if you voluntarily participate over here and we have NIST and we have all these other things, here is the information about these programs. Here are things of how you can make an informed deci-

sion. That information would feed into this. We are specifically looking at these are the specific systems and components that are built into the current infrastructure.

The other effort that the Department is doing is through the Grid Modernization Initiative and the GMLC, which is Grid Modernization Lab Consortium, because a lot of the information that you're talking about, they develop. Then how do I then transfer that out and say these are the best practices? This is how you can do it. This is how you can leap ahead.

We just had a briefing yesterday on an initiative that has been three years in the making that is really going to help leap ahead the industry as a whole. And now we're figuring out what's the best way to get it out into industry so that the E-ISACs and the industry as a whole can use it.

Senator CANTWELL. Alright.

Madam Chair, I know my time is expired.

The CHAIRMAN. Thank you, Senator Cantwell. You have always pushed the Committee to focus on these cyber issues and your leadership on this is greatly appreciated. Thank you.

Senator Hoeven.

Senator HOEVEN. Thank you, Madam Chairman.

Mr. Robb, how do you answer the question when somebody says, is our energy infrastructure, is our grid, safe and secure from cyberattacks? How do you know? Are we safe? How do you know?

Mr. ROBB. Senator, it is the issue that keeps us all up at night. And what I can represent very confidently is that the industry takes this threat very, very seriously. We have, through the mandatory cyber critical infrastructure protection standards, we've a very strong foundation of defense in the grid. We can always do better on the information sharing and analysis of emerging attack vectors and so forth to build real-time situational awareness and defense of specific threats, but the foundational security of the grid in this country is very, very strong.

Senator HOEVEN. How do you know?

Mr. ROBB. Because we have mandatory standards in place. We audit the utilities against those standards and they're subject to a financial penalty if they are found in violation of those standards.

Senator HOEVEN. How do you make sure on the one hand you are integrated, but on the other hand if there is a problem somewhere it does not invade the whole system?

Mr. ROBB. One of the great design features of the North American Electric Grid is that it's sectionalized in many ways and the whole purpose of the standards is to ensure that if something bad does happen to some part of the grid, that it's contained and does not propagate across it. So that if an incident did occur in New Jersey or something like that, it stays there, right, as opposed to compromising the entire system. That's the whole design principle of the reliability standards we have.

Senator HOEVEN. Do the participants in the grid, writ in large, have the ability both to participate but also to protect themselves from a threat that might enter the system?

Mr. ROBB. I'm sorry, I didn't catch the question, sir.

Senator HOEVEN. For all the participants in the grid, do they have both the ability to be integrated and operate interoperably but

also the ability to segregate themselves, if necessary, in the case that there is some type of virus or other threat or problem?

Mr. ROBB. Yes, sir, they do.

Senator HOEVEN. And you are able to check that and verify it? We are not guessing like some of the financial hybrids before the market meltdown?

Mr. ROBB. No.

Senator HOEVEN. All the regulators thought that, didn't they? Remember, they all said all those financial hybrids, they had risk management all squared away? But it didn't work. So how do you know?

Mr. ROBB. Well, there's always potential for a failure in any complex system. What I can say is that the standards that are in place with which industry must comply and again, subject to audit and penalty if not, provide that base level of security and support.

Senator HOEVEN. And you feel the regulatory oversight and the audits are sufficiently transparent, understandable and so forth that it is verified, that we do have that security in place and if there is a weakness it is identified in a timely way?

Mr. ROBB. I believe so, sir.

Senator HOEVEN. Can be addressed?

Mr. ROBB. Yes.

Senator HOEVEN. Mr. Chatterjee, good to see you again.

Mr. CHATTERJEE. Good to see you, Senator.

Senator HOEVEN. Based on your new role and your years of experience here on the Hill, have you seen any legislation out there that you think would be most helpful in this cybersecurity area that we should be advancing or do you know any concepts for legislation that you think we ought to be advancing that could, that would help and be beneficial?

Mr. CHATTERJEE. I think, and I mentioned this earlier, you know, the workforce issues are critical. Finding cyber expertise, dealing with information sharing is essential to this and identifying that workforce, all of us making this societal investment and making sure people are educated.

There's been a lot of talk about cyber hygiene and the vulnerabilities within organizations tend to be driven by human beings in this space, and we saw some of the supply chain issues that arose as a result of that.

And so, I think anything we can do to get expertise on this area throughout the country, throughout stakeholders in industry, and I understand there's a bill regarding a federal rotational cyber workforce program, introduced by the Senator from North Dakota. I'm certainly supportive of that concept, because it is hard to find and train good employees.

Senator HOEVEN. You have not lost your touch.

[Laughter.]

You are a good man.

And certainly, getting our noms through and getting positions filled would be helpful too, wouldn't it?

Mr. CHATTERJEE. Yes, sir.

Senator HOEVEN. That would be beneficial, right?

Secretary Evans, being a northern border state, obviously, we work with Canadians all the time. We love them. Greatest ally

ever. How do we make sure that we are managing the cyber risks and threats across border in a good, solid, integrated way?

Ms. EVANS. Sir, we do work in partnership with NERC. I'm so glad we can say NERC, instead of saying the whole name. And so, we do work in partnership with them. I know the Canadians actively participate in that.

The Office of Electricity also is working on what the, I want to make sure I get the NAERM right, which is North American Energy Resiliency Model, of how that is all going to play across the board.

Senator HOEVEN. Yes.

Ms. EVANS. That does involve our Canadian partners in that as well.

Again, it's making sure that we can share the information with them. They are our allies. We need to make sure that we can share the information and that we understand the shared risk.

I would also go back to some of your questions about how do we know?

The reason why we do the exercises and, again, all of us have talked about the exercises, is because we think we have the best plans in place until we have to actually exercise them.

Senator HOEVEN. Right.

Ms. EVANS. And so, the exercises really point out if we have any weaknesses so that we can identify that that's why our partners here talk about several of the exercises that we participate in so that we can highlight that because we don't want to get into that situation of now we're in a crisis and we find out we don't have the best plan.

Senator HOEVEN. Is there any legislation vis-à-vis Canada that you have seen that is helpful or that is on your screen?

Ms. EVANS. I believe the way that the Hill is looking at this in multiple different ways. There are things that you are talking about from the workforce perspective that is very helpful. That's been outlined already by Chairman Chatterjee.

The things in supply chain risk management and how you're looking at that and giving us the longer-term view of how we need to put those programs in place would allow for us to do that.

And I think the industry and I would share this with my colleagues if they have any insight into that, but what I hear often is, is that they want to make sure the bidirectional happens but they are concerned as they continue to move through this and we get into very interactive information sharing that the proper protections are in place as they take actions as a collective.

Senator HOEVEN. Thank you.

The only other thing I would offer is Major Keber, thanks for your service. We appreciate it.

Thank you, Madam Chairman.

The CHAIRMAN. Thank you, Senator Hoeven.

Just a couple quick things. I know we are wrapping up. I know that Senator King wanted to add on.

I wanted to just go a little bit further. Senator Cantwell raised the same issue that I had raised initially with you, Mr. Whitehead, in terms of innovation versus regulation and the inherent conflict there.

We have had a lot of discussion about the mandatory standards we have in the electric sector. We are the only ones here that have mandatory and enforceable cyber standards, and we know what the violations can lead to.

We had a witness here before the Committee last year, a gentleman by the name of Rob Lee of Dragos. He was a hands-on cyber expert. He suggested to us that utilities are perhaps overly focused on the legal aspects of compliance and sometimes these mandatory NERC standards that basically cause you to check the box to make sure that you are meeting the standard, that is, focus on compliance rather than the creativity, the innovation that we need in order to do all this. We are going to use our limited bandwidth because we have talked about the fact that we do not have enough people in this area that are the smart, forward-thinking, leaning-in brains to make this happen. So we set our resources to just the compliance side. He actually suggested a three-year cooling off period to let the utilities focus on cyber threats instead of, he called, the cyber lawyers.

Comment on that, if you will, Mr. Robb and Mr. Whitehead.

Mr. ROBB. Sure.

So, I hear that a lot. I'm not sure I believe it. For the most part the standards that we have in place for cybersecurity don't require any unnatural acts. They really codify what good utility practice is in these spaces.

And I think the fact of the matter in the conversations that I always have with the CEOs, and I believe that the CEOs of organizations get this, that a secure operation is going to be compliant with the standards that we have in place. It's not really an either/or. It's a yes/and.

Again, when I look at the number of violations that we have of CIP standards and the root causes, they typically result, the root causes are typically on things like management culture and so on and so forth. So that, there's really a lot that the CEOs can do to drive a secure and compliant organization. They work hand in glove. It's not a tradeoff that someone has to do x or y. And if that tradeoff is ever presented, our advice to the entities is always do what you need to do to be secure, and we'll deal with the compliance aspects later. And if there's something silly in the compliance world, we'll deal with that in an appropriate way.

The CHAIRMAN. Mr. Whitehead.

Mr. WHITEHEAD. Yeah, I'll have a little fun with Mr. Robb for just a second as I think you can—

[Laughter.]

—it's okay—I think you can be compliant but not necessarily secure, right?

The CHAIRMAN. Right. My point.

Mr. WHITEHEAD. People can check all the boxes and you could still have a challenge or an issue.

So you always have to be careful. I think that's what, I know Rob pretty well, Rob Lee. I think that's what he was really alluding to is that what you want to make sure is that you're not stifling creativity or taking the responsibility out of somebody really thinking about what they're doing, right?

Just filling in checkboxes is not going to make you secure, maybe it makes you compliant, but it's not going to make you secure. So requiring people or certainly giving them the ability to think about how their particular situation, their particular networks, their particular critical infrastructure is designed and operating and then how security overlays on top of that, I think, is the critical aspect to keeping our assets all secure. I think that's it.

And Senator Cantwell, thank you for SDN. One word of caution, SDN is a great technology. We've got solutions for it. What I like the idea of is that hey, the government is saying this is a great technology, Mr. Utility, you should look at this. What I would hate though is to say, Mr. Utility, you have to deploy this technology because I've got 800 engineers back in Pullman coming up with the next greatest thing and I would hate to say, you know what, everybody has to focus on SDN when we've just come up with a great new solution for protecting our critical infrastructure.

The CHAIRMAN. Thank you for that.

Senator King, you wanted to jump in?

Senator KING. Please.

Chairman Chatterjee, I know it just slipped your mind. You wanted to mention to Senator Hoeven S. 174, the Risch-King bill, as an important step in the right direction. Would you say yes to that?

Mr. CHATTERJEE. I would absolutely say that additional R&D about possible defenses is always helpful, and I very much encourage those efforts.

Senator KING. Thank you. I appreciate that.

Madam Chair, I just wanted to make a final point on this issue.

All we have been talking about today is protecting ourselves, patches, standards, hygiene, all of those kinds of things. The missing part of this discussion, and it is true governmentwide, is deterrence. Our adversaries who are attacking us in this way, thus far anyway, have not felt that there was a price to be paid for those attacks, that we were a cheap date.

That part of what we have to develop and this is going on in a number of different forums over the next year or so and indeed the Administration has produced some good work on this, but we need to be talking about how we make, how we change the calculus for our adversaries when they decide to venture into our electric grid or our gas pipelines, that there will be a price to be paid? It may be cyber. It may be sanctions. It may be other kinds of responses. But thus far, there has not been a doctrine or a strategy in this country that deters these kinds of attacks as there is in other areas of our national security.

So I would just point out that we will never be able to patch our way out of this threat. We would be like a boxer who was really skilled at ducking and bobbing and weaving, but if you can never punch back, you are not going to win the fight.

I just want to mention that as a larger background issue that is involved in this question, whether it is this kind of cyberattack, a cyberattack on our election system, or any other intrusion of that kind, our adversaries have to begin to realize that there will be a cost to them for attacking this country in this way. Until they do

so, they are going to continue to do it, as they have over recent years.

Thank you.

The CHAIRMAN. I certainly concur it is an important part of it, and I think we want to be in the position that we are not reactive in this deterrent aspect, that we have made quite clear from a proactive perspective that there are consequences.

Senator Cantwell.

Senator CANTWELL. Yes, Madam Chair, if I could just quickly.

I don't know if we have put our finger on it this morning yet but I do think, to Mr. Whitehead's point, yes, we want to keep innovating. That is the challenge. We want to keep innovating.

I do not even know if there is a private sector Good Housekeeping seal that somebody is putting on for utilities. I think that is the key, right, is that and, at least as it relates to the FERC role and the agency roles, is are there entities out there that are doing their job and doing their best?

At the same time, as you said, you are going to develop, your engineers are going to—first of all, the threat is to keep up on them.

So I certainly agree with you, Senator King, that there is a lot that we should be doing on an international basis to basically stop the arms race that is happening on cyberattacks. And we should be joining other nations in promulgating—we should be spending as much time on this as we are on this discussion because if we were, I guarantee you, we would get someplace.

This security is critical, and we have to get other nations to say that you do not tolerate these kinds of actions by governments and you basically are going to stop people from engaging them.

But anyway, back to this. I just think we need more discussion about, Madam Chair, what kind of rapid response system can we establish, and how do we know when we get to a point where we really think people should deploy something we think is viable—without representing a software state—is an ongoing discussion.

I think from the consumer perspective they are like, oh, another upgrade, and I am supposed to do that? Yet, every upgrade really does get us a greater layer of security. That is what each system does. Not that it does not have problems with it, it too has bugs. I just think we need to keep talking about how we establish this communication back to the government about what we should be deploying. I think it is tricky and hard, but I don't think it is impossible.

I think having all that information flow on a constant basis would be very helpful to making us more—again, a few bobs and weaves would not hurt us right now while we are getting this larger thing in place.

Thank you.

The CHAIRMAN. Thank you, colleagues, and thank you to the members of the panel. I think it has been a very interesting discussion, a very important discussion.

But I do harken back to Senator McSally's comments that she could close her eyes and this could have been the same conversation 19 years ago. We do not want to be sitting here or have those who follow us 19 years from now be sitting here asking "what were they doing in 2019 here?"

There is a heightened sense of urgency for action. It has to be coordinated. We have to recognize that here in Congress we have jurisdictional issues that we wrestle with. We have to figure out those issues just as it needs to be figured out in our agencies and in the private sector. There is simply too much on the line.

We appreciate all the engagement. We look forward to FERC's technical conference and the continued, very important dialogue.

With that, the Committee stands adjourned.

[Whereupon, at 12:08 p.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Responses to Questions for the Record Submitted to the Honorable Neil Chatterjee

Questions from Chairman Lisa Murkowski

Question 1: Next month FERC and DOE will co-host a conference on “Security Investments for Energy Infrastructure.” Among other issues, the conference will explore how FERC can incentivize needed investments to improve the cybersecurity of our electric grid and gas pipeline system.

- What options does FERC have to encourage additional cybersecurity investments?

Response: The Commission has statutory authority to allow entities the opportunity to recover prudently incurred costs for security investments. Specifically, the Commission’s current cost-recovery policies provide the opportunity to recover security investments for electric transmission and pipeline infrastructure, including cybersecurity investments, as a matter of course. The Commission also has authority to provide for, and has taken a number of additional steps to allow, recovery of such investment costs, including:

- The Commission allows utilities to utilize formula transmission rates that permit the recovery of infrastructure security costs as they are incurred, without the need to make an additional filing for approval to do so.
- The Commission has identified and granted pre-approval for the implementation of multiple innovative rate treatments that allow utilities the opportunity to recover security-related expenditures in their rates.
- Under the Commission’s statutory authority to provide incentives to encourage efficient investment in critical transmission infrastructure security, the Commission has issued multiple orders that specifically address those investments.
- The Commission has statutory authority under section 219(b)(4)(A) of the Federal Power Act (FPA) to ensure registered entities have the opportunity to recover prudently incurred costs necessary to comply with mandatory reliability standards adopted pursuant to section 215 of the FPA.

Importantly, the Commission also coordinates with other federal agencies with security authority to encourage regulated entities to take steps to address security issues. This coordination may result in those entities making investments to protect critical transmission infrastructure security. As discussed above, those entities have the opportunity to recover the costs of cybersecurity investments in their Commission-jurisdictional rates.

The Commission’s upcoming March 28, 2019 technical conference on security investments will explore, among other things, how security investments are presently incentivized, and what type of incentives would be most effective to facilitate security investment.

U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Responses to Questions for the Record Submitted to the Honorable Neil Chatterjee

- Do current cost recovery policies discourage or otherwise limit these investments in any way?

Response: I do not believe that the Commission's current cost recovery policies discourage or limit cybersecurity investments. As noted above, the Commission currently provides the opportunity to recover prudently incurred investments in critical infrastructure security, including cybersecurity. However, I believe that we should continue to engage with industry and our federal and state partners to ensure that the Commission is taking all necessary steps to facilitate appropriate cybersecurity investments.

Question 2: In the FAST Act, Congress strengthened protections for the sharing of information with the federal government as well as state governments by providing Freedom of Information Act (FOIA) exemptions for Critical Energy Infrastructure Information (CEII).

- How important have these FOIA exemptions been? Have they resulted in a greater exchange of information between the federal government and the utility sector as intended?

Response: While the Commission provided CEII to and received CEII from entities on an as needed basis prior to the FAST Act, the FAST Act exemptions provide the Commission and third parties with greater certainty that any exchanged CEII is protected from both state and federal mandatory public disclosure laws. This increased degree of certainty has resulted in a more dependable exchange of information between the Commission and the utility sector.

- The energy sector has expressed concerns about the ease at which persons can obtain CEII by merely signing a non-disclosure agreement with FERC. Do you agree that this is a security gap? If so, are you considering tightening FERC's disclosure policies?

Response: Since the Commission instituted its CEII request and approval procedures in 2003, the Commission has required requesting parties to execute a non-disclosure agreement (NDA). The Commission is not aware of any instances of an intentional breach of an NDA.

I appreciate that NDAs alone are not necessarily sufficient to prevent the misuse of CEII, especially by those intent on malicious action, which is why the Commission's regulations provide additional tools to prevent improper disclosures. Under the Commission's regulations, a requester receives CEII only after the Commission determines that the requester is legitimate and that its need is valid. In addition, the Commission's regulations allow the Commission to impose additional conditions on a requester's access to the CEII above and beyond what the standard NDA requires. Further, in the event an NDA is breached, the Commission has the authority to

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Responses to Questions for the Record Submitted to the Honorable Neil Chatterjee

impose sanctions and prohibit a requester from receiving CEII in response to any future requests. Finally, an individual who purposely falsifies a request for CEII could be subject to criminal prosecution under 18 U.S.C. § 1001.

Question 3: On an annual basis, FERC requires many electric utilities to submit data to the Commission on their power grid operations in FERC Form No. 715. Not only does this form require a utility to submit “maps and diagrams” of the grid, but actual grid data in electronic format is also required. FERC acknowledges that this data is CEII and treats it as such.

- I understand that FERC’s policy is to release that data to the public on the basis of the public’s “right to know.” While I am in favor of transparency, CEII is sensitive information and protected from disclosure under FOIA. Do you consider the release of this data a security gap? Should FERC consider changing its policy regarding the release of CEII to a “need to know”?

Response: Under 16 U.S.C. § 824l(b), Congress directed the Commission to “promulgate a rule requiring that information be submitted annually to the Commission by transmitting utilities which is adequate to inform potential transmission customers, State regulatory authorities, and the public of potentially available transmission capacity and known constraints.” The Commission created Form No. 715 in 1993 in response to that Congressional directive. Prior to September 11, 2001, this information was routinely available in the Commission’s public files. Shortly after September 11, 2001, the Commission created the CEII designation and treated the information submitted under Form No. 715 as CEII. In addition, the Commission took steps to control the distribution of information designated as CEII, including removing documents from its public files and eLibrary database that were likely to contain detailed specifications about critical infrastructure.

In November 2016, the Commission revised its CEII regulations to implement provisions of the FAST Act. Under the Commission’s regulations, an entity requesting CEII must show “a particular need for information designated as CEII.” The regulations also state that “[t]he CEII Coordinator will balance the requester’s need for the information against the sensitivity of the information.” Requesters seek CEII for a variety of purposes. For example, requesters include individuals whose land is impacted by proposed energy infrastructure so they may learn of the proposals; resource developers seeking to identify suitable locations for generation interconnections; and existing utilities to analyze potential transmission capacity and system constraints, conduct economic modeling, and verify transmission data. The Commission balances the legitimate need for access to Form No. 715 data with the responsibility to safeguard CEII through the Commission’s CEII regulations and procedures. As noted in my response to Question 2 above, the Commission has implemented mechanisms and safeguards to address any improper disclosure of CEII.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Responses to Questions for the Record Submitted to the Honorable Neil Chatterjee

- Does FERC do any monitoring over how members of the public use this CEII information after they receive it? If not, why not?

Response: In Order No. 833, the Commission indicated that it may audit the recipient's compliance with the NDA. However, to date, the Commission has not found any actual instance in which a signatory has breached the NDA. In those instances where the Commission has received an allegation of breach, staff has reviewed the circumstances and determined that no actual breach had taken place. Accordingly, the Commission has not observed any instances of conduct that suggest additional monitoring is necessary at this time.

Question 4: DOE has its Cybersecurity Risk Information Sharing Program and NERC has the Electricity Information Sharing and Analysis Center and the Department of Homeland Security has its National Cybersecurity & Communications Integration Center.

- Do we need all these programs?

Response: Each of these agencies and programs fulfill a different mission in sharing information. The Department of Homeland Security (DHS) serves all of the critical sectors and has the broadest view of incidents across all sectors. The DHS National Cybersecurity & Communications Integration Center (NCCIC) serves as a hub of cyber and communications information, providing a classified environment for federal agencies and industry experts to view current threats across sectors in real-time while also defending federal networks and responding to significant incidents.

The Department of Energy (DOE) serves as the sector-specific agency for the energy sector, including oil, gas, and electric distribution. DOE works closely with other federal agencies, such as the Commission and those in the intelligence community, to identify threats and determine effective mitigation measures. DOE also works with the North American Electric Reliability Corporation's (NERC) Electricity Information Sharing and Analysis Center (E-ISAC) to receive Cybersecurity Risk Information Sharing Program (CRISP) data from industry to focus on the electricity subsector. The E-ISAC serves all vetted electricity owners and operators in North America and allows for a place to share information openly without regulatory compliance concerns. As part of that role, the E-ISAC administers CRISP and facilitates the exchange of cybersecurity information between industry, E-ISAC, and DOE on a voluntary basis.

The Commission has acknowledged the value of these organizations. For example, it directed NERC to improve cyber-incident reporting and to share this information with DHS's NCCIC and NERC's E-ISAC. Additionally, the Commission coordinates with NERC's E-ISAC to review

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Responses to Questions for the Record Submitted to the Honorable Neil Chatterjee

industry alerts prior to their issuance. The Commission also temporarily assigns staff to the NCCIC to coordinate with other energy industry and cross-sector participants.

- How well do they coordinate? In particular, are they sharing responsibilities and minimizing duplicative overlap in a productive way?

Response: I am unaware of any issues regarding coordination between DOE, NERC E-ISAC, and DHS NCCIC. These organizations would be better able to answer this question.

Question 5: As you know, one of the best ways to be prepared for an attack is training.

- What type of cyber training are the operators in our control rooms receiving? Is it sufficient?

Response: NERC's Critical Infrastructure Protection (CIP) Reliability Standards require operators of the Bulk Electric System to implement informational security awareness programs. These security awareness programs, which operators must perform at least once each calendar quarter, reinforce cybersecurity practices (which may include associated physical security practices) for the operators' personnel who have authorized electronic or authorized unescorted physical access to Bulk Electric System Cyber Systems. The CIP Reliability Standards also require operators to implement formal training programs that must be completed every 15 calendar months on various aspects of cybersecurity, including cybersecurity policies, physical access controls, electronic access controls, and visitor control programs. Commission staff has observed some of these training programs, which provide operators' personnel with an understanding of threats, vulnerabilities, tactics-techniques-procedures used by attackers, and how to recognize an event. Additionally, operators' personnel participate in exercises related to cyber and physical events. The CIP Reliability Standards provide a baseline that requires operators to regularly drill and train their personnel to help protect the reliability of the grid.

- Is this training reaching down to all grid operators? Or is it only reaching the biggest companies with the greatest resources?

Response: The CIP training requirements apply to all operators of the Bulk Electric System, regardless of the size of the entity. I note, however, that by law the CIP requirements do not apply to operators of local distribution systems.

- Since the Ukraine attacks are real-world events where control room operators were forced to handle an attack, are the lessons learned about Ukraine being taught in training classes here in America?

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Responses to Questions for the Record Submitted to the Honorable Neil Chatterjee

Response: NERC released a recommendation to industry titled “Mitigating Adversarial Manipulation of Industrial Control Systems as Evidenced By Recent International Events” in February 2016, which shared techniques observed in the December 2015 attack on Ukraine’s electrical system. In addition, Idaho National Laboratory held a series of Cyber Strike Workshops intended to translate real-world cybersecurity events, such as the Ukraine events, to protect utilities in the United States. The Commission has also assisted the Office of the Director of National Intelligence (DNI), DOE, DHS, Federal Bureau of Investigation (FBI), and others to conduct further sessions with industry and state officials to inform them about the threats and mitigations from these events.

Question 6: While the federal government regulates wholesale sales and transmission of electricity, the states regulate the local distribution networks that deliver power to individual homes and businesses. How does the federal government coordinate with the states to ensure that distribution-level facilities remain protected against cyber threats that could impact the larger electric grid?

Response: Through the Commission’s Office of Energy Infrastructure and Security, the Commission works closely with other federal agencies, state partners, and industry to provide cybersecurity threat briefings to state partners and to assist with the development and identification of best practices that the states may consider for cybersecurity risk mitigation. As part of these efforts, the Commission has worked and continues to work with DNI, DOE, DHS, FBI, and others to help support key cybersecurity initiatives. In addition, the Commission has assisted the states with the development of cybersecurity materials such as threat assessments, recovery plans, state action plans, and training programs. The Commission has also assisted with table top simulations and exercises for cyber and physical security attacks to help the states prepare and react to events within their jurisdictions. Further, the Commission has included state representatives when conducting individual cybersecurity assessments of energy infrastructure.

Questions from Senator Bill Cassidy

Question 1: What additional strides still need to be taken to ensure federal agencies are appropriately identifying critical infrastructure and facilities and taking necessary steps to help the private sector mitigate against the cyber threats we face in 2019?

Response: The Commission works closely with other federal agencies, such as DHS, FBI, and the Nuclear Regulatory Commission, as well as NERC, trade organizations, and utilities to understand cyber threats, learn how utilities protect their networks, assess the effectiveness of the CIP Reliability Standards, and gather feedback on how improvements can be made.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Responses to Questions for the Record Submitted to the Honorable Neil Chatterjee

Further, the Commission will continue to support DOE, DHS, DNI, the Transportation Security Administration, and others to identify energy infrastructure facilities that, when disrupted, can cause regional or national effects on public health or safety, economic security, or national security. The appropriate protection and recovery plans can then be identified for further action.

Question 2: In the absence of transferring authority, what opportunities for improved synergies between FERC, PHMSA, TSA, and CESER do you believe exist?

Response: The Commission continues to work collaboratively with other federal agencies, the states, and the owners and operators of energy infrastructure to identify and address matters of mutual concern, including the security of natural gas pipelines. As an example, the Commission, TSA, the DHS National Risk Management Center, and DOE's CESER have announced a joint pipeline cybersecurity initiative to conduct assessments to get a broader understanding of the risks facing natural gas pipelines. Joint efforts like this allow our agencies to leverage our resources and expertise to better understand the threat landscape and direct more targeted and prioritized risk management activities.

Question from Senator Martin Heinrich

Question: After our intelligence community issued repeated warnings about the threat of using Huawei equipment, the FCC moved last summer to block Huawei products from being used on our communications network. The Congress later prohibited U.S. government communications systems from using Huawei equipment. Now Huawei is selling advanced power inverters and control systems to be used on our electricity grid, particularly in utility and residential solar markets. Does FERC have the same concerns about Huawei equipment being used on our electricity grid?

Response: The Commission relies on the federal intelligence community to determine risks to its jurisdictional infrastructure from supply chain threats. DOE, as the sector specific agency for energy, is the intelligence community member responsible for receiving and analyzing these threats. The Commission is currently coordinating with intelligence agencies, including DOE, on this and other matters related to the security of the electric sector supply chain.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

QUESTIONS FROM CHAIRMAN MURKOWSKI

- Q1. For several months now, you have been in in charge of DOE's newly created Office of Cybersecurity, Energy Security, and Emergency Response (CESER).
- Q1a. Do you think that CESER is accomplishing its goals of strengthening cybersecurity preparedness and coordinating cyber incident response? What more needs to be done?
- A1a. As the Sector-Specific Agency (SSA) for the energy sector, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is undertaking several efforts to enhance cybersecurity preparedness across the sector. CESER works closely with the Department of Energy (DOE) Office of Intelligence and Counterintelligence to hold regular threat briefings for industry partners, including monthly classified briefings with the Electricity, Oil & Natural Gas, and Downstream Natural Gas Information Sharing and Analysis Centers (ISACs). These meetings provide awareness and context of the latest threats facing the energy sector, leveraging DOE's subject matter expertise, and are an opportunity to discuss and develop potential mitigation measures to be shared with the broader sector. In addition, CESER recently developed Analysis of Risks in the Energy Sector (ARES) reports, in collaboration with DOE's Office of Intelligence and Counterintelligence, to share timely and actionable unclassified cyber security threat information with the energy sector through trusted channels.

CESER also continues the development and execution of programs to help enhance cybersecurity preparedness across the sector. CESER's Cybersecurity Testing for Resilience of Control Systems (CyTRICS) program is a central capability for DOE's efforts to increase energy sector cybersecurity and reliability through testing and enumeration of critical components to identify embedded cyber vulnerabilities. CESER continues to move forward on the goals outlined in the DOE Multi-Year Plan for Energy Sector Cybersecurity, including accelerating game-changing research and development to mitigate cyber incidents in today's systems and to develop next-generation resilient energy delivery systems while developing analyses to quantify the resulting relative risk reduction. Another effort that supports this goal is our continued engagement with the

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

Cybersecurity Risk Information Sharing Program (CRISP), which is managed by the Electricity Information Sharing and Analysis Center (E-ISAC). The most tangible effort within that engagement funded by DOE is the +30 initiative, for the inclusion and provides coverage of additional entities. Finally, CESER has also been developing the Cyber Analytics Tools and Techniques (CATT 2.0™) sensor agnostic program, which will allow a more robust analysis of threats, significantly reduce the cost to utilities, and enhance information sharing with industry in a timelier manner.

CESER has been working with the Department of Homeland Security, the Federal Bureau of Investigation, the U.S. intelligence community, and the National Security Council to clarify roles and responsibilities during a cyber incident and ensure unity of effort across the interagency. CESER hosts and participates in a variety of exercises, with both industry and interagency partners, to understand gaps and refine coordination procedures. These efforts support a whole-of-government approach and are aligned with the Administration's National Cyber Strategy that directs the clarification of roles and responsibilities of Federal agencies.

Strengthening the cybersecurity of the energy sector will be a continuous effort as threats continue to advance. CESER will need to continue to provide regular information and threat briefings to industry partners, improve platforms for information sharing, and invest in new research and development to mitigate threats and analyze information.

- Q2. Under the FAST Act, DOE has authority to issue emergency orders to industry for grid security emergencies. The effectiveness of this authority will require close coordination with industry and NERC.
- Q2a. What is the status of DOE's work with industry and NERC to ensure this coordination?
- A2a. DOE issued procedural regulations concerning the Secretary of Energy's issuance of an emergency order following the President's declaration of a Grid Security Emergency, under the Federal Power Act, as amended. The procedures can be found in 10 CFR Part 205 and have been reviewed by stakeholders through public comment and other forums.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

DOE regularly works with NERC. One example of this coordination is through exercises like NERC's Grid Security Exercise (GridEx) series. GridEx simulates a cyber and physical attack on electric and other critical infrastructures across North America. DOE is a participant in the biennial GridEx exercise series.

- Q3. I understand that there are many people in industry awaiting security clearances – what can be done to expedite this process?
- A3. DOE and private energy sector personnel, through the Department of Homeland Security (DHS) Private Sector Clearance Program, both depend on the Office of Personnel Management's (OPM's) National Background Investigations Bureau (NBIB) to perform background investigations for clearances and we defer to OPM for ways to expedite the process. The transfer of NBIB from OPM to the Department of Defense to help alleviate the issue in the future is still ongoing.
- Q4. While the federal government regulates wholesale sales and transmission of electricity, the states regulate the local distribution networks that deliver power to individual homes and businesses.
- Q4a. How does the federal government coordinate with the states to ensure that distribution-level facilities remain protected against cyber threats that could impact the larger electric grid?
- A4a. CESER leads the Department's efforts to secure our Nation's energy infrastructure against hazards, reduce the risks of and impacts from cyber and other disruptive events, and assist with restoration activities. The office works closely with the private sector, as well as Federal, state, local, tribal, and territorial government partners, to enable more coordinated preparedness and response to cyber and physical threats and natural disasters. As the Sector-Specific Agency for the energy sector and for cybersecurity in the energy sector, DOE takes seriously its role in coordinating with intergovernmental communities. Through the state and local representative membership organizations with an energy security focus, including the National Governors Association (NGA), National Association of Regulatory Utility Commissioners (NARUC), National Association of State Energy Officials (NASEO), National Emergency Management Association

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

(NEMA), National Conference of State Legislatures (NCSL), and the American Public Power Association (APPA), CESER supports the development of resources, including guidance and workshops, to advance energy security planning and response to cybersecurity threats.

For example, DOE's Cybersecurity Capability Maturity Model (C2M2) is a public-private partnership effort established as a result of the Administration's efforts to improve electricity and oil and natural gas systems cybersecurity capabilities and to understand the cybersecurity posture of the grid. C2M2 helps utility organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity capabilities. The model is based on and also supports the adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. To complement C2M2, CESER is working with NARUC to develop a framework to ensure public utility commissioners know what questions to ask of utilities when determining their cybersecurity posture and evaluating the answers they receive.

Another example is the Viking Shadow Midwest Regional Energy Assurance Workshop that NASEO hosted in July 2018 in Minnesota, during which 15 state energy officials, emergency managers, and public utility commission staff assessed their preparedness and response capabilities to a fuel disruption and a cyberattack impacting the electricity, petroleum, and natural gas sectors. The key findings included the need to make energy security and assurance plans more actionable and to provide more training. This was the impetus for CESER initiating an online training program in Fiscal Year (FY) 2019.

Threat information sharing is also an important part of ensuring that distribution-level facilities remain protected against cyber threats that could impact the larger electric grid. DOE and the Department of Homeland Security are preparing a work plan to host quarterly threat briefings for cleared energy-focused state officials and industry representatives on a regional basis to share information on the threat landscape in the energy sector.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

All of CESER's projects at the state, local, tribal, and territorial level are shared with, and informed by industry, in the interest of cross-collaboration.

- Q5. With the Secretary of Energy designated under the FAST Act as the lead cyber official for energy security, military and other agencies should be reaching out to DOE for coordination.
- Q5a. How well is the government coordinating its efforts on energy security?
- A5a. As the Sector-Specific Agency for the energy sector and for cybersecurity in the energy sector, DOE leads the Energy Government Coordinating Council (EGCC) with DHS, to convene interagency partners, States, and international partners and discuss the important security and resilience issues for the energy sector. This forum ensures that Federal government agencies are working together for a whole-of-government response. The EGCC meets thrice annually with the industry-led Electricity Subsector Coordinating Council (ESCC) and the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) to discuss energy security and mitigate critical infrastructure vulnerabilities and help reduce impacts from threats.

Further, CESER coordinates with interagency partners through the National Security Council to implement the National Cyber Strategy. The first pillar of the National Cyber Strategy is Protect the American People, the Homeland, and the American Way of Life. Securing critical infrastructure is a focus area within the pillar and highlights of relevant activities include: refining roles and responsibilities and prioritizing actions according to identified national risks. Both efforts will support strengthening government coordination to address energy security.

- Q5b. Has CESER met with FERC and DHS officials on improving coordination?
- A5b. CESER regularly engages through the EGCC, which is co-led by DHS and DOE. Additional engagement happens more frequently as well, including weekly coordination of ongoing activities. The Federal Energy Regulatory Commission (FERC) and DOE

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

Technical Conference on Energy Infrastructure Security Practices held on March 28, 2019, is an example of the positive coordination that is underway to explore threats to energy infrastructure and identify best practices for mitigation, investment incentives, and cost recovery practices.

- Q5c. What is the status of DOE's relationship to the National Guard and other branches of the military?
- A5c. CESER regularly engages with the U.S. Department of Defense and the U.S. Coast Guard (USCG) through the EGCC, which is co-led by DHS and DOE. CESER also maintains regular communication with the USCG to share threat information and engage in ongoing USCG regional activities. The USCG is a regular participant in the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) meetings. Regarding the National Guard Bureau, CESER staff met twice in the last month with National Guard Bureau officials on engaging them in DOE's annual exercises, providing training through the CyberStrike program, and coordinating state, local, tribal, and territorial program activities.
- Q5d. How can these relationships be improved?
- A5d. The relationships continue to improve through the ongoing coordination that is already underway.
- Q6. Antitrust compliance generally precludes agreement among competitors regarding the availability of a service, product design, terms of sale, and other activities that restrain competition.
- Q6a. How are the antitrust laws impacting the ability of the energy industry to properly defend its assets against a cyberattack?
- A6a. DOE defers to our energy industry partners with regards to how legal matters impact individual organizations' efforts to protect against a cyberattack. Many energy industry associations may also be able to articulate their constituents' concerns.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

Q6b. Should Congress consider holding a hearing or taking other action?

A6b. The Department will continue to monitor the situation and seek informal feedback from industry.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

QUESTIONS FROM RANKING MEMBER MANCHIN

- Q1. We discussed concerns about the information sharing process not working quickly enough, especially for component manufacturers. What do you think the solution is?
- A1. Establishing a next-generation information sharing model —advancing technology, policy, and partnerships—will dramatically improve speed, reduce cost, and increase industry participation. This initiative capitalizes on the existing information technology (IT) and operational technology (OT) experiences and concepts, using the latest available technology, architecture, and innovative partnerships with the energy sector to provide the enhanced cyber protection for the energy sector. The vision is to increase industry participation and to gain a higher level of threat detection capability. The current process for sharing component vulnerabilities and recommended mitigations can take months or years to lead to implementable solutions for utilities. The Office of Cybersecurity, Energy Security, and Emergency Response’s (CESER’s) programs, like Cybersecurity Testing for Resilience and Control Systems (CyTRICS), Cybersecurity for the Operational Technology Environment (CyOTE), and the Improved Consequence Prioritization (ICP) process, will develop situational awareness for utilities including indicators of cyber-attack, implementable vulnerability mitigations, and high-impact security enhancements that CESER will share both through Analysis of Risks in the Energy Sector (ARES) reporting and through high-speed automated data feeds and alerts with Cyber Analytics Tools and Techniques 2.0 (CATT 2.0™). This initiative capitalizes on the existing IT and OT experiences and concepts, using the latest available technology, architecture, and innovative partnerships with the energy sector to provide enhanced cyber protection for the energy sector. The vision is to dramatically increase industry participation and to gain a higher level of threat detection capability.

The Department of Energy (DOE)’s Office of Energy Efficiency and Renewable Energy, in partnership with CESER, intends to release a Funding Opportunity Announcement entitled Clean Energy Manufacturing Innovation Institute: Cybersecurity in Energy Efficient Manufacturing. Research funding will be up to \$70 million over five years,

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

excluding private partner cost share. The institute, will focus on understanding the evolving cybersecurity threats to greater energy efficiency in manufacturing industries, developing new cybersecurity technologies and methods, and sharing information and expertise to the broader community of U.S. manufacturers.

The institute is expected to help identify solutions to alert and mitigate cybersecurity threats in automated manufacturing systems. The anticipated technical focus for the Institute will include: supporting coordinated vulnerability disclosure (CVD) activities to improve the safety and security of manufacturing and energy-intensive industries; improving security for agile on-demand, dynamic, energy-aware and cost-effective supply chains; enabling autonomy and connected processes for manufacturing systems with secure asset and energy management; improving supply chain centric real-time prescriptive data analytics for security threats, risk reduction and mitigation; and improving security related supply chain efficiency.

- Q2. The interactions between information technology and operational technology systems present significant vulnerabilities for our grid infrastructure.
- Q2a. What defenses, security measures, or detection measures are best to employ between informational technology networks and operation technology networks in order to defend the electric grid's physical infrastructure from attacks by hackers, insider attacks, negligence, or mistakes?
- A2a. Utilities often employ segmentation using firewalls between IT and OT networks to scan for malicious code and route information in a protected way between domains. A best practice is that IT and OT are never connected and are separated by a demilitarized zone (DMZ). Information does not go directly from IT to OT or vice versa.
- Q2b. How should utilities mitigate the risks of connecting information technology systems to operational technology systems?
- A2b. Enterprise IT networks are exposed to the public-facing internet, significantly increasing the risk of cyber threats. A typical approach to mitigating this risk is to segregate the IT and OT networks for greater protection, making sure that there is clear demarcation

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

between the networks. The OT network is devoted to running critical infrastructure. Utilities should ensure the safety of these operations and continuously monitor and mitigate their energy delivery systems equipment for cyber threats and vulnerabilities and to ensure proper segmentation.

- Q3. As we establish workforce training programs at colleges and universities, we must be certain that we are training people for jobs that exist locally. We must ensure that the DOE is focused on creating jobs in all communities – particularly vulnerable communities – and that all training programs target and recruit from groups that are often neglected.
- Q3a. What is your plan for the Department of Energy to accomplish this?
- A3a. The Secretary has prioritized workforce development, especially in the energy-cyber field. We will continue to explore and improve programs that contribute to this priority and leverage DOE's National Laboratories, located across the country, as ideal locations for our Nation's best and brightest. Through the DOE's CyberForce Competition™, an annual collegiate-level cyber-defense competition, DOE has leveraged seven National Laboratories and invited more than 150 colleges and universities to participate in the competition. bNew to the competition in 2018, both Historically Black Colleges and Universities and community colleges were invited and competed in the event. To better support the awareness of local and rural cooperative utilities' cyber workforce development needs, DOE also partnered with the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) to bring in municipally-owned utility representatives to directly participate in a career fair during the competition, interact with student teams, and provide the keynote speaking engagement prior to the competition's kickoff.
- Q4. Forbes reports that by 2021 there may be as many as 3.5 million unfilled positions in the cybersecurity sector.
- Q4a. Once these jobs are available in a community, what is the best way for us to get our workers trained with these much needed skills and into the cybersecurity workforce?

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

- A4a. Through efforts such as the CyberForce Competition™, an annual DOE-sponsored collegiate-level cyber-defense competition, the Department's goal is to familiarize and inform the next generation of cyber defenders about the roles a cybersecurity specialist can have in both the private sector utility arena as well as in the research-focused National Laboratories. The competition continues to improve annually, including better alignment with the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) Framework. The NICE mission is to energize and promote a robust network and ecosystem of cybersecurity education, training, and workforce development.

Through professional training, such as the Department's CyberStrike workshops, cybersecurity professionals at our Nation's utilities and key partners are offered hands-on, simulated demonstrations of replicated real world cyberattacks on the energy sector to help them mitigate against and respond to similar attacks. Further, the CyberStrike workshops continue evolving to ensure U.S. critical infrastructure owners and operators are trained on emerging cyber threats. These efforts, combined with others from the Department, other Federal agencies, and the private sector, contribute towards the future training of our cybersecurity workforce.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

QUESTIONS FROM SENATOR WYDEN

- Q1. The Department of Homeland Security has the authority, pursuant to the Federal Information Security Modernization Act of 2014, to issue “compulsory direction to an agency that . . . is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk.” Agencies are required to comply with these directives. In recent years, DHS has issued a number of these Directives, requiring agencies to adopt email and website encryption, to prohibit the use of software made by Kaspersky, and most recently, to protect their domain name system infrastructure. DHS does not, however, have the authority to require the adoption of these cybersecurity best practices by the private sector, including companies in critical infrastructure sectors like the Energy industry.
- Q1a. Has the Department of Energy (DOE) taken steps to require or at least recommend that energy companies regulated by DOE adopt the cybersecurity best practices outlined in the DHS directives published at <https://cyber.dhs.gov/>?
- A1a. The Department of Energy (DOE) promotes and recommends that the electric sector adhere to relevant best practices including directives issued by the Department of Homeland Security (DHS). These organizations decide which industry best practices are applied and how they are integrated depending on their unique operations and facilities. In addition, DOE regularly meets with the electricity sector to discuss these directives and changing vulnerabilities as they arise. The Federal Energy Regulatory Commission (FERC) is a regulatory agency, not DOE.
- Q1b. If not, for each of the directives issued by DHS, please describe why you do not believe that these best practices are appropriate for the energy sector.
- A1b. These directives may be appropriate at this time for the energy sector; however, DOE does not have the authority to require energy sector entities to adopt cybersecurity best practices.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

- Q2. The National Institute of Standards and Technology (NIST) published updated guidance on multi-factor authentication in June of 2017. NIST's guidance raises particular concerns about cybersecurity risks associated with the use of the public switched telephony networks (PSTN) for multi-factor authentication, such as cellular text messages. Numerous media reports published during the past two years have highlighted incidents in which cyber-criminals have intercepted multi-factor authentication tokens transmitted via cellular text messages, enabling them to steal money from bank accounts and otherwise gain unauthorized access to victims' online accounts.
- Q2a. Should cellular text message-based multi-factor authentication be used by energy companies' employees for any online account, personal or work-related, which, if the account were compromised by hackers, could negatively impact U.S. national security?
- A2a. Energy companies follow cybersecurity standards, industry best practices, and published guidelines, as well as applying processes, policies, and procedures that are in line with emerging cybersecurity standards. Energy companies are required by regulators to follow compliance-based approaches to cybersecurity. In instances where compliance is not required, a risk-based decision-making approach to technology selection is often taken considering many things such as the effectiveness, company policies, standards, regulations, and impacts.
- Q3. Since 2017, the National Institute of Standards and Technology (NIST) has recommended against the previously-widespread practice of forcing users to regularly change their passwords. NIST joins the Federal Trade Commission and the government of the United Kingdom in recognizing that routinely forcing users to change their passwords can in-fact result in worse security.
- Does DoE still mandate automatic password rotation for any of its computer systems?
 If yes, how many DoE systems still mandate routine password rotation, and what plans, if any, does DoE have to adjust its password policies to be consistent with NIST-recommended best practices?
- A3. No, DOE does not mandate automatic password rotation but permits password rotation consistent with NIST risk-based approach to security control implementation and a comprehensive security posture. We do not at this time have a count of how many systems using this technique across the complex but consistent with federal direction, encourage the adoption of multi-factor authentication wherever practicable.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

The Department cybersecurity program is executed under a Departmental Directive, DOE Order 205.1B, *Department of Energy Cybersecurity Program*. The Order is consistent with Federal best practices and requires that Departmental Elements manage cybersecurity programs based on Federal requirements and appropriate national standards. The Order allows every Departmental Element to execute password administration and management based on its mission, goals, and assessment of risk. It is expected that Departmental Elements will consider National Institute of Standards and Technology (NIST) guidance, such as the Special Publication that deals with password management (NIST SP 800-63-B, *Digital Identity Guidelines - Authentication and Lifecycle Management*), in risk-based protection of information systems and assets.

A wide variety of assets comprise the DOE operational environment, and each asset may entail a different risk profile. The Departmental cybersecurity policy allows for tailored, mission-driven, risk-based management of information assets. There are assuredly systems within the DOE, particularly legacy systems, for which password expiration is selected as a risk mitigation strategy to limit the time period an adverse actor has to attempt access with a compromised password; however, there are few DOE systems for which passwords are the sole authentication method. The risk of password usage, and static passwords in particular, is significantly mitigated by implementation of multi-factor authentication, controls on privileged access, credentialing processes, and other technical controls.

The current NIST Special Publication discourages mandatory periodic password change policies. The Department recommends, but does not require, relaxing of periodic password expiration periods for user access; Departmental Elements are able to determine how best to implement NIST guidance for their information systems. The Office of the Chief Information Officer, for example, relaxed its password expiration rules from 60 days to 365 days on its Energy Information Technology Services (EITS) environment based on an assessment of the security posture of supported systems. EITS also enforces mandatory password change if there is evidence of compromise of the

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

authenticator and lockout if 5 invalid password attempts are made in a 15-minute period.
These are other facets of password administration recommended by NIST.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

QUESTIONS FROM SENATOR RISCH

- Q1. Assistant Secretary Evans, I understand your office received \$10 million this year to conduct some consequence based methodology work to enhance the energy sector's control system cybersecurity. As you may be aware, Senator King and I have a bill, the Securing Energy Infrastructure Act, in this area that we hope to get enacted this Congress. As such, can you tell the Committee about how the office plans to utilize the funding?
- A1. A primary element of the Automated System R&D initiative is the Improved Consequence Prioritization (ICP) Process. This initiative will manage cyber-risk by prioritizing energy sector defenses against high cyber-attack consequence events, simplify and isolate automated systems, and remove vulnerabilities. The ICP effort will conduct up to six, distinct assessments with energy sector partners over a two-year period. Each ICP assessment will execute: the consequence prioritization and modeling process; the steps of the system-of-systems breakdown; consequence-based targeting and Industrial Control System (ICS) cyber kill chain development; and development of key mitigations and protections, primarily designed to simplify critical/vulnerable automated systems.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

QUESTIONS FROM SENATOR STABENOW

- Q1. It is deeply troubling that key parts of our energy system are made in other countries – like China – raising the potential for tampering, theft, or the insertion of malware in our energy supply chain.
- Q1a. Would you please speak to the vulnerabilities within our energy supply chain, and to whether our growing dependence on foreign-made energy components presents a potential national security threat?
- A1a. The entire energy sector faces a cybersecurity challenge compounded by the use of common underlying subsystems and components, both hardware and software, which share similar vulnerabilities. Behind the brand labels of operational technology devices are collections of subcomponents, often produced by second-tier vendors that may contain poorly constructed or poorly controlled software, firmware, and hardware elements. Vendors may use similar subcomponents for common functions, unbeknownst to them or the asset owner, which may introduce unanticipated common vectors that can be exploited. Though common applications of components can offer financial and operational advantages, they also reduce the diversity and resilience of systems. These issues must be addressed, no matter the country of origin, to secure critical infrastructure.
- Q2. Due to the increasing interdependence of our critical infrastructure, any attack on our energy system would cause significant disruptions across our economy. Our hospitals, homes, and businesses cannot operate without power, and today's trends towards digitization and automation mean they are relying more on electricity than ever before. Moreover, new cybersecurity threats are emerging as transportation becomes increasingly electrified and autonomous. By 2040, 55 percent of all new car sales are projected to be electric; and by 2020, 90 percent of new cars are projected to be connected to the internet.
- Q2a. How is the Department of Energy coordinating with federal and state regulators to ensure the speedy recovery of other critical assets – such as hospitals, banks, and factories – following a cyber-attack on our energy network?
- A2a. As the lead for the Department of Energy's (DOE's) Emergency Support Function (ESF) #12 responsibilities, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) regularly coordinates with interagency, industry, and state, local, tribal, and territorial partners on the restoration of electricity to critical facilities and

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

infrastructure across all sectors during incident response. CESER also works closely with the U.S. Army Corps of Engineers (USACE) as the lead for ESF #3 (Public Works and Engineering) to identify locations that may experience prolonged outages to support USACE's temporary power mission. CESER also encourages state energy offices to work with critical energy infrastructure owners and operators to plan priorities and coordination of restoration.

- Q3. As the Ranking Member of the Senate Agriculture Committee, I am especially aware of the challenges small utilities and rural electric cooperatives face in addressing cybersecurity. For example, it is especially harder for smaller and not-for-profit utilities to overcome the costs associated with cybersecurity protections, including the hiring, training, and retention of in-house top cyber experts.
- Q3a. Rural electric cooperatives and publicly owned utilities deliver more than 25 percent of our country's electricity, so it is imperative they are adequately protected. What actions is the Department of Energy taking to address the immediate workforce needs of small utilities?
- A3a. CESER works with the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) to promote a culture of security and resiliency within the public power and cooperative community, and to coordinate with existing and future state, local, tribal, territorial and Federal programs. CESER supports APPA and NRECA in the development of tools, educational resources, updated guidelines, and training (e.g., exercises and site assessments) on common strategies for fostering an improved resiliency and security culture with the primary objective of these cooperative agreements being the inception of internal cyber resiliency and security programs at public power and cooperative utilities.

Specifically, APPA and NRECA provide outreach, training, educational materials, exercises, workshops, site assessments, and technical assistance via in-person or virtual platforms to their members to research and evaluate emerging technologies and support the development of cybersecurity guidelines that provide a baseline to protect against known vulnerabilities. The projects support efforts to: advance development of cyber

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

security tools and guidelines; evaluate and mitigate cyber and physical system vulnerabilities; research, develop, and adopt emerging technologies to improve resilience and security; and enhance capabilities to share key information among public power providers. The tasks and activities are performed to support the modernization of the Nation's energy infrastructure, the advancement and use of new energy technologies, and the resilience of the Nation's energy system. APPA and NRECA coordinate with other electric sector organizations, as appropriate, to leverage resources and accomplish project objectives in an efficient and cost-effective manner.

- Q3b. Are there retraining, apprenticeship programs, or partnerships with community colleges that encourage onsite cyber training in smaller communities?
- A3b. DOE's annually-sponsored collegiate-level cyber-defense competition, the CyberForce Competition™, is helping develop the next generation of cybersecurity professionals to help defend and bolster the Nation's critical energy infrastructure and ensure our energy security.

Students from 64 colleges and universities, including community colleges and Historically Black Colleges and Universities, participated in the December 2018 competition. This competition featured teams representing 27 states and Puerto Rico. Participants ranged from undergraduate freshmen to Ph.D. candidates. The goal of the competition is to familiarize and inform the next generation of cyber defenders about the roles a cybersecurity specialist can have in both the private sector utility arena as well as in the research-focused National Laboratories. The competition continues to improve annually, including exploring opportunities for students to learn more about available internships and careers within the energy sector, while preparing for and participating in the competition.

CESER works with the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) to support smaller communities and promote a culture of security and resiliency within the public power and cooperative

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

community, and to coordinate with existing and future state, local, tribal, territorial and Federal programs. CESER supports APPA and NRECA in the development of tools, educational resources, updated guidelines, and training (e.g., exercises and site assessments) on common strategies for fostering an improved resiliency and security culture with the primary objective of these cooperative agreements being the inception of internal cyber resiliency and security programs at public power and cooperative utilities.

Specifically, APPA and NRECA provide outreach, training, educational materials, exercises, workshops, site assessments, and technical assistance via in-person or virtual platforms to their members to research and evaluate emerging technologies and support the development of cybersecurity guidelines that provide a baseline to protect against known vulnerabilities. The projects support efforts to: advance development of cyber security tools and guidelines; evaluate and mitigate cyber and physical system vulnerabilities; research, develop, and adopt emerging technologies to improve resilience and security; and enhance capabilities to share key information among public power providers. The tasks and activities are performed to support the modernization of the Nation's energy infrastructure, the advancement and use of new energy technologies, and the resilience of the Nation's energy system. APPA and NRECA coordinate with other electric sector organizations, as appropriate, to leverage resources and accomplish project objectives in an efficient and cost-effective manner.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

QUESTIONS FROM SENATOR CASSIDY

- Q1. To what degree are companies complying with best practices in order to prevent the spread of a cyberattack, malware infection or virus into a regional transmission system such as the Midcontinent Independent System Operator (MISO)?
- A1. The Department of Energy's (DOE's) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) does not have regulatory authority to require energy sector entities to comply with cybersecurity best practices. The Federal Energy Regulatory Commission (FERC) has been delegated the authority for compliance and enforcement of best practices. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) non-compliance can result in fines up to \$1 million per day depending on the severity of the violations.
- Q2. Are there current best practices to isolate such an attack or infection to an individual company or do other companies along the regional transmission system become vulnerable too?
- A2. There are best practices for cybersecurity event recovery, including the NIST SP 800-184 Guide for Cybersecurity Event Recovery. These best practices involve identifying the root cause(s) of the cyber event and planning for the response, containment, and response actions. However, cascading failures, interdependencies among utilities, and other critical infrastructures are still a concern and additional R&D could help. The Cybersecurity for Energy Delivery Systems (CEDS) R&D program has projects that are working to provide automated response to a cyber incident. As one example, the projects' pre-engineer alternative operational network paths that can be used automatically to help sustain critical functions in the event of a cyber incident. In another example, they help anticipate the physical consequences to power system operations if a received command is executed and reject commands that could jeopardize grid stability, and in another example, help tailor access controls to immediate circumstances, such as restricting access to cyber-assets in the case that physical intrusion is detected for containment and eradication.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

- Q3. Is there a minimum standard of cyber security required of utilities or is it entirely voluntary? If there is a minimum standard, what is it?
- A3. There are NERC Critical Infrastructure Protection (CIP) cybersecurity and reliability standards which are mandatory and enforceable standards. These standards cover the security of electronic perimeters and the protection of critical cyber assets.
- Q3a. If there isn't, what steps is the Department taking, in conjunction with industry and other federal partners, to establish minimum standards?
- A3a. There are mandatory and enforceable cybersecurity and reliability standards for the energy sector. In addition, DOE's CEDS Program interacts with the Department of Commerce's National Institute of Standards and Technologies (NIST) to support standards development. NIST is responsible for the development and maintenance of cybersecurity standards for the smart grid. NIST is fulfilling its responsibility, under the Energy Independence and Security Act of 2007 (Title XIII, Section 1305), to coordinate standards development for the smart grid. NIST solicits input and cooperation from private and public-sector stakeholders in developing cybersecurity standards. DOE also works closely with the three energy sector information sharing and analysis centers (ISACs)—the Electricity ISAC, downstream natural gas ISAC, and oil and natural gas ISAC—to share best practices, threat-related information, and training initiatives. These activities help DOE promulgate cybersecurity practices that go above and beyond the standards.
- DOE is in the process of updating its Cybersecurity Capability Maturity Model (C2M2) tool that aligns to the NIST Cybersecurity Framework. DOE's C2M2 is another tool used by industry to review their own cybersecurity practices across multiple domains and then make informed decisions to improve policies, procedures, and technologies.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

QUESTIONS FROM SENATOR HIRONO

- Q1. I have heard from operators of critical energy infrastructure in my state about need access to actionable threat intelligence and threat indicators from federal agencies in a timely manner, along with the ability to evaluate company data logs using the threat information. The operators have told me they are constrained by the inability to get company personnel the appropriate security clearances and access to Sensitive Compartmented Information Facilities (SCIFs), where they can view classified information.
- Q1a. What is needed to expedite clearances and access for appropriate personnel at critical energy infrastructure operators?
- A1a. The Department of Energy (DOE) and private energy sector personnel, through the Department of Homeland Security (DHS) Private Sector Clearance Program, both depend on the Office of Personnel Management's (OPM's) National Background Investigations Bureau (NBIB) to perform background investigations for clearances and we defer to OPM for ways to expedite the process. The transfer of NBIB from OPM to the Department of Defense to help alleviate the issue in the future is still ongoing.
- Q1b. For steps that need to be taken by other federal departments or agencies, what is the Department of Energy doing to work to resolve the issue with the other agencies?
- A1b. DOE meets with DHS regularly to discuss improving processes for the Private Sector Clearance Program.
- Q2. We have several cyber education programs in Hawaii that work collaboratively with the National Security Agency and the Department of Homeland Security, such as the National Centers of Academic Excellence in Cyber Defense and Center of Academic Excellence in Research. In your testimony, you described the DOE's Office of Cybersecurity, Energy Security, and Energy Reliability's (CESER's) efforts to hold two annual cybersecurity competitions for college and university teams.
- Q2a. Is CESER doing anything to improve post-secondary educational cybersecurity training curricula or supporting student fellowship opportunities in the energy sector to help meet the growing need of cyber security professionals in the sector?
- A2a. Through efforts like the CyberForce Competition™, the annual DOE-sponsored collegiate-level cyber-defense competition, the Department's goal is to familiarize and

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to the Honorable Karen Evans

inform the next generation of cyber defenders about the roles a cybersecurity specialist can have in both the private sector utility arena as well as in the research-focused National Laboratories. The competition continues to improve annually, including exploring opportunities for students to learn more about available internships and careers within the energy sector, while preparing for and participating in the competition.

CESER also works with the American Public Power Association (APPA) and the National Rural Electric Cooperative Association (NRECA) to promote a culture of security and resiliency within the public power and cooperative communities. CESER supports APPA and NRECA in the development of tools, educational resources, updated guidelines, and training (e.g., exercises and site assessments) on common strategies for fostering an improved resiliency and security culture with the primary objective of these cooperative agreements being the inception of internal cyber resiliency and security programs at public power and cooperative utilities.

Specifically, APPA and NRECA provide outreach, training, educational materials, exercises, workshops, site assessments, and technical assistance via in-person or virtual platforms to their members to research and evaluate emerging technologies and support the development of cybersecurity guidelines that provide a baseline to protect against known vulnerabilities. The projects support efforts to: advance development of cyber security tools and guidelines; evaluate and mitigate cyber and physical system vulnerabilities; research, develop, and adopt emerging technologies to improve resilience and security; and enhance capabilities to share key information among public power providers. The tasks and activities are performed in support of the modernization of the Nation's energy infrastructure, advancement and use of new energy technologies, and resilience of the Nation's energy system. APPA and NRECA coordinate with other electric sector organizations, as appropriate, to leverage resources and accomplish project objectives in an efficient and cost-effective manner.

U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Questions for the Record Submitted to Major William J. Keber

Questions from Senator Debbie Stabenow

Questions: As the Ranking Member of the Senate Agriculture Committee, I am especially aware of the challenges small utilities and rural electric cooperatives face in addressing cybersecurity. For example, it is especially harder for smaller and not-for-profit utilities to overcome the costs associated with cybersecurity protections, including the hiring, training, and retention of in-house top cyber experts.

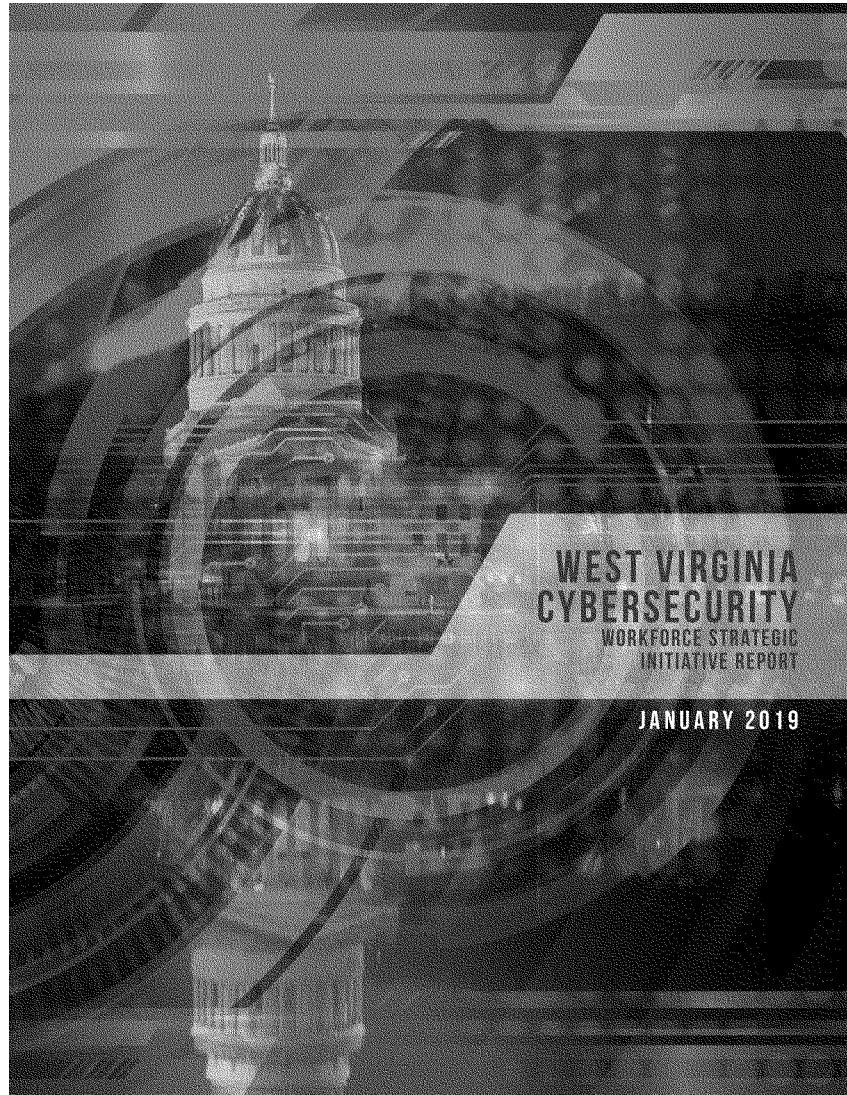
Rural electric cooperatives and publicly owned utilities deliver more than 25 percent of our country's electricity, so it is imperative they are adequately protected.

What actions is the National Guard taking to address the immediate workforce needs of small utilities? Are there retraining, apprenticeship programs, or partnerships with community colleges that encourage onsite cyber training in smaller communities?

Response: Ranking Member Stabenow, thank you for your inquiry concerning the workforce needs of smaller utilities in smaller and rural communities. The West Virginia National Guard is not currently training small utilities specifically, but we are in discussions with the West Virginia State Office of Technology to develop assessment opportunities in partnership with state entities. This has the potential provide engagements to address the topics presented here. As assessments are conducted, the opportunity to mentor and discuss best practices with smaller utilities is there.

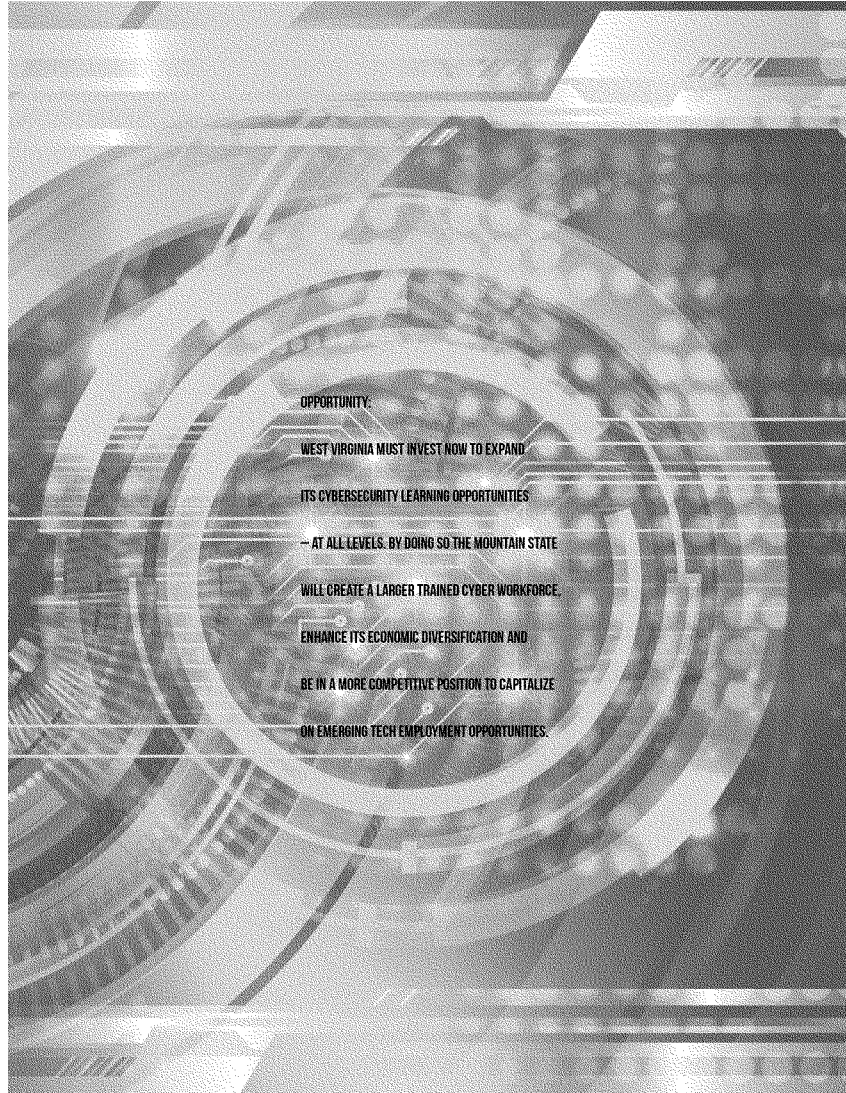
West Virginia TechConnect has done an excellent job gathering and presenting the cybersecurity education opportunities available at universities and colleges within the state. The forums they have hosted provide insightful dialogue into not only what West Virginia institutions are doing, but also what other states are doing with cybersecurity workforce development. This has the potential to address the skills gap you are describing. The *West Virginia Cybersecurity Workforce Strategic Initiative Report* not only highlights the fields of study and cyber certification opportunities within West Virginia institutions, but other programs that other states are organizing to enhance cybersecurity workforce development. All of these opportunities have the potential to reach outlying rural communities.

I have accompanied the report with this document. Additionally, the link to the *West Virginia Cybersecurity Workforce Strategic Initiative Report* is: https://techconnectwv.org/wp-content/uploads/2018/12/MURC_WVCybersecurityWorkforce_Book_FINAL.pdf



**WEST VIRGINIA
CYBERSECURITY**
WORKFORCE STRATEGIC
INITIATIVE REPORT

JANUARY 2019



CONTENTS

5-45	WV CYBERSECURITY WORKFORCE STRATEGIC INITIATIVE REPORT
47-49	LIST OF PARTICIPANTS ON W.VA. CYBERSECURITY WORKFORCE STRATEGIC PLANNING GROUP
50-55	W.VA. DEPARTMENT OF EDUCATION CYBER EDUCATION PLAN
56-62	NGA REPORT ON STATE CYBER WORKFORCE INITIATIVES

THANK YOU TO OUR PARTNERS
FOR THEIR COMMITMENT TO THIS PROJECT.



**HIGH TECHNOLOGY.
FOUNDATION**



CYBERSECURITY



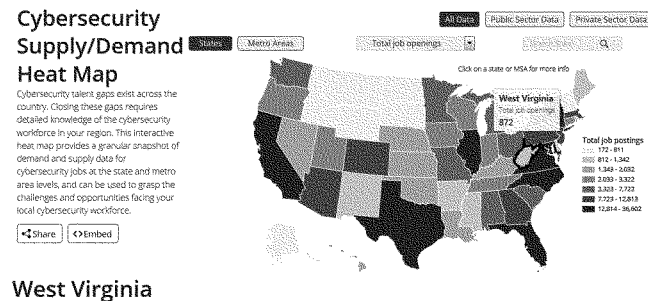
West Virginia Cybersecurity Workforce Strategic Initiative Report

TechConnect West Virginia has been the driving force behind the West Virginia Cybersecurity Workforce Strategic Initiative. TCWV is a non-profit coalition committed to the advancement of the innovation economy in West Virginia, focused on four technology sectors: advanced energy, chemicals and advanced materials, biosciences, and biometrics. With broad representation from private industry, the public sector, and higher education, TechConnectWV seeks to diversify the state's economy, promote economic prosperity and create high-paying jobs.

Among other key partners supporting this initiative are the West Virginia Office of Technology, the W.Va. High Technology Consortium, the West Virginia National Guard and West Virginia Forward.

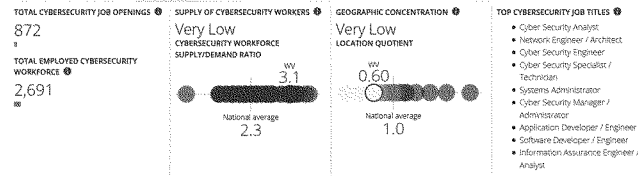
1. Opportunity

Job opportunities for cybersecurity professionals are growing significantly, but a large percentage is going unfilled within the United States (and the world), particularly within the military and the federal government -- national and homeland security as well as intelligence (Rand, 2014). Such unfilled positions complicate securing the nation's networks and may leave the United States ill-prepared to carry out conflict in cyberspace. And, this cyber shortage also poses dangers to critical infrastructure, our health care and banking systems, to governments of all sizes and to business large and small. According to cyberseek.org (2018) in West Virginia (WV) there are currently 872 cybersecurity job openings with a total employed cybersecurity workforce of 2,691. At the national level there are 313,735 total cybersecurity job openings with a total employed cybersecurity workforce of 715,715.



CYBERSECURITY

West Virginia

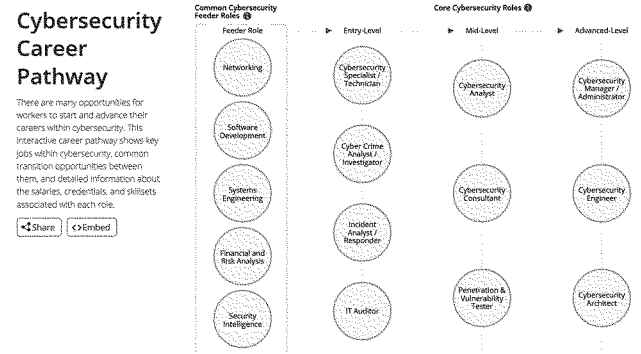


These numbers will increase because, according to the Department of Labor's Bureau of Labor Statistics, the field of cybersecurity is projected to grow at a rate of 28% from present to 2026. Other reports indicate that the need for cybersecurity works is approaching staggering numbers:

- By 2022 there will be a need for 1.8 million more professionals in the cybersecurity field, according to a 2017 report from the Center for Cyber Safety and Education™ (the Center) — part of its eighth Global Information Security Workforce Study (GISWS) - sponsored by (ISC)® and Booz Allen Hamilton. <https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/02/13/Cybersecurity-Workforce-Shortage-Continues-to-Grow-Worldwide>
- Another report puts this cyber workforce need at 3.5 million by 2021: <https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html>
- NICE Workforce Demand fact sheet https://www.nist.gov/sites/default/files/documents/2017/11/16/workforce_demand_111617_final.pdf

CYBERSECURITY

However, more and more positions continue to go unfilled because employers cannot find candidates with the correct skills. Here is an outline of cyber career pathway: (Source: <https://www.cyberseek.org/pathway.html>)



West Virginia must invest now to expand its cybersecurity learning opportunities – at all levels. By doing so the Mountain State will create a larger trained cyber workforce, enhance its economic diversification and be in a more competitive position to capitalize on these emerging tech employment opportunities.

CYBERSECURITY

2. Overview

Mission

To develop a strategic plan on how to accelerate cybersecurity education in both K-12 and higher education.

Objectives

- 1) Align interested agencies, institutions, businesses and stakeholders in a focus on cybersecurity workforce training and employment opportunities
- 2) Seek input and recommendations from cybersecurity businesses and specialists
- 3) Analyze and make recommendations on workforce training programs across the educational attainment continuum
 - a. High school
 - b. Two-year
 - c. Four-year
 - d. Certificate
- 4) Review policies and projects in other states (Virginia, Michigan)
- 5) Develop strategies on workforce development and economic opportunities related to cybersecurity ...share with Governor Justice in the fall of 2018.

Action Items

- Compile an overview of the existing cybersecurity degrees provided in West Virginia (WVU, Marshall, FSU, UC, AB, C&TCs)...and new programs (WVU, Marshall) being developed.
 - Share this info with key state leaders and key policy makers
- Provide analysis to the WVSBCD on its cyber assessment on-line tool and promote tech firms to add their cyber services to the WVSBCD.
- Have cyber employers evaluate the current cybersecurity curriculum and degrees provided by the community & technical colleges -- BridgeValley, Pierpont, Blue Ridge, Northern.
- Explore the development of cyber internship programs with employers -- large and small.
- Work with the W. Va. Dept. of Education to provide recommendations on cybersecurity learning courses and STEM applications for middle and high school students. The CyberPatriot high school program provides useful curricula components for incorporation into classroom learning.
- Help recruit more cyber specialists to be "tech experts" to grow youth cyber programs/activities (CyberPatriot, GirlsGoCyberStart, etc.) at more high schools in the state.
- Prepare an overview of the key resource needs facing the existing cybersecurity degree programs at four-year institutions, particularly related to the high costs associated with cyber software needed for classroom instruction.
- Work with existing federal agencies (NOAA, NASA, U.S. Dept. of Commerce, etc.) and contractors in WV to understand their cybersecurity workforce needs.
- Develop an integrated cybersecurity workforce plan of action.
- Outline a new web site that will provide information on high-tech training programs, curriculum and degrees in the areas of cybersecurity (and maybe coding).
 - Seek a volunteer web/back-end developer

Findings

Provided are key cyber job domains that the work group identified:

Security and Risk Management.
 Asset Security.
 Security Engineering.
 Communications & Network Security.
 Identity & Access Management.
 Security Assessment & Testing.
 Security Operations.
 Software Development Security.

<https://resources.infosecinstitute.com/the-cissp-domains-an-overview/>

Provided are cyber industry certifications that the group identified:

- Industry
 - Certified Information Systems Auditor (CISA)
 - Certified Information Security Manager (CISM)
 - Certified Information Systems Security Professional (CISSP)
 - Certified Ethical Hacker
- DoD 8570
 - CompTIA Security+ certification
 - ISC2 CAP certification
- NIST - <https://nccs.us-cert.gov/training/search/itsm-solutions-llc/nist-cybersecurity-framework-foundation-certification-training>
 - Cyber Operations
 - Training, Education and Awareness
- Other
 - CompTIA Security+
 - GSEC: SANS GIAC Security Essentials

CYBERSECURITY

Working Groups

As part of this group's deliberations, subgroups were developed to analyze key cybersecurity educational strategies and make recommendations on the workgroup's ongoing focus areas:

- 1) Cybersecurity Career Pathway/Training Program
 - o Work with the state education leaders to analyze and provide recommendations on an integrated career pathway in cybersecurity and relevant course offerings
 - High School (W.Va. Dept. of Education)
 - Community & Technical College (one-year, two-year)
 - Four-year programs (University of Charleston, Marshall, WVU, Fairmont State, etc.)
 - Online learning options
 - Model? - http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cyber-courses-2017.pdf
 - o Develop informational resources to share with students so they understand other non-education factors for those interested in pursuing careers in cybersecurity
 - Credit history
 - Personal activities
 - Criminal record
 - Soft-skills
 - o Develop a speaker forum of cyber specialists who could meet with students.
 - o Explore the expansion or introduction of cyber STEM activities
 - [CyberPatriot program](#) (currently being introduced in WV)
 - Build cyber programs off of the state's successful [WV Robotics Alliance](#)
- 2) Real-World Experience/Private-Sector Needs
 - o Outline needs and unique issues (clearances) of different employers as it relates to cyber workforce:
 - Government agencies, contractors
 - Financial industry
 - Health care industry
 - Private-sector cyber services providers
 - o Evaluate benefits of generalist (mile wide, inch deep) vs. specialist?
 - o Develop course curriculum recommendations to develop a baseline cyber education program
 - Explore "certificate" programs in WV
 - o Examine new ideas to reduce employment barriers related to clearances
 - State cyber incentive program (to cover the costs of security clearances)
 - o Review existing industry-recognized cybersecurity credentials
 - o Develop a state cyber internship program and other policy matters
 - o Develop a Cyber Civilian Corps program (modeled after Michigan's)
- 3) Recruitment/Outreach
 - o Develop a strategic campaign (and resources) to recruit cyber specialists/security clearance individuals back to WV
 - o Enact state legislation to provide tax relief to cyber specialist who return to WV
 - Military retirees
 - o Develop an outreach and education campaign to encourage cyber education/training and promote job opportunities among interested West Virginians of all ages
- 4) Long-Range Strategy
 - o Interconnect with the state Office of Technology on its cyber strategic objectives
 - o Study model programs in other states
- 5) Military
 - o Develop a plan of action on how to leverage and recruit WV National Guards people, veterans and military retirees who have cyber skills or who could be trained.

3. Cyber Workforce Team Members

A multi-disciplinary team of cyber experts, employers, government officials and educators from across West Virginia has assembled as part of this strategic planning process. Those members include representatives from higher education, government, private industry, tech firms, technology-related organizations and the military.

See Appendix A for a complete list of the workforce team members.

4. Situational Overview

According to McKinley & Company, every year, hackers produce some 120 million new variants of malware. Several billion data sets are breached. And companies report thousands of attacks every month, ranging from the trivial to the extremely serious. Think WannaCry, NotPetya, Meltdown, and Spectre. And, these statistics do not include cyber incidents from within companies or agencies.

In December 2016 the Information Systems Security Association (ISSA) and analyst firm Enterprise Strategy Group (ESG) published a report from a survey of cyber security professionals worldwide that concluded that current staff lack the skills to properly defend networks. The study found: "Some 54% of organizations in the study have suffered at least one security event in the past year, and most attribute the events to a lack of security staff or training. Some 70% of organizations report the cybersecurity skills gap has had an impact on them.

Among the reasons for these security failures: the cybersecurity team isn't big enough (31%); insufficient training for non-technical employees (26%); cybersecurity isn't a high priority for business, and executive management (21%). Nearly 55% say their existing cybersecurity teams are facing heavy workloads given the lack of manpower available such that 35% do not have enough education and training in their security tools to successfully fulfill their jobs. "One of the things leading to some breaches is in fact some lack of cybersecurity talent," says Jon Olsik, Enterprise Strategy Group. "To me, this is an existential threat that changes our strategy on what we have to do in cybersecurity." The survey findings also indicated that security pros feel they don't have adequate time or resources for training to keep up with new threats and defenses." "

Presidential Executive Order

To respond to this critical workforce shortage, President Trump issued an Executive Order in the fall of 2017 that directs the U.S. Secretary of Commerce, in conjunction with the Secretary of Homeland Security and in consultation with other Federal Departments and Agencies, to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future. This includes cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education. The order also calls for a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in the public and private sectors.

<https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure>

CYBERSECURITY

Articles

The articles and links listed below provide additional information about the workforce needs in the cybersecurity field.

Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens (ISC)² CYBERSECURITY WORKFORCE STUDY, 2018

<https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx>

This link summarizes a cyber workforce study done by (ISC). While there are no major revelations in the study, there is some interesting data on education:

- The least important factor in the “Qualifications for Employment (pg.9) was “Cybersecurity or related undergraduate degree.”
- Additionally, 34% reported having a Masters and 39% having a Bachelors, with an average of 13 years in IT, and 7 years on cybersecurity initiatives.

Unraveling the Cyber Skills Gap & Talent Shortage

<https://www.cybrary.it/2018/03/unraveling-cyber-skills-gap-talent-shortage/>

Three Ideas for Solving the Cybersecurity Skills Gap

One possibility: Create a Cybersecurity Peace Corps

<https://www.wsj.com/articles/three-ideas-for-solving-the-cybersecurity-skills-gap-1537322520>

Boosting the Cyberworkforce

Amid persistent shortages in cybersecurity positions, what can states do to strengthen their numbers? [http://www.govtech.com/data/Boosting-the-](http://www.govtech.com/data/Boosting-the-Cyberworkforce.html?mc_cid=6056097651&mc_eid=629541aaa5)

[Cyberworkforce.html?mc_cid=6056097651&mc_eid=629541aaa5](http://www.govtech.com/data/Boosting-the-Cyberworkforce.html?mc_cid=6056097651&mc_eid=629541aaa5)

Cybersecurity Workforce Development: A Primer

<https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/>

Cybersecurity could be WV's next big growth area, leaders say

<http://wvmetronews.com/2017/08/05/cybersecurity-could-be-wvs-next-big-growth-area-leaders-say/>

Why Cyber Security Degrees Are Becoming Increasingly Valuable

http://everydayconsumer.org/why-cyber-security-degrees-are-becoming-increasingly-valuable?articleid=1059&&utm_campaign=1410658&utm_medium=msn-defaulthomepage&utm_source=300192

5. Cyber Threats

Cyber threats facing the United States come from several primary sources: international governments, criminal elements and individual hackers. And, generally, these take the forms of the following:

- Industrial IoT Hacks
- Ransomware
- Phishing
- Internal threats, data thefts
- Denial of service

"Connected devices are essential to our professional and personal lives, and criminals have gravitated to these platforms as well. Many common crimes—like theft, fraud, harassment, and abuse—are now carried out online, using new technologies and tactics. Others, like cyber intrusions and attacks on critical infrastructure, have emerged as our dependence on connected systems revealed new vulnerabilities. Successfully mitigating these threats relies on a combination of information sharing, prevention efforts, and enforcement work. Government agencies, law enforcement, the private sector, and individuals all have a role to play."

Source: FBI, <https://www.fbi.gov/news/stories/ncscom-2018>

The threats and costs associated with cybersecurity crimes are increasing and becoming more and more complex. It is projected that cyber crime damage costs are projected to hit \$6 trillion annually by 2021.

Source: *Top 5 cybersecurity facts, figures and statistics for 2018*

Predictions and observations provide a 30,000-foot view of the cybersecurity industry

<https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>

CYBERSECURITY

6. Cyber Employment and Economic Opportunities in West Virginia

Cybersecurity jobs exist in West Virginia, and many of these jobs are clustered in a few areas:

- Northcentral West Virginia (Harrison, Marion and Monongalia Counties)
 - Federal agencies including the FBI, NASA, NOAA, NETL and the U.S. Dept. of Commerce
 - Businesses such as Northrop Grumman, Leidos, ManTech, General Dynamics IT, IBS Corporation, Fusion Technology, XO Security, Sevatec and Critical Solutions
- Rocket Center (Mineral County)
 - IBM
 - Northrop Grumman
- Eastern Panhandle (Berkeley and Jefferson Counties)
 - Coast Guard
 - Office of Personnel Management

In addition, a variety of cybersecurity jobs are embedded in hospitals, banks, local governments and in state government.

In early 2019 there will be an effort made to better quantify these jobs and to highlight those employers in West Virginia who have cybersecurity jobs and openings.

7. Cyber Learning Opportunities in West Virginia

There are a variety of learning opportunities in West Virginia for those interested in cybersecurity. These opportunities begin in high school and progress to a Master's level.

Five four-year institutions of higher learning in West Virginia currently provide cybersecurity degrees:

1. Alderson Broaddus University
2. Fairmont State University
3. Marshall University
4. University of Charleston
5. West Virginia University

Two other institutions are developing new cyber programs. Bethany College is developing a new B.S. in Cybersecurity, and Bluefield State University is planning to offer a minor in cybersecurity.

Cyber education overviews from each are provided below. These also include information on how the institutions are working to provide "hands on" learning experiences and skills.

Alderson Broaddus University

1. An overview of your institution's cybersecurity offerings and specialties

Alderson Broaddus University started a new higher education program on cyber security in Fall 2018. The program is firmly grounded in the computer science and engineering discipline, with extensive opportunities for hands-on practical and industry level applications. The program offers a number of academic degrees that provide student teachings in a broad range of knowledge areas through a rich, robust, and industry-focused cybersecurity curriculum.

AB's cybersecurity program is created with a vision to ensure the provisioning of fundamental knowledge and practical hands-on experience that comprise the major areas of cyber security science. This vision is emphasized in the program design, academic plans, and curricular considerations. The curricula of AB's cybersecurity programs are structured based on the academic requirements of the NSA DHS National Centers of Academic Excellence in Cyber Defense. All coursework related to computer science is structured based on the IEEE/ACM 2013 standards for computer science programs.

Through a firm engagement with cybersecurity industry, Alderson Broaddus University assures the consideration of the contemporary domain challenges and the latest cyberspace technology in the program teachings. A board of university industry alliance advisory provides informed guidance to the cybersecurity program on the campus and shares expertise and knowledge by reviewing program curriculum, facilities, equipment, budget, etc.

The main goal of AB's cybersecurity program is to produce skilled professionals with practical cyber defense expertise strengthened by computing and information technology skillsets. The program will prepare AB's students for the multi-disciplinary aspects of securing software, networks, web and mobile systems. Through different program terms and specializations, AB's degree programs provide options for students to pursue careers of interests in both general and industry-specific cybersecurity domains.

Program Mission and learning outcomes

The mission of the Cyber Security program at Alderson Broaddus University is to provide a Bachelor of Science degree in Cyber Security consistent with the university mission that prepares students to protect against attackers and malicious activities, design secure software systems, assure information security, and understand professional, ethical and legal responsibilities.

CYBERSECURITY

The program enables students to attain the following goals by the time of graduation.

1. Use and apply knowledge of computing and mathematics appropriate to the discipline.
2. Apply knowledge of cyber security to protect against attackers and malicious activities.
3. Design and develop secure software systems.
4. Protect against network threats and internet hijacks.
5. Assure information security and implement secure system access control.
6. Design security methods and secure algorithms using cypher communication.
7. Demonstrate professional, ethical, legal, security and social issues and responsibilities.
8. Utilize advanced security techniques in the fields of digital forensics, healthcare informatics, or cyber security management.
9. Use current techniques, skills, and tools necessary for security practices.

Degree Programs:

Bachelor of Science degree in Cyber Security

The BS degree in cybersecurity is a four-year program with three concentrations on digital forensics, healthcare security, and cybersecurity management. In its main stream, the BS degree will prepare students in a broad range of cyberspace disciplines including secure software, networks security, web and mobile system security. The program provides students with the required knowledge and skillsets to take strong leadership roles in protecting organizations' information infrastructures and mobilize appropriate resources to maintain stable operations. In addition to the broad knowledge about the state-of-the-art methods and techniques of cybersecurity, students will be equipped with the required knowledge base and expertise to foster new security solutions to defend against cyber-attacks and all types of malicious activities. Further capacities and tactics will be focused on in this program including the capabilities to combat hacking, intrusion, and other cyber threats and to assure information system's secure access and to construct new cryptographic methods and secure algorithms in cypher communication. Moreover, students will be acquainted with the existing software vulnerabilities and the methodologies to design and development secure software systems and consider the suitable countermeasures in these systems with respect to the prevention of, detection of, reaction against, and recovering from cyber-attacks. Furthermore, they will be able to guide and prepare organizations to the compliance with the latest cybersecurity standards.

Through a set of elective courses, the students will extend their learning with the knowledge about valuating technology assets and the risks of cyber threats associated with them. It also enriches their intellect with the methodologies to critically analyze an organization's risk profile, implement a suitable risk mitigation strategy, and protect from unauthorized disclosure, modification, or withholding of information resources. Through the program's elective courses, the students will be exposed to the latest tools and resources for monitoring and defending cyber activities. Other cybersecurity management skills include the capabilities to analyze network traffic and identify malicious activities at the communication and application levels. Students will be able to apply their learnings on digital forensics to investigate computing scenes, detect security breaches, and assure containment. They will be also capable of conducting forensic analysis methods at multiple high- and low-level technology tiers including application, system, software, network, and communication. They will also be equipped with ethical computer hacking tactics to conduct digital forensic activities by following the fundamental principles and legal considerations. Further concentration will be on healthcare security. The healthcare security concentration will prepare students to take an effective role in securing healthcare informatics by extending their learning to the specific features and security requirements of medical organizations. Understanding the nature of medical and clinical data, as well as the ethical and privacy concerns of this data is a vital goal of this concentration. Students will also be acquainted with basic knowledge about the main activities in the healthcare process, the major technology resources of medical organizations, and the fundamental security techniques to secure the healthcare

activities of these organizations. This knowledge will also enable the student's capabilities to perform cyber risk analysis and security management activities of medical organizations.

Minor degree in Cyber security

The minor degree in cybersecurity allows students in other disciplines (e.g., computer science and business administration) to supplement their major degrees with basic cybersecurity skills. In addition to improving their professional expertise and career plans, these students will be prepared to take effective cybersecurity roles in their specific domains. Students in these programs will learn the basic knowledge of cybersecurity and the broad aspects of cyber threats and security countermeasures. They will focus their cybersecurity learning on network and internet security in addition to the underlying knowledge about computer science and computer networks.

Associate degree in Cyber security

The associate degree in cybersecurity is a two-year program that allows students to start their career path earlier by focusing their learning on core cybersecurity knowledge areas appropriate to most employers. Then, these graduates can pursue further education, training, or certification tracks according to their employer needs. Students in this program will learn the basic knowledge of cybersecurity and the broad aspects of cyber threats and security countermeasures. They will focus their cybersecurity learning on network, internet, and software security in addition to the underlying knowledge about computer science, software design, computer architecture, and computer networks.

2. Ensuring the provisioning of hands-on experiences with the latest tools and technology

The cyber security program at Alderson Broadus University is created with a vision to ensure the provisioning of practical hands-on experience. This vision is emphasized in the program design aspects as follows:

- **Program design philosophy**

At AB, we believe that native and robust cyber security solutions are mostly implemented at the low level of computing and engineering domains. Thus, our cybersecurity program will produce skilled professionals with practical cyber defense expertise strengthened by computing and information technology skillsets.

- **Curriculum design**

The curricula of our cybersecurity programs are structured based on the academic requirements of the NSA/DHS National Centers of Academic Excellence in Cyber Defense.

- **Program scope**

Our Cyber Security program prepares students in a broad range of cyberspace disciplines including secure software, networks security, web and mobile security, information and system security, cyber risk management, ethical hacking, digital forensics, security operation technology, in addition to system administration, cryptography, software and system programming, database systems, and others.

- **Program learning outcomes**

The program provides broad knowledge about the state-of-the-art methods and techniques of cybersecurity. Students will be equipped with the required knowledge base and expertise to foster new security solutions to defend against cyber-attacks and all types of malicious activities. Further capacities and tactics will be focused in this program including the capabilities to combat hacking, intrusion, and other cyber threats and to assure information system's secure access and to construct new cryptographic methods and secure algorithms in cypher communication.

CYBERSECURITY

· Lab work in program courses

Since most of the program courses are practical and require hands-on skills, the courses are designed to include extra 1-credit hour of lab work. Labs are designed based on the state-of-the-art techniques as well as the ongoing needs of industry.

· Industry Alliance

Through a firm engagement with cybersecurity industry, AB assures the consideration of the contemporary domain challenges and the latest cyberspace technology in the program teachings. A board of university-industry alliance advisory provides informed guidance to the cyber security program on the campus and shares expertise and knowledge by reviewing program curricula, facilities, equipment, budget, etc. The Industry alliance board also assists in locating needed resources and help strengthens the program graduates' quality and improve their employment opportunities, among several other responsibilities.

· Concentrations

Through different program terms and specializations, our degree programs provide options for students to pursue careers of interests in both general and industry-specific cybersecurity domains. Through a set of elective courses, students will be able to extend their learning in special knowledge areas, namely, digital forensics, healthcare security, and cybersecurity management.

Fairmont State University

The Center of Excellence (COE) for Cyber at Fairmont State University (Fairmont State) provides the leadership and best practices necessary for the cyber-related challenges of tomorrow. The Center is a collaboration among multiple disciplines throughout the University allowing it to be more efficient and effective at providing the next generation workforce to the world. The Center is that logical grouping of disciplines that in isolation provide value-added disciplined scientists, engineers and managers, etc. In order to combat tomorrow's challenges however, industry and government cannot rely on disciplined/isolated solutions. A holistic solution is needed to solve tomorrow's cyber-related challenges, an integrated capability, in which we can leverage the strengths from each of the specialized disciplines to produce the highest quality graduates armed with a breadth of knowledge, skills, and capabilities.

The COE for Cyber has integrated the University's capabilities related to the Cyber-disciplines to ensure the curriculums are relevant, practical experiential learning, state-of-the-art, and produce the highest quality graduates. The Center includes the disciplines of computer science, cyber security, national security and intelligence, information systems management, and robotics. Integrating these capabilities into a Center of Excellence enables the University to be more efficient with its resources while increasing the quality of education and services it provides not only to its students but to its customers across industry and government.

Fairmont State University Capabilities:

Computer Science with a Concentration in Cybersecurity

The Bachelors of Science Degree in Computer Science with a concentration in Cybersecurity at Fairmont State offers extensive hand-on experience through the incorporation of rigorous laboratory sections and/or coding projects in all the main cybersecurity courses.

In Fundamentals of Computer Security, students acquire hands-on laboratory experience starting the second week and continuing on a bi weekly basis throughout the semester. In the lab, students learn how to navigate the Linux command line, OpenSSL encryption, crack passwords using Kali Linux, manipulate Linux environment variables

CYBERSECURITY

and file permissions like set-UID, and perform the BASH exploit Shellshock. Students also learn about secure application coding by implementing a buffer overflow attack in C.

In Cryptography, students learn to implement encryption and decryption algorithms in C++, starting with ancient Roman ciphers and progressing through modern ciphers including the symmetric DES and AES ciphers and the asymmetric RSA encryption algorithm.

In Network Security, students learn basic networking and fundamental principles of network security as well as intermediate network attacks and countermeasures. In the separate lab section, students explore tracking cookies, examine and implement C code for packet sniffing and constructing raw packets, use the Linux netwox toolkit and built-in Kali Linux tools to perform and counter ARP poisoning, Denial of Service attacks, and TCP session breaking and hijacking for remote code injection. Students learn networking security principles by hands on configuration exercises with Cisco wireless routers, Cisco adaptive security appliances, and Linux firewalls and application proxies.

In Vulnerability Assessment, the Cybersecurity capstone course, students learn to analyze computer system vulnerabilities by working through a variety of actual and theoretical security breach scenarios. In a controlled lab environment, students acquire hands-on experience by directly examining several common vulnerabilities and countermeasures, including cross site scripting, sql injection, and Android malware and rootkits. They also perform pen testing experiments using Kali Linux and compete in a “capture the flag” pen testing competition. We have partnered with the Networking and IT department at Fairmont State, allowing students to gain professional skills by deploying two common vulnerability scanner software systems, NMAP and Nessus Home, and creating vulnerability assessment reports of various networks on campus that they present, as a group, to campus networking professionals. In the future, we are adding training with the popular SIEM software QRadar through a series of exercises implementing and operating a small scale SOC in the cybersecurity lab on campus

National Security and Intelligence (NSI) Program

The biggest demand at the federal level is in the Departments of State, Defense, Justice, and Homeland Security, as well as the traditional opportunities at the Central Intelligence and National Security Agencies. The NSI program is designed to provide students with the tools they need to pursue those career goals as research and/or intelligence analysts.

The Open Source Intelligence Exchange (OSIX) is the laboratory and applied research component of the University's NSI program. Student analysts work with faculty mentors to engage in intelligence gathering from open sources. OSIX students receive state of the art practical experience and share their work with real customers in the national security and law enforcement communities. The CIA, FBI, Department of Defense, and Department of State, as well as to state and local law enforcement agencies in West Virginia have received intelligence products from Open Source Intelligence Exchange students.

Information Systems Management (ISM) Program

Fairmont State University offers a Bachelor's of Science (BS) degree in Information Systems Management (ISM) that encompasses operating systems and network technologies, software application development, web technologies for mobile and cloud platforms, software application testing and secure coding, big data and data analytics, machine learning principles and tools, information assurance and cyber security, and project management principles and practices.

Along with a breadth of topics the students complement their knowledge by gaining real world experiences on projects related to Enterprise Networks and Solutions, Project Management, Software Application Development and Testing, and Information Assurance and Cyber Security. Some example projects include working with local police

CYBERSECURITY

department's students provided threat analysis and vulnerability assessments on local law enforcement IT infrastructure. Students developed image processing software used for identifying threats in seized digital assets. Students developed machine learning applications that utilized open source social media data for threat intelligence. Students also provided threat and risk assessments for local businesses near campus.

Automation and Robotics

Fairmont State University offers a minor in Automation and Robotics which provides a multidisciplinary approach for the skills and knowledge needed to design, implement, and troubleshoot embedded, automation, and robotic systems that are being realized across multiple industries such as manufacturing facilities, healthcare industry, automotive industry, power generation plants, etc.. With an increase in these technologies it is important for students within the Mechanical and Electrical Engineering or Computer Science programs to be able to complement their discipline knowledge with a minor in automation and robotics.

Fairmont State hosts several state, regional, and national robotics competitions throughout the year providing all of its students with hands on practical experiences. These robotic initiatives have grown considerably across the state increasing the interest of future students but in industry realizing there is a workforce in WV that can be relied upon.

Resource Needs:

The state-of-the-practice experiential learning obtained at Fairmont State University in Computer Science, Cybersecurity, National Security and Intelligence, and Information Systems Management prepares students to be leading members of the cybersecurity workforce in West Virginia and the nation.

Our forward-thinking field experts and scholars have positioned Fairmont State University to be a leading authority in educating the future workforce of West Virginia (WV). The experiential learning conducted in the classrooms is a result of the collaborations established with industry and government. These collaborations help ensure the curricula are at the cusp of innovation, relevant and valuable to government, industry and to students.

To continue this exceptional service and push to greater heights, Fairmont State University seeks to become a NSA National Center of Academic Excellence in Cyber Operations and a DIA Intelligent Community Center of Academic Excellence.

Financial resources in the amount of \$1.6 million are sought to achieve the vision outlined above, and the specifics outlined below. This funding will enable Fairmont State University to position West Virginia and the University as the hub for Cybersecurity in the nation.

Tools and computing resources:

- Security Operations Center (SOC) – establishing a SOC on the University campus to secure the University's digital assets as well as local towns and state governments that wish to utilize the resource. This Operations center would enable advanced research to be conducted to grow the University's research capabilities as well as provide experiential learning to its students.
- Cyber range in the cloud – establishing hands-on cybersecurity learning is paramount to fulfilling the needs of industry and government. To date, Fairmont State University has done a tremendous job in providing hands-on learning in the classrooms. With the University's aging laboratories, funding is needed to enhance its classroom laboratories as well as support advanced research conducted by the faculty.
- Open Source Intelligence Exchange (OSIX) – the OSIX laboratory and applied research component of the National Security and Intelligence (NSI) program provides exceptional learning opportunities for the University's students to put into practice what is taught in the classroom. The OSIX laboratory is also a major service provider to the Intelligent Community within the state of WV. Additional resources are needed to enhance the laboratory's computing platforms as well as well as enhance the software tools utilized.

CYBERSECURITY

- Community Outreach – Additional funding will support the online delivery of courses across the state to all of WV's high schools to better prepare the high schools students to enter the cybersecurity disciplines. Advanced cyber labs will be established with all the high schools across the state, connected to Fairmont State's cyber-labs so that training and skill development can be provided remotely across the state by University professors.
- Professors, Certifications, and Curriculum Development:
 - All cybersecurity-related classes offered at the University provide real world, hands-on semester projects in order to enhance the student's practical skills as well as allow the University to be a leading service provider in the state. Additional internships and collaborations are required for these kinds of value-added projects and must be integrated across the state.
 - Additional professors are needed to support the growing demand of cybersecurity students. Three professors will be added to the cybersecurity disciplines in order to support the growing need of classes as well as to conduct cutting-edge research to address cybersecurity challenges.
 - Masters of Business Administration (MBA) concentration in cybersecurity will be established in the Fall of 2019 to enhance the knowledge, skills, and abilities of the professionals working in the state of WV.
 - The University will establish collaborations with appropriate organizations. Certifications in cybersecurity will be offered to Fairmont State University's students and to the public at-large. The University will offer training and testing facilities/materials such that its trainees can affordably acquire the certifications required by the government and industry.
 - The University will establish a conduit for Veterans, active duty reservists, and Guard men and women to utilize their unique skills and abilities. This initiative will advance offerings of the University by providing advanced strategies (computing platforms, remote offerings, etc.). It will also make the training and University degrees more accessible via online classes to better serve the needs of this population throughout the state and the nation.
 - The University will establish a mentoring program and advanced training facility for the workforce of WV to be retrained in the cybersecurity-disciplines. The workforce in WV needs to have an avenue to retool and be retrained in new skills. The University's coaching and mentoring program will help retrain members of the nation's armed services coming off active duty, employees that have been displaced, and employees that desire a career change.
 - Fairmont State University is a force multiplier in addressing the workforce challenges facing the state.

Marshall University

Marshall University provides cybersecurity offerings at both the College of Information Technology and Engineering (CITE) and within the Digital Forensics and Information Assurance (DFIA) program.

Marshall University College of Information Technology and Engineering (CITE)

1. An overview of cybersecurity offerings and specialties

The College of Information Technology and Engineering (CITE) has an aggressive plan to produce hundreds of undergraduate and graduate students every year in Computer Science, Information Systems, Computer and Information Security, and Cybersecurity. The Weisberg Division of Computer Science in CITE at Marshall University offers a new Bachelor of Science (BS) degree program in Computer and Information Security beginning in fall 2018. CITE has also offered an online Graduate Certificate in Information Security with 15 hours of course credit for many years for students pursuing security positions in the federal and private sectors.

The MS in Information Systems and the MS in Technology Management in CITE incorporate elements of Cybersecurity in the curriculum that will allow key personnel in the managerial capacity to properly design, manage and strengthen the security of their cyber infrastructure. The current offering of BS and MS in Computer Science provide critical elements needed for Cybersecurity professionals such as networking, data

CYBERSECURITY

analysis and programming. CITE is discussing the potential with many industries and partners to create pathways for students' success with internships and co-op programs. The College is also working on the development of 2+2 with community and technical colleges.

Collaborative and cutting-edge research in cybersecurity is expected to be conducted in partnership with other universities and research institutions along with industries and government entities at the state and federal level. Current faculty research in the Weisberg Division of Computer Science includes cryptography, IoT security, mobile and wireless network security, penetration testing and prevention, and more.

The Division is specifically committed to ensuring that the graduates from the program will strengthen the Cybersecurity workforce and fill in the current needs. The degree programs offered and its graduates will contribute to West Virginia's economic development and advance its competitive edge regionally, nationally and globally.

2. Information about how the institution is ensuring that cyber graduates have "hands-on experience with the latest tools and techniques ready to hit the ground running."

The Weisberg Division of Computer Science aims to strengthen the quality of the program through several focuses:

- *Strength of Knowledge Body:*
The BS in Computer Science program in the Weisberg Division of Computer Science at Marshall University recently received accreditation from the Accreditation Board for Engineering and Technology (ABET) and we expect the new BS in Computer Science and Information Security program will be among the first programs in the nation to earn ABET accreditation as well. The curriculum for the Bachelor of Science in Computer and Information Security is designed to meet the requirements of ABET's Computing Accreditation Commission for Cybersecurity. This ensures that the course offerings and the topics covered are in accordance to the current and future needs of Cybersecurity professionals. In addition, the curriculum is also aligned with Knowledge Unit (KU) requirements of the National Center for Academic Excellence in Cyber Defense (CAE-CD) sponsored by the Department of Homeland Security (DHS) and the National Security Agency (NSA). The CAE-CD Knowledge Unit requirement will ensure each graduate to have critical core technical and non-technical knowledge along with an optional knowledge unit that covers specific topics in the field of Cybersecurity. By aligning the curriculum with two national standards, graduates of the program will have the necessary and most up-to-date skills and knowledge that are currently needed in the field of Cybersecurity. In addition, the curriculum will also prepare students to obtain Cybersecurity certifications that are currently used in the industry such as the Certified Ethical Hacker (CEH), Palo Alto Networks Certified Network Security Engineer (PCNSE), Certified Information Systems Security Professional (CISSP), Cisco Certified Network Associate Security (CCNA-Security) and CompTIA Security+.
- *Strength of Research:*
Faculty of the Weisberg Division of Computer Science are constantly engaged in scholarly activities related to Cybersecurity. The research encompasses the fields of Wireless Security, Data Analytics, Machine Learning and Internet of Things Security that will enrich the academic side of the program along with opening opportunities for students to be the producer of future technologies.
- *Strength of Experience:*
Students in the Computer and Information Security program will be involved with Cybersecurity projects through internships and research projects. The curriculum requires students to complete at least one semester of internship prior to graduation. In addition, students will also participate in competitive events and activities such as the National Collegiate Cyber Defense Competition and DEFCON contest among others. Students will also be expected to increase interest in the field of

CYBERSECURITY

Cybersecurity by providing mentoring to youth groups through activities such as the Cyber Patriot Camp and the Cyber Patriot Competition. The Division successfully hosted the first and only Cyber Patriot Camp in West Virginia in July 2018 and will continue to offer the camp along with the advanced Cyber Patriot Camp in the following years.

- *Strength of Collaboration:*
The Weisberg Division of Computer Science has existing collaboration with federal and state entities along with industry collaboration that will allow internship opportunities and placement of graduates in the cybersecurity field immediately after graduation. The strength of collaboration will also open the opportunity to imbue the course offerings to include the latest and cutting edge topics in the field of Cybersecurity. The Division is also planning to partner with other higher education institutions in the area to create a 2+2 agreement, faculty exchange and other collaborations that will ensure that graduates of the program will be able to meet and exceed the current requirement for a cybersecurity professional.
- *Strength of Infrastructure:*
The Division houses several labs including a networking and cybersecurity lab that incorporates an internal network within the lab which allows for full environment simulation that reproduces a target environment, as closely as possible, rather than relying on virtual machines and virtual networks. For example, the lab will allow students to practice penetration testing through the simulation of a corporate environment within the lab without affecting the existing university network. This lab is housed in the Arthur Weisberg Family Applied Engineering Complex and is the only one of its kind at Marshall University.

3. Details on what additional resources, if any, will be needed by your institution to provide more or expanded learning opportunities to meet the growing employment opportunities in the cybersecurity world.

The Weisberg Division of Computer Science in CITE at Marshall University offers the B.S. in Computer and Information Security and the M.S. in Cybersecurity program (waiting for BOG approval). The curricular of the programs were designed to satisfy the ABET Cybersecurity accreditation and cover core Knowledge Unit (KU) of National Centers of Academic Excellence in Cyber Defense (CAE-CD). Faculty members in the Weisberg Division of Computer Science have demonstrated expertise in the area of cybersecurity with strong research and publication records. Their specific interests include security in computers and networks, mobile and wireless networking, Internet of Things (IoT), cloud computing, and quantum computing, etc. The division is very active in K-12 education in Cybersecurity working with local middle/high schools and hosted the first and only Cyber Patriot Camp in West Virginia in summer and plan to provide training/retraining of cybersecurity workforce in WV at entry-level cybersecurity jobs. Since employers frequently look to certification as an important measure of excellence and commitment to quality, we examine possible cybersecurity certificate programs in the division preparing students for cybersecurity job market without going through regular degree programs such as CompTIA Security+, GIAC Security Essentials at the entry level as well as more advanced level certification such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Information Security Manager (CISM). The division runs multiple state-of-the-art computer labs for teaching and research including dedicated Cybersecurity lab. Based on division's interest and plan for providing advanced and expanded learning opportunities to students and building workforce in cybersecurity fields, following additional resources will be very beneficial:

CYBERSECURITY

1. Building Academic Partnership to provide cybersecurity certifications

Establishing partnership(s) with certification entities in cybersecurity will cost extra fee and expense to the division but students will have better access to the learning and testing materials and reduce the certification exam fee.

2. Equipment and maintenance of facility:

To properly utilize the existing infrastructure built into the networking and cybersecurity lab and other computer labs at the College of Information Technology and Engineering, the labs will need to be supplemented with various software and hardware that can emulate various cyber infrastructures that are currently used in the field. Networking hardware along with sandbox server will allow students to have hands-on experience with actual cyber infrastructure. To emulate a Secure Operations Center (SOC), labs with display wall that can provide situational awareness of the current state of the infrastructure. In addition, to ensure that such software and hardware are properly deployed and maintained and student assistants will need to oversee the day-to-day operation of the lab both for academic and scholarly activities. Lab assistants will assist the lab administrator hired by Marshall University to develop and deploy the lab for classroom and research activities.

Based on our Strategic Plan submitted above in Aug. 2018, we request following *estimated* budget* to support it:

Item	Description	Qty	Amount
Networking Equipment	Networking equipment for SOC	5	\$50,000
Servers	SOC Sandbox Servers to run virtual machines	3	\$12,000
Displays	SOC Scoreboard display	2	\$10,000
Student Assistants	Four student assistants working 20 hours/week for \$12/hour per year (50 weeks)	4	\$48,000
Academic Partnership	Academic Partnership Membership and Service Fee	5	\$10,000
Certificate Exam Fee	Vouchers for students to take certifications exams	100	\$10,000
Total			\$140,000

* -The budget above is to support and cover the initial costs for one year without any indirect cost involved. For a 5-year plan, financial resources in the amount of \$700,000 will be needed to achieve the vision outlined above --supporting more labs and increased number of students in the programs.

Marshall University Digital Forensics & Information Assurance

The Marshall University Digital Forensics and Information Assurance program produces graduates that can use science and technology to solve investigative and cyber security problems. The program is practitioner focused, intent on providing students with the education and skills they need to help fill the cyber security skills gap. The DFIA program emphasizes critical thinking, problem solving, and communication. The curriculum is delivered in a challenging, hands-on environment, using many of the same professional tools, techniques, and procedures they will use upon entering the workforce. The MU DFIA program is also seeking the NSA and DHS designation for National Centers of Academic Excellence.

Undergraduate Curriculum

Courses taught in the curriculum reflect our focus on the practitioner and the skills and education they need. The curriculum includes cyber security classes that develop both offensive and defensive skills. Some of our courses include Network Penetration and Attack, Network Defense, Cyber Warfare, Web Application Penetration Testing, Applied Digital Forensics, Network Forensics, and Mobile Forensics among others.

All of our core courses contain separate lab sections where students hone their digital forensics and cyber security knowledge and skills. Students get extensive experience using industry standard tools such as AccessData's Forensic Toolkit, Kali Linux, Cellebrite, WireShark, Social Engineering Toolkit (SET), Network Miner, Metasploit, Armitage, NMAP and many others. Students are able to take certification tests for both AccessData and Cellebrite forensic tools.

CYBERSECURITY

MU DFIA Lab exercises focus on building discrete skills that culminate in realistic projects or scenario-driven problems requiring students to apply what they learned during the semester.

These culminating exercises are developed with realism in mind. Take DFIA 460 Applied Digital Forensics for example. At the end of the class, students are given digital evidence from a simulated arson case. The students perform the examination and analysis and deliver a realistic final report. Many of our courses include this type of problem-based learning assignment.

The program concludes with an intense capstone experience where students put their knowledge and skills to the test by working through challenging simulated cases, penetration tests, and real-world cyber security problems. This capstone experience is designed to assess and reinforce the major learning objectives from all of the program's core courses.

Learning Outside the Classroom

The opportunities to learn don't stop when the students leave the classroom. Students are afforded additional skill-building opportunities through internships, research projects, the Colligate Cyber Defense Competition (CCDC) team, and our Open Source Intelligence Exchange (OSIX). The OSIX uses selected, vetted students to do real-world open source intelligence collection and analysis. We do this work for various clients including law enforcement, NASA, the WV Intelligence Fusion Center, and Operation Underground Railroad (OUR). The MU OSIX works closely with Operation Underground Railroad to help fight international child sex trafficking. MU DFIA students have provided intelligence that has assisted in the rescue of 40 children and the arrest of 10 suspected traffickers.

Students also engage in applied research guided by faculty. Some of the research topics include vehicle forensics, voting machines, wearable devices with geolocation, FitBit, etc.

Students can also gain practical skills through several conferences including Blackhat, DerbyCon, AIDE, and SecureWV. Students can attend AIDE and SecureWV free of charge and compete against professionals in capture the flag and network king of the hill events. Our students also have access to the BlackHat Student Internship Program that allows students a paid week helping to organize the BlackHat cyber security conference in Las Vegas. Students are given room and board as well as exclusive access to conference to workshops, lectures, and exclusive VIP networking opportunities.

Looking Ahead

We will be launching a graduate program in Fall 2019. Like our undergraduate program, our MS degree will also be practitioner-focused. We are also working on additional ways to prepare our students to pass the industry standard certifications most often sought by employers. "Bootcamp" style preparation courses are also being planned for the summer of 2019.

As far as additional resources, funding would be at the top of list. We could use money to offset the costs related to development and creation of practical lab exercises, case simulations, table top exercises, and the like. Undergraduate and graduate students, working at the direction of faculty, could provide very cost-effective labor for this effort. Additional funds could also be used to offset the costs for more applied research (i.e. costs of consumer products, software, tools, etc.). Lastly, funding could also be used for student and faculty activities outside the university (conferences, etc.). Another potential need would be administrative assistance to help manage the NSA/DHS CAE program paperwork.

CYBERSECURITY

Marshall University Master's Degree Program in Forensic Science

The Master's degree program in Forensic Science offers an area of emphasis in digital forensics. The course offerings within the digital forensics curriculum merges classroom instruction with practical, laboratory-based training. The latter culminates with students taking the Access Data Exam (ACE), successful completion resulting in a certificate.

Those students pursuing the digital forensics area of emphasis also benefit from having a working digital forensics unit housed within the MU Forensic Science Center. Although our students cannot be directly involved in criminal casework, mock exercises have been developed that simulate actual cases and allow students to use the Cellebrite mobile forensic tool, AccessData FTK 6 and other forensic software. Students have performed research projects on drones, automobiles, Alexa and copy machines to determine the type and amounts of stored data that could serve as evidence in criminal investigations.

Resource Needs:

As far as additional resources are concerned, funding would be at the top of list. Funding would be used for:

- Additional lab, teaching space and equipment.
- Development and creation of more practical, hand-on lab exercises, case simulations, table top exercises, and the like.
- More applied research (i.e. costs of consumer products, software, tools, etc.).
- Student and faculty activities outside the university (conferences, etc.).
- Administrative assistance to help manage the NSA/DHS CAE program paperwork.

Together, this amounts to \$140,000:

- Lab Equip & Furnishings - \$75,000
- Academic Lab Exercise Development - \$10,000
- Test devices for Applied Research - \$10,000
- Student & Faculty External Activities - \$15,000
- Faculty Training - \$15,000
- Admin Support for NSA - \$15,000

University of Charleston

The University of Charleston West Virginia (UCWV) offers two cyber security degrees inclusive of a 2 Year Bachelor of Science in Cyber Security (BSCS) degree completion program emphasizing certifications as a part of the curriculum (e.g. Certified Ethical Hacker, Certified Incident Handler, and Certified Security Analyst). The University will pursue a four year in-seat Bachelors degree to further provide hands on teaching and technical skills for the traditional student exiting high school, amongst other sources. The Masters of Science in Cyber Security (MSCS) emphasizes program management curriculum that has been mapped to the NIST framework, to learn the leadership skills necessary in today's Cyber Operations and Defensive based organizations.

Bachelor's of Science in Cyber Security:

The Bachelor's degree consists of approximately 50% of the curriculum inclusive of hands on techniques, ethical practices, and lab environment activities in partnership with ECCouncil where UCWV is an Accredited Training Center.

Hands on Activities include, but are not limited to:

- Ethical Hacking,
- Incident Handling,
- Security Auditing,
- Initial Forensics,
- Enumeration,
- Network Analysis, and
- Security Trending Analysis.

CYBERSECURITY

The mission of the Bachelor of Science in Cyber Security (BSCS) is to provide graduates within the program with the ability to apply learned skills and experiential knowledge of security technology to make a significant contribution to the information security of individuals, corporations, governmental services and the national community. The following represent the program outcomes for the BSCS:

Outcome 1: The graduate will establish and supervise legal and ethical practices in the cyber security arena.
Outcome 2: The graduate will develop and implement a comprehensive cyber security strategic plan for individuals, corporations, governmental services and/or the national community.
Outcome 3: The graduate will detect, assess, and remediate ongoing cyber security threats and vulnerabilities.
Outcome 4: The graduate will effectively communicate cyber threats and remediation strategies across organizational levels in both verbal and written formats.
Outcome 5: The graduate will integrate technical knowledge, software and hardware capabilities, and threat and vulnerability awareness across varying technology formats such as operating systems, networking, social media, mobile, and handheld devices.

Masters of Science in Cyber Security:

The Master's degree picks up where the Bachelor's degree leaves off where students in the Bachelor's degree can matriculate into the Masters to learn the managerial and leadership skills necessary in today's Cyber Operations and Defensive based organizations.

Hands on Activities include, but are not limited to:

- Financial ROI/NPV Analysis,
- Intelligence Collection and Analysis,
- Data Analytics,
- Cyber Operation Analysis,
- Information Assurance Tactics,
- Synthesis of Legal Cases,
- Research Based on Cyber Trends and Forecasts.

The mission of the Masters of Science in Cyber Security (MSCS) is to educate graduates to make a significant contribution, with a commitment toward moral purpose and productive work, within the information security community in support of individual, corporation, governmental services and organizational strategic goals. The following represent the program outcomes for the MSCS:

Outcome 1: The graduate will evaluate and defend the mission of an organization requiring security defense by analyzing the needs and costs of creating security related programs and strategies.
Outcome 2: The graduate will analyze the demands of systems security and practiced methodologies for protecting data integrity and confidentiality through ethical practices.
Outcome 3: The graduate will synthesize a variety of challenging policy, legal, and technological concepts in relation to cyber security.
Outcome 4: The graduate will evaluate security theories, apply experiential lessons learned, evaluate new research and generate new research and security models for organization's who require security related and information management strategies.

Workforce and Economic Development Recommendations:

We recommend that a proactive strategy be developed to make West Virginia the nation's leading destination for cyber and information security education. Doing so will require identifying key career pathways, the research and programs needed to prepare people for each pathway, and a collaborative approach to program development across institutions that maximizes pathway impact and minimizes within-state competition.

CYBERSECURITY

A [recent article](#) on cybersecurity degree differentiation across colleges and universities in Indiana illustrates such possibilities. While the distinct character of the IU, Purdue and other programs may not have been intentional from an indirect competition standpoint, being strategic in how our WV universities distinguish their cyber programs is a smart model. Being proactive in this regard will pre-empt direct competition between institutions, when we should be competing against other states for students and future workers. Collaborating should also generate positive external equity and open up public-private funding opportunities for all. If done effectively, we can present WV as the nation's leader in cyber security education through offering a rich portfolio of distinct programs across our institutions.

UC welcomes the opportunity to participate in and lead this effort.

Other specific recommendations include:

- Training opportunities in technological initiatives to include building knowledge in programming, analytics, security, intel, operations, defensive tactics, and ethical practices. UC is developing new degree programming in data sciences, coding and computer programming that can be integrated into future cyber programs.
- A shared or collocated cloud-based lab environment would be of assistance to many Statewide resources who can pursue the technical skills necessary through online training programs to include certificates, MOOCs, specific training needs, and/or skill-based offerings as deemed by organizational needs.
- Internship opportunities would also be of added value to funnel individuals through the aforementioned training, while helping to ensure the resources stay within the organization, and within the State of WV.
- Shared research opportunities that can provide the State, organizations, and academic institutions with a shared responsibility to grow cyber knowledge, collectively.

West Virginia University

1) Provide an overview of your institution's cybersecurity offerings, specialties and degrees.

Starting Fall 2018, WVU has expanded its cybersecurity offerings with new degrees and certificates in Computer Science and Business Cybersecurity Management.

Computer Science Offerings:

The new undergraduate degree in [Cybersecurity](#) is offered by the [Lane Department of Computer Science and Electrical Engineering](#) and provides students with a solid foundation in programming, Computer Science, and core technical aspects of Cybersecurity through courses such as Foundations of Cybersecurity, Cybersecurity Principles and Practice, Secure Software Development, Host Based Cyber Defense, Practicing Cybersecurity: Attacks and Countermeasures, and Computer Incident Response. In addition, the program includes interdisciplinary courses in Cryptography, Information Ethics, and Cybercrime to allow a well-rounded perspective on the field. Students will have the chance to choose between electives exploring software design, artificial intelligence, computer forensics, networking and databases.

To supplement the new degree, undergraduate students who are already majoring in Computer Science, Computer Engineering, and Biometrics Systems can add an Area of Emphasis in Cybersecurity which consists of a sequence of five courses; while undergraduate students of other majors can receive a [Minor in Cybersecurity](#), by completing a sequence of six courses.

In addition, WVU is in the process of reorganizing the existing [Graduate Certificate in Computer Forensics](#) as a Graduate Area of Emphasis in Cybersecurity. WVU is designated by NSA/DHS as a [National Center of Academic Excellence in Cyber Defense Education and in Cyber Defense Research](#). The new educational initiatives leverage

CYBERSECURITY

existing strengths and aim to produce work-force ready cybersecurity experts and increase the prospects of enhanced economic development for West Virginia.

Business Cybersecurity Management

The College of Business and Economics now offers a Master of Science in Business Cybersecurity Management (CYBR) and Minor in Business Cybersecurity Management, both situated at the intersection of business and cybersecurity management. The program focuses on developing the managerial and technical skills needed to identify weaknesses, manage vulnerabilities, protect assets, defend networks, and audit the security of information systems. Learning is accomplished in an online environment using hands-on vulnerability assessments, statistical analysis, and risk-based decision making. Business Cybersecurity entails optimizing the management of protection of a company's hardware, software and information assets as well as preventing the disruption or misdirection of those assets. Part of the CYBR initiative in the WVU College of Business & Economics is to help our partner organizations better understand and develop their cybersecurity effectiveness. This allows organizations to partner not only with students, but also with faculty on advanced cybersecurity projects that can result in co-branded publications. West Virginia University is working with IBM and other organizations to provide general IT, software development and cyber security training to increase the number of qualified candidates for in state companies. The first class began in August, 2018, and, with little advertising, has already enrolled 14 graduate students.

- 2) **Provide information about how the institution is ensuring that cyber graduates have "hands-on experience with the latest tools and techniques ready to hit the ground running." This should include addressing this statement by Greg Blaney:**

"NASA IV&V along with the rest of the Federal Agencies are in desperate need of folks possessing both integrity and cyber security skills. And I'm not just talking about academic training; we need folks with hands-on experience with the latest tools and techniques ready to hit the ground running. Here at NASA IV&V, we are setting up a training lab which will allow folks to train in ethical cybersecurity activities as well as participate in cybersecurity competitions. I suggest the more we partner in providing hands-on activities here in the state, the more WV will be able to lead in the cybersecurity area."

The WVU Computer Science Cybersecurity programs include classes with hands-on activities using available tools, programming assignments, and term projects. Moreover, the BS in cybersecurity has two capstone courses for which students will work in groups to design and implement cybersecurity related projects. The Statler College, home of the Lane Department of Computer Science, has excellent working relationships with a number of area businesses including Leidos, KeyLogic, NASA Independent Verification and Validation Facility and the FBI's Criminal Justice Information Services Division; all of these are excellent future partners for internships and training opportunities for students in the Cybersecurity program. Additionally, many governmental employers require applicants to have a degree from a designated Center of Excellence in Cyber Defense, a designation which WVU already has. The formal course offerings are supplemented by less formal cybersecurity related student organizations. In particular, CyberWVU is open to all undergraduate and graduate students. Students and faculty meet regularly, work on different hands-on cybersecurity topics, and compete in multiple competitions throughout the year.

The WVU Business Cybersecurity Management program is suitable for participants from a broad range of backgrounds who have interest in a career in cybersecurity. The program is a combination of online coursework, which allows students the flexibility of maintaining a career, that is augmented by two, two- to three-day residencies where they focus on experiential learning. Coursework includes Business Intelligence, Data Management, Information Security Assurance Management, Data Communications, Network Security, Cybercrime Management, Ethics and Legal Procedures, Fraud Data Analysis, Business Data Visualization and a capstone business cybersecurity practicum class. Learning is heightened through obtaining certifications, working in teams, professional communication, lab based problem solving and engagement with real-world business cyber

CYBERSECURITY

challenges. Project work includes working with a client organization to provide an analysis, data collection and a recommended solution to cybersecurity business problems. Students may also obtain temporary placement with public or private enterprises for professional competence development.

- 3) **Providing details on what additional resources, if any, will be needed by your institution to provide more or expanded learning opportunities to meet the growing employment opportunities in the cybersecurity world. These details will be provided to Matt Turner at the HEPC and the aggregated as part of the final report.**

The high-quality instruction we envision for experiential and hands-on cybersecurity learning, combined with training in research/thought leadership and continuing/executive education, demand an investment in personnel and infrastructure in order to grow and nurture a robust pipeline of cybersecurity talent in WV. Already, both new WVU cybersecurity programs have experienced significant interest even in their first year. Over 100 students are currently enrolled in the CS and Business cyber courses with no advertising of the new majors as of yet. These programs will clearly require additional resources to fully address the pent up demand. The addition of three new faculty lines in each program (total 6 new lines) would significantly accelerate the program development, allowing WVU to leverage existing cybersecurity expertise and our growing industrial and federal partnerships, and to utilize NSA Center of Excellence designations in order to become a regional powerhouse for interdisciplinary cybersecurity education and research. Furthermore, there is significant ancillary benefit to WV by aligning the research efforts of these new hires with regional business priorities. This provides routes to externally funded projects supported by SBIR/STTRs with concomitant economic development opportunities. These new investments in essential faculty require salary and benefits support at the level of \$750K/yr.

In addition to personnel, state-of-the-art programs call for on-campus cybersecurity labs that provide “sandbox” infrastructure to permit simulated cyberattacks, that are as realistic as possible, but that do not compromise functioning university systems. These facilities allow for the hands-on learning that employers expect. Such laboratories consist of a network of devices, including a variety of PCs, as well as mobile devices and industrial controllers, which reflect the assortment of information infrastructure that is subject to cyber attacks. The devices are networked behind a hardware router and firewall to separate them from the university computing network, and allow flexible experimentation for both teaching and research. The sandbox should also include the capability to simulate a larger virtual network of machines in a cloud-environment such as Amazon Web Service, to prepare students for realistic network scenarios. The infrastructure would require a one-time capital investment of \$300K and need the supervision of a paid full-time Teaching Associate with IT experience at the rate of \$75K/year including benefits.

These investments at a critical juncture in the development of the WVU Cybersecurity programs will fast track the programs to provide maximum benefit and opportunity to both WV students and the our growing cybersecurity economy.

In addition, two state higher education institutions are developing new cyber learning opportunities:

Bethany College

Bethany is planning to provide two majors in Cybersecurity: one leading to the Bachelor of Arts degree and the other to the Bachelor of Science degree. The Bachelor of Arts plan is designed for those students seeking a career in information assurance that focus on the identification of threats and vulnerabilities in order to protect business and government digital systems. Students in this major complete courses in programming, project management, computer security, ethics, computer organization and assembly language, network architecture, computer forensics, operating systems, network security, operating system security, principles of management, writing in the field, senior project, and a comprehensive exam at the completion of the program. The Bachelor of Science plan is designed for students seeking a career in cybersecurity focused on the research and development of software and systems for protecting digital assets. Student in this major complete courses in programming, computer security, data structures, computer forensics, two courses in calculus, calculus-based probability and statistics, cryptography,

CYBERSECURITY

numerical analysis, network architecture, network security, operating systems and security, writing in the field, senior project, and a comprehensive exam at the completion of the program.

Bethany plans to ensure the provisioning of hands-on experiences with the latest tools and technology:

ZeroChaos Cybersecurity Lab

Through a donation from ZeroChaos, work force management company, and efforts of a Board of Trustee Doug Goin, the ZeroChaos Cybersecurity air-gap lab has been established on-campus. The lab space is dedicated to the student learning experience in a variety of courses. This set of computers that will operate on a completely separate network to allow students the opportunity to learn in a protected environment.

IBM Mainframe z System Certification

There is high demand in the private sector currently for those individuals who can program mainframes. Bethany College, through an alumni connection, is offering the interested student the opportunity to gain professional certification for his/her skills in working with IBM mainframes. Through the IBM mainframe z System, a foundational knowledge of the COBOL programming language and the IBM "Master the Mainframe" z OS training is being offered for the students. The students are taught an introductory component in the Computer Science I course and then offered a series of trainings to assist them in earning professional certification.

Advisory Board

Alumni, trustees, and members of the community will be serving on an advisory board for the major. The board will advise the program on the skills and technology that the field is looking for from students. This will provide the faculty quick feedback on ways to improve the program and to keep Bethany students current in the field.

Bluefield State College

Bluefield State is in the process of creating a minor in cybersecurity within computer science (with full implementation in 2019), offering the following courses:

- COSC 241 Intro to Linux/Unix (3 CH)
- COSC 342 Computer Forensics (3 CH)
- COSC 382 Penetration Testing (3 CH)
- COSC 404 Ethical Hacking (3 CH)

This minor will be available in 2019.

CYBERSECURITY

8. CyberSecurity Offerings – W.Va. Two-Year Institutions

Provided is information on cybersecurity programs and degrees offered by the state's community & technical college system.

Blue Ridge CTC

The Cyber Security program at Blue Ridge offers an Associate of Applied Science Degree, incorporating vendor certification training, for students preparing for entry-level employment or advancement in a variety of occupations and courses in Cyber Security. The program offers students the opportunity to select one of two tracks; Network Security Hardware or Network Security Application. These two tracks will provide the student with the knowledge to enter the Cyber Security workforce and/or transfer to a four-year institution for further undergraduate education. Students will complete hands-on activities that will provide an overview of basic principles and security concepts related to active mitigation of known common threats. The curriculum discusses risk, threat, and security assessments and utilizing them to develop security policy, business continuity, disaster recovery, and incident response planning. The program also covers security methods, controls and procedures, ethics, laws, and computer forensics. In addition, the program describes the use of cryptography as a tool, software development processes, and protection. Students will develop an understanding of the information assurance progression and how they can apply this knowledge to support their organization. Industry certifications within cyber security include:

- Certiport IC3
- CompTIA A+ (Jumpstart)
- CompTIA Network+
- CompTIA Security+
- Linux LPI I and LPI II --- combined makes CompTIA Linux+
- Cisco Certified Entry Level Network Technician (CCENT)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Associate – Security (CCNA-Security)
- Cisco Certified Network Associate – Wireless (CCNA-Wireless)
- Cisco Certified Network Professional – (CCNP)

BridgeValley CTC

The Cyber Security A.A.S degree program at BridgeValley provides a general background in computer repair, computer networking, internetworking, enterprise computing practices, implementing and maintaining security on computers and networking equipment, and assessing security risks. The breadth of coverage produces a multi-skilled entry-level information technology "jack of all trades" with a high degree of career flexibility in large business organizations and the ability to independently handle the information technology needs of small and medium size businesses. Industry certifications within cyber security include:

- Cisco Certified Entry Networking Technician (CCENT)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Associate Cyber Operations (CCNA Cyber Ops)
- Routing Pro
- Switching Pro
- Security Pro, also eligible to take the CompTIA Security +

CYBERSECURITY

Mountwest CTC

The Associate in Applied Science Degree Program in Network Systems Security offers comprehensive network training from Mountwest Community and Technical College's Microsoft Information Technology Academy and Cisco Networking Academy. Within the two-year Associate Degree program, students take courses developed by Microsoft and Cisco, providing specialized skills in network administration, design, and security. Industry certifications within cyber security include:

- CompTIA's A+ Hardware and Operating Systems
- Microsoft's MCSA: (Microsoft Certified Solutions Associate)
- CompTIA's Linux+
- Cisco's CCNA (Cisco Certified Network Associate)
- CompTIA's Security+
- CompTIA's Server

The program is designed so graduates will be capable of performing network administration, design, maintenance, and security on a variety of network operating systems and devices.

- Microsoft Certified Solutions Associate manage and troubleshoot system environments running the Windows 2008 operating system.
- Cisco Certified Network Associates design, build, and maintain computer networks using a variety of network devices.
- CompTIA Security+ and Cisco Network Security Specialists design and implement security solutions that reduce network vulnerability.
- Cisco Wireless LAN Support Specialists implement and troubleshoot Wireless LANs.

MCTC's Network Systems Security option provides fundamental networking knowledge and skills with specific network security training crucial for entry into information security positions in public corporations and government entities.

Pierpont CTC

The Associate of Applied Science degree in Information Systems Technology with a concentration in Cyber Security provides students with valuable skills and knowledge in computer and network design, installation, support and computer and network security. The program enables and encourages students to learn essential problem-solving skills, industry best-practices, software applications, and core technical skills used by information systems and technology industry professionals. Additional Cyber Security skills will focus on intrusion prevention and detection, proactive support and penetration testing. Industry certifications within cyber security include:

- Cisco CCENT (only AAS)
- CompTIA A+ (only AAS)
- CompTIA Security + (AAS and CAS)
- EC Council CEH
- EC Council CND

CYBERSECURITY

WV Northern CTC

The Associate in Applied Science degree in Computer Information Technology with a concentration in Cyber Security is prepares students to:

- Identify the scope of security problems, identify risk assessment, and describe malicious logic and security policies
- Identify major concepts of theories used in Cloud computing and architecture
- Describe Cloud ROI models, deployment models, and Cloud computing implementation
- Identify hacker attack techniques and methodologies, network worms, viruses, and malicious code, computer crimes, organizational intelligence regarding their technologies, and information technology warfare
- Identify major concepts used in cyber security, and psychological influences of cyber security
- Describe the mentality of a hacker and a hacker's manifesto
- Identify major concepts regarding network security and abnormal networking behavior and its causes
- Describe network defense fundamentals, concepts related to managing firewalls, and the use of Intrusion Detection Systems.

Industry certifications within cyber security include:

- EC- Council CEH
- CompTIA Net +
- CompTIA A +
- Cisco CCNA
- Cisco CCENT
- CompTIA Sec+

WV Northern CTC also has a 2+2 cyber security degree with the University of Charleston.

WVU at Parkersburg

The Associate of Applied Science in Computer and Information Technology gives students a foundation in computer hardware and operating systems, and provides hands-on coursework in network administration through Cisco Networking Academy courses, and systems administration through Microsoft Windows and Linux courses. Industry certifications within cyber security include:

- CompTIA Network+
- Cisco CCNA Security Certification

Proposal: West Virginia Community and Technical College System West Virginia Apprenticeships in Motion (AIM) Program Strategic Plan

West Virginia is now undergoing a diversification and expansion of key business sectors, and one of those is the technology and knowledge-based sector. However, the skills needed for this sector are ones that require specialty and post-secondary education. Recognizing this, policy-makers, state agencies, educational institutions and private entities have developed a workforce solution to meet this industry's requirements and to enable more West Virginia residents to gain the skills to seek employment opportunities in these high tech jobs.

Under the leadership of the West Virginia Development Office and the W.Va. Community and Technical College System, an Apprenticeship in Motion planning team has created and has prepared The West Virginia Community and Technical College System West Virginia Apprenticeships in Motion (AIM) Program Strategic Plan. This plan was built upon the Vision 2020: An Education Blueprint for Two Thousand Twenty (State Code §18B-1D-3), which directed West Virginia's educational institutions to focus on programs which create and retain jobs in the

CYBERSECURITY

state especially among the emerging high-technology, knowledge-based businesses and industries.

The implementation of strategies for the ongoing AIM commitment will take a sector-based approach, beginning with Information Technology, as this sector represents some of the best middle-skill career opportunities for West Virginians. The outreach and engagement strategies will be targeted specifically to this sector during year one. At the same time, the systems change envisioned by AIM will not be exclusive to the IT sector. The plan's implementation will enhance the alignment of the workforce system overall, to the benefit of all participating employers and residents.

The work of the Plan will be carried out by the West Virginia Community and Technical College System and will network with workforce and industry partners committed to implementing the systems change and strategies associated with the plan. A \$4 million grant application has been submitted to the U.S. Department of Labor that, if approved, would provide funding for this plan.

The Apprenticeships in Motion (AIM) Program will focus on the following objectives:

- Develop and launch a branding campaign that will provide visibility to the comprehensive AIM program and all its connecting parts;
- Cultivate interest in high-demand, high-pay middle skill careers focused on IT and cybersecurity;
- Create awareness within the business community about CTCS' AIM program and how they can take advantage of the West Virginia Learn and Earn program;
- Equip adult students with the skills needed to succeed in the workplace and prepare under-employed individuals to upscale within their current employment space, utilizing an on-the-job-training component in high-demand tech career credential programs;
- Develop responsive curriculum in high-demand tech career pathways (including cybersecurity) that are co-developed with industry partners, data-informed and ensure success and career readiness for students; and
- Ensure statewide alignment of a cohesive, demand-driven education, job skills development, and career training system that focuses on developing and delivering student-centered career pathways.

Projected Outcome

- By 2020, 8,000 additional West Virginian adults will have earned post-secondary credentials through the community and technical college work-based learning programs, **including 1,600 through the AIM - information technology program.**

CYBERSECURITY

9. Cybersecurity Education -- K-12

The West Virginia Department of Education has developed a cyber educational plan, which includes curricula and courses that will be available to students in the fall of 2019. These courses will provide a pathway not only to gain knowledge but also to prepare for a cybersecurity industry certification (Security+, CySE+). See Appendix B.

In addition, there are emerging cybersecurity youth programs that are becoming available to young people in West Virginia. These include:

- [GirlsGoCyberStart](#), a free online game of discovery that provides high school girls in West Virginia who are interested in a cybersecurity career with a tool to learn basic cybersecurity skills and test their cyber aptitude;
- CyberPatriots for high school students – <http://www.usecyberpatriot.org/>;
- Marshall's GenCyber camp for high school students in West Virginia; and
- RCB's summer cyber education programs for young people.

CYBERSECURITY

10. Cyber Development Plan – Military and Veterans

The U.S. Department of Defense updated and issued its 2018 Cyber Strategy, and that document represents the Department's vision for addressing this threat and implementing the priorities of the *National Security Strategy* and *National Defense Strategy* for cyberspace. https://media.defense.gov/2018/Sep/18/2002041658/-1/-/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Key among the recommendations is one pertaining to cyber workforce development:

The Department plays an essential role in enhancing the Nation's pool of cyber talent in order to further the goal of increasing national resilience across the private and public sectors. To that end, we will increase our efforts alongside other Federal departments and agencies to promote science, technology, engineering, mathematics, and foreign language (STEM-L) disciplines at the primary and secondary education levels throughout the United States. The Department will also partner with industry and academia to establish standards in training, education, and awareness that will facilitate the growth of cyber talent in the United States.

In West Virginia, the W.Va. National Guard is working to enhance its cybersecurity capabilities. Provided below are a number of recommendations that would complement the WVNG's and state's efforts:

- **Develop Cyber Mountaineer Veterans:** Cyber Mountaineer Veterans would provide veteran with a consolidated resource for information related to cybersecurity opportunities in the state, including cyber education at Community Colleges and four year institutions, information on financial support, and tools to help veteran build a career track in the cyber workforce. Also...credit a database of military and veterans with cyber skills. This would be modeled after a similar program in Virginia: <http://cybervets.virginia.gov>. See more at: <https://governor.virginia.gov/newsroom/newsarticle?articleId=19188#sthash.PEWFJhAd.dpuf>
- **Cyber Vets Training Program**
Create a Cyber Mountaineer Veterans training initiative in partnership with offering by the SANS Institute. The offerings would provide veterans another pathway into the cybersecurity workforce via the SANS VetSuccess Immersion Academy. See more: <https://governor.virginia.gov/newsroom/newsarticle?articleId=19188>
- **WV Cyber Mountaineer Veteran Incentive Program**
Develop a state tax incentive/credit program to cover moving expenses for veterans and retired military who move to West Virginia and either work or consult on cyber activities. Credit will be provided to companies or firms who hire under the Cyber Mountaineer Veterans program (see #1).
- **WV Cyber Corp Network**
Have the WVNG and the WVDPMs outline a civilian cyber response network modeled, in part, after the program that has been set up in Michigan - https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---00_html. This network would be designed to enable quick communication/collaboration about major cyber events, facilitate coordinated training activities and provide for a mechanism for affected entities to seek cyber assistance.
- **Incent CyberPatriot Coaches**
Efforts are underway to expand this program to more schools and students across the state. However, cyber coaches are needed for these new clubs. One idea is to provide paid time off to members of the WVNG who volunteer as coaches for the CyberPatriot Youth Program.

CYBERSECURITY

Training Resources

- **NICCS Cyber Training:** <https://niccs.us-cert.gov/training/veterans>
 - o **FREE training**— veterans can access free cybersecurity training through the Federal Virtual Training Environment (FedVTE).
- **U.S. DHS Cyber Training:** <https://www.blogs.va.gov/VAntage/30058/veterans-can-take-advantage-in-free-cybersecurity-training/>
 - o The Department of Homeland Security (DHS) and Hire Our Heroes have teamed up to offer training for Veterans in cybersecurity, in support of Veterans join our nation's cybersecurity workforce.
 - o DHS's Federal Virtual Training Environment (Fed VTE) offers free online, on-demand cyber security training to government employees and Veterans. Veterans can sign up for an account through the [Hire Our Heroes website](#) and follow instructions through "ID me" to verify veteran status and register for a FedVTE account.

11. Cyber Education Resources

There are a diverse variety of web sites and on-line resources regarding cybersecurity education and workforce training. Among these are:

- a. NIST Cyber Resources - <https://www.nist.gov/topics/cybersecurity>
- b. National Initiative for Cybersecurity Education - <https://www.nist.gov/itl/applied-cybersecurity/nice>
- c. NICE Cybersecurity Workforce Framework: Categorizing and Describing Cybersecurity Work for the Nation: Special Publication 800-181 (Attached) <https://www.nist.gov/news-events/news/2017/08/nist-publishes-nice-cybersecurity-workforce-framework-categorizing-and>
 NICE – National Institute for Cybersecurity Education - <https://www.nist.gov/itl/applied-cybersecurity/nice>
 - i. Cyber career pathway info -<https://www.cyberseek.org/pathway.html>
- d. USDHS NICCS Educational Resources:
 - i. [Cybersecurity Workforce Planning Diagnostic \(PDF\)](#) – see *workforce planning* section
 - ii. [Students' Guide to Cybersecurity Careers \(PDF\)](#)
 - iii. [Teachers' Guide to Engaging Students in Cybersecurity \(PDF\)](#)
- e. NICCS Education and Training Catalog - <https://niccs.us-cert.gov/training/search>
- f. Cybersecurity Supply/Demand Heat Map <http://cyberseek.org/heatmap.html>
- g. National CyberWatch Center's Curriculum Standards (NCC-CSP) <https://www.nationalcyberwatch.org/programs-resources/curriculum/>
- h. NSA/DHS National Centers of Academic Excellence in Cyber Defense
<https://www.usa.gov/resources/educators/centers-academic-excellence/cyber-defense/>
- i. State cyber strategic proposals - http://www.govtech.com/data/Boosting-the-Cyberworkforce.html?mc_cid=6056097651&mc_cid=629541aaa5
- j. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6005833/>

Also, many states are developing and implementing cybersecurity learning and training programs. See a listing provided by the National Governors Association (See Appendix C)

CYBERSECURITY

12. Cybersecurity Workforce Strategic Plan - Recommendations

- 1) Establish a WV Cyber Education/Training Collaboration Consortium in order to increase the number of individuals being trained in cybersecurity, avoid/pre-empt direct competition among institutions, aid overall collaboration to generate positive external equity and open up added public-private funding opportunities. If done effectively, West Virginia can become one of the nation's leaders in cybersecurity education through offering a rich portfolio of distinct programs across our institutions.
- 2) Work with the state's congressional delegation to seek federal funding from agencies, such as the U.S. Department of Homeland Security, to establish a pilot project that would create a statewide Cyber Center of Excellence in West Virginia.
- 3) Work with West Virginia institutions of higher education to become part of a federal cyber scholarship program: US OPM <https://www.sfs.opm.gov/>.
- 4) Work with West Virginia institutions of higher education to become part of the U.S. DOE's Cyberforce Competition program: <https://cyberforcecompetition.com/>. Possibly link with the NETL.
- 5) Consider utilizing WVNET's PEAK professional development portal as a medium for state-wide training opportunities.
- 6) Task WVNET to investigate the cost and resources involved in creating virtual labs/machines for K-12 and higher education.
- 7) Prepare a funding proposal for the FY 2019-20 state budget that provides additional dedicated resources to grow the cybersecurity capabilities of the state's four-year institutions:
 - i. More professional development resources/funds are needed at Fairmont State to ensure faculty and trainers are recruited, retained and skilled
 1. Various resources are needed to fully realize the needed capabilities such as:
 - a. Upgraded computer labs - \$500,000
 - b. Cybersecurity software packages for the class rooms and labs - \$250,000
 - c. Faculty support - \$250,000
 - ii. To better serve the Marshall's students and strengthen the academic program, additional resources will be needed to obtain two components:
 1. *Academic Partnership*
Partnership with entities providing certification in cybersecurity to allow students to have better access to the testing materials and reduce the fee to take the certification. Becoming an academic partner of CompTIA and EC-Council, for example, will allow students to have access to several of the in-demand cybersecurity certifications at a significantly reduced price.
 2. *Equipment and Maintenance of Facility:*
To properly utilize the existing infrastructure built into the networking and cybersecurity lab, the lab will need to be furnished with software and hardware that can emulate various cyber infrastructures that are currently used in the field. In addition, to ensure that such software and hardware are properly deployed and maintained, a lab administrator will need to oversee the day-to-day operation of the lab for both academic and scholarly activities.
 - iii. To continue the expansion of Marshall's cyber and digital forensics programs, expanded funding resources also would help provide:
 1. Additional lab, teaching space and equipment.

2. Development and creation of more practical, hand-on lab exercises, case simulations, table top exercises, and the like.
 3. More applied research (i.e. costs of consumer products, software, tools, etc.).
 4. Student and faculty activities outside the university (conferences, etc.).
 5. Administrative assistance to help manage the NSA/DHS CAE program paperwork.
- iv. To provide for the high-quality instruction envisioned for experiential and hands-on cybersecurity learning, combined with training in research/thought leadership and continuing/executive education, the state's colleges and university will need added investment in personnel and infrastructure in order to grow and nurture a robust pipeline of cybersecurity talent in WV. The state's programs will require additional resources to fully address the pent up demand and to meet the rapidly emerging employment opportunities. At WVU, the addition of three new faculty lines in each program (total 6 new lines) would significantly accelerate the program development, allowing WVU to leverage existing cybersecurity expertise and our growing industrial and federal partnerships, and to utilize NSA Center of Excellence designations in order to become a regional powerhouse for interdisciplinary cybersecurity education and research. Furthermore, there is significant ancillary benefit to WV by aligning the research efforts of these new hires with regional business priorities. This provides routes to externally funded projects supported by SBIR/STTRs with concomitant economic development opportunities. These new investments in essential faculty require salary and benefits support at the level of \$750K/yr.

In addition to personnel, state-of-the-art programs call for on-campus cybersecurity labs that provide "sandbox" infrastructure to permit simulated cyberattacks, that are as realistic as possible, but that do not compromise functioning university systems. These facilities allow for the hands-on learning that employers expect. Such laboratories consist of a network of devices, including a variety of PCs, as well as mobile devices and industrial controllers, which reflect the assortment of information infrastructure that is subject to cyber attacks. The devices are networked behind a hardware router and firewall to separate them from the university computing network, and allow flexible experimentation for both teaching and research. The sandbox should also include the capability to simulate a larger virtual network of machines in a cloud-environment such as Amazon Web Service, to prepare students for realistic network scenarios. The infrastructure would require a one-time capital investment of \$300K and need the supervision of a paid full-time Teaching Associate with IT experience at the rate of \$75K/yr including benefits.

These investments at a critical juncture in the development of the WVU Cybersecurity programs will fast track the programs to provide maximum benefit and opportunity to both WV students and the our growing cybersecurity economy.

8) Enact a new state tax development incentive that would provide high-technology companies a rebate (up to 10%) of payroll taxes for 5 years. Rebate dollars could be used for either capex OR opex. Eligible high-technology companies would be those engaged in one of the following: applications development, coding, e-commerce services, game development, data analytics, cloud services or cybersecurity.

9) Explore e-learning and tele-learning best practices for the support and management of online learning and online adjunct faculty teaching cyber security.

10) Leverage the West Virginia Cyber Education/Training Collaboration Consortium and added state resources to help develop more cyber internship programs. Also consider the development of a Governor's Cyber Internship Program and grants, and an annual Governor's Cybersecurity School during the summer for high school students.

CYBERSECURITY

11) Focus cyber education programs and curricula that address these key employment areas:

- Network operations
- Systems administration
- Cyber monitoring and incident response
- Vulnerability assessment analyst
- Policy development, implementation and adherence

12) Support the W. Va. Dept. of Commerce's and West Virginia Community and Technical College System's \$4 million grant application to the U.S. Department of Labor that, if approved would provide funding for The Apprenticeships in Motion (AIM) Program. This community college program would focus on the following objectives:

- Develop and launch a branding campaign that will provide visibility to the comprehensive AIM program and all its connecting parts;
- Cultivate interest in high-demand, high-pay middle skill careers focused on IT and cybersecurity;
- Create awareness within the business community about CTCS' AIM program and how they can take advantage of the West Virginia Learn and Earn program;
- Equip adult students with the skills needed to succeed in the workplace and prepare under-employed individuals to upscale within their current employment space, utilizing an on-the-job-training component in high-demand tech career credential programs;
- Develop responsive curriculum in high-demand tech career pathways (including cybersecurity) that are co-developed with industry partners, data-informed and ensure success and career readiness for students; and
- Ensure statewide alignment of a cohesive, demand-driven education, job skills development, and career training system that focuses on developing and delivering student-centered career pathways.

13) Develop and fund an ACE (13th year) cybersecurity learning program through the West Virginia Department of Education for recent high school graduates.

14) Develop and host a statewide high school cybersecurity competition and annual event.

15) Continue providing state funds to the West Virginia STEM fund so resources are available to offer mini-grants that will generate the creation of more youth cyber activity programs.

16) Encourage more special programs focused on girls and women to consider cybersecurity as a career choice and field.

17) Develop informational resources to share with students who are interested in pursuing careers in cybersecurity so they understand other key non-education requirements:

- Good credit history
- Appropriate personal behaviors and activities
- No criminal record
- Awareness of critical thinking and soft skills

18) Develop a speaker forum of cyber specialists and employers who could meet with students.

CYBERSECURITY

19) Below are a number of cyber recommendations that would complement the West Virginia National Guard's cybersecurity capabilities and development efforts:

- Cyber Mountaineer Veterans – The creation of Cyber Mountaineer Veterans would provide veterans and military personnel with a consolidated resource for information related to cybersecurity opportunities in the state, including cyber education at Community Colleges and four-year institutions, information on financial support, and tools to help veteran build a career track in the cyber workforce. Also...credit a database of military and veterans with cyber skills. This would be modeled after a similar program in Virginia: <http://cybervets.virginia.gov> See more at: <https://governor.virginia.gov/newsroom/newsarticle?articleId=19188&sthash.PEWfJjAd.dpuf>
- Cyber Vets Training Program - Create a Cyber Mountaineer Veterans training initiative in partnership with offering by the SANS Institute. The offerings would provide veterans another pathway into the cybersecurity workforce via the SANS VetSuccess Immersion Academy. See more: <https://governor.virginia.gov/newsroom/newsarticle?articleId=19188>
- WV Cyber Mountaineer Veteran Incentive Program - Develop a state tax incentive/credit program to cover moving expenses for veterans and retired military who move to West Virginia and either work or consult on cyber activities. Credit will be provided to companies or firms who hire under the Cyber Mountaineer Veterans program (see 1).
- WV Cyber Corp Network - Have the WVNG and the WVDPMs outline a civilian cyber response network modeled, in part, after the program that has been set up in Michigan - https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419--,00.html . This network would be designed to enable quick communication/collaboration about major cyber events, facilitate coordinated training activities and provide for a mechanism for affected entities to seek cyber assistance.
- Incent CyberPatriot Coaches - Efforts are underway to expand this program to more schools and students across the state. However, cyber coaches are needed for these new clubs. One idea is to provide paid time off to members of the WVNG who volunteer as coaches for the CyberPatriot Youth Program.

Other

- Support WVForward's exploration and study effort into how to develop a better, clearer security clearance process for individuals who want to pursue employment in cybersecurity fields. This may involve a sequence of steps to help facilitate easier and faster entry-level employment and then continue with low-cost ways for individuals to get necessary clearances in order to advance.
- Develop new educational programs and degrees that focus on cybersecurity policy. Programs are needed across the country that produce graduates capable of answering questions such as:
 - What existing policies address pressing cybersecurity threats? Where are there gray areas exploitable by malicious actors?
 - Who has jurisdiction when a major cybersecurity attack occurs?
 - What redundancies, contradictions, and gaps are revealed when examining local, state, and federal cybersecurity policy?
 Source: https://www.wilsoncenter.org/sites/default/files/cybersecurity_workforce_preparedness.pdf
- Create a central web portal that will share information on cyber learning programs across the educational continuum as well as list job opportunities, resume postings, internships, sanctioned cyber competitions, etc.

CYBERSECURITY

13. Related Efforts

- **WVForward Security Clearance Roundtable**

WVForward is spearheading a roundtable discussion and work group to analyze the issues associated with the backlog of security clearances nationwide, and to explore how this creates challenges and inhibits job growth for many West Virginia industries, including cybersecurity and federal tech contractors.

- **WVSBDC Cyber Threat Awareness Initiative**

The West Virginia Small Business Development Center has created two new cybersecurity resources for the state's small business community:

- The Small Business Big Threat assessment web site is available at www.smallbusinessbigthreat.com/west-virginia. The "Small Business Big Threat" online course is designed to increase business owners' cybersecurity awareness of threats, prevention and response. The assessment enables business owners to test what they know, review best practices and identify a cybersecurity action plan for their businesses. Suitable for both cyber-savvy and nontechnical owners, the course presents lessons learned from the experience of other small businesses. In the "cybersecurity challenge," the business owner pits his or her knowledge against cyber villains who attack through weaknesses such as data protection, passwords and physical security. Participants who complete the program receive a free Cybersecurity Readiness Checklist.
- The SBDC "Small Business Big Threat" cybersecurity workbook (see attachment or download from the Resources page at www.wvsbdc.com). The booklet includes identification of the most common methods of cyber breaches, the National Institute of Standards and Technology five-part framework to reduce the risk of a cyberattack, cybersecurity tips for small businesses and additional resources.

- **WV Manufacturing Extension Partnership**

The West Virginia Manufacturing Partnership (WVMEP) provides multiple services to small businesses in the area of Cyber Security. Firstly, they partner with cyber security experts from the National Institute of Standards and Technology (NIST) which is the parent organization of the national MEP program, to provide educational workshops on the types, breadth, and depth of the cyber threats. During these workshops the attendees see and hear how the attacks occur, what information the attackers are seeking, and methods to prevent and/or slow down the attacks. Also, there is an overview of the cyber security standards required to do business with the DoD, and general best practices for all businesses. Secondly, the WVMEP has developed a Cyber Security assessment that small businesses can easily understand and utilize to evaluate their level of security and identify weaknesses. This assessment was developed from the NIST Cyber Security assessments and was designed to be a low level evaluation. And finally, the WVMEP will help our clients evaluate the assessment to determine if they need to retain a Cyber Security expert that can do a more detailed assessment and provide countermeasures to the weak areas and ongoing support. The WVMEP has identified qualified experts that provide Cyber Security services in West Virginia.

14. 2019 Activities

Provided are activities planned for 2019 as a continuation of this strategic planning process:

- Quantify Cyber Employment Needs, Opportunities in West Virginia
- Outreach and Awareness Plan
 - WVU, Marshall alumni and students
 - West Virginia business community
 - West Virginia media
- Link with cyber outreach and recruitment plan being developed to focus on military and veterans
 - WV National Guard

CYBERSECURITY

Appendices

- A. List of participants on W.Va. Cybersecurity Workforce Strategic Planning Group
- B. W.Va. Department of Education Cyber Education Plan
- C. NGA Report on State Cyber Workforce Initiatives

WV Cybersecurity Workforce Working Group

Anne	Barth	TCWV	anne@techconnectwv.org
Larry	Malone	Malone Consulting & Strategies	lmalone@malonccs.com
4-Year			
Matt	Turner	HEPC	mturner@hepc.wvnet.edu
Mary	Stewart	WVNET	mstewart@mail.wvnet.edu
Harmony	Garletts	WVNET	hgarletts@mail.wvnet.edu
John	Maher	Marshall University	maherj@marshall.edu
John	Sammons	Marshall University	john.sammons@marshall.edu
Bill	Gardner	Marshall University	bill.gardner@marshall.edu
Terry	Fenger	Marshall University	fenger@marshall.edu
Wook-Sung	Yoo	Marshall University	yoow@marshall.edu
Paulus	Wahjudi	Marshall University	wahjudi@marshall.edu
Wael	Zatar	Marshall University	zatar@marshall.edu
Martin	Roth	University of Charleston	martiroth@ucwv.edu
Michael	Levy	University of Charleston	michaellevy@ucwv.edu
John	Barnette	University of Charleston	johnbarnette@ucwv.edu
Matthew	Gonzalez	University of Charleston	matthewgonzalez@ucwv.edu
EK	Esawi	University of Charleston	eesawi@ucwv.edu
Matt	Harbaugh	WVU	Matt.Harbaugh@mail.wvu.edu
Katerina	Goseva	WVU	katerina.goseva@mail.wvu.edu
Mark	Gavin	WVU	mark.gavin@mail.wvu.edu
Virginia	Kleist	WVU	Virginia.Kleist@mail.wvu.edu
Sheena	Murphy	WVU	sheena.murphy@mail.wvu.edu
Larue	Williams	WVU	Larue.Williams@mail.wvu.edu
Brian	Woerner	WVU	Brian.Woerner@mail.wvu.edu
Priscila	Santos	WVForward	priscila.santos@mail.wvu.edu
Josh	Cook	WVForward	joshua.cook3@mail.wvu.edu
Rocky	Goodwin	WVForward	ragoodwin@mail.wvu.edu
Marcus	Fisher	Fairmont State	mfisher13@fairmontstate.edu
Todd	Clark	Fairmont State	Todd.Clark@fairmontstate.edu
Mirta	Martin	Fairmont State	Mirta.Martin@FairmontState.edu
Tom	Devine	Fairmont State	tdevine1@fairmontstate.edu
Joan	Propst	Alderson Broaddus	propstil@ab.edu
Michael	Bochke	Alderson Broaddus	bochkcmj@ab.edu
Atef	Shalan	Alderson Broaddus	shalanam@ab.edu
Lisa	Reilly	Bethany College	L.Reilly@bethanywv.edu
Naveed	Zaman	WV State University	zamanna@wvstateu.edu
Ted	Lewis	Bluefield State	tlewis@bluefieldstate.edu
Dave	Carrick	WVU Industrial Extension-WV Manufacturing Extension Partnership	David.Carrick@mail.wvu.edu
Gary	Hampton		Gary.WayneHampton@gmail.com

CYBERSECURITY

WV Cybersecurity Workforce Working Group

WV Govt.			
Ashley	Summit	Governor's Office	Ashley.E.Summitt@wv.gov
Jordan	Damron	Governor's Office	Jordan.L.Damron@wv.gov
Jeff	Vandall	WV Development Office	Jeffrey.W.Vandall@wv.gov
Josh	Spence	Office of Technology	Joshua.D.Spence@wv.gov
Jody	Ogle	WV National Guard	jody.w.ogle.mil@mail.mil
Sallie	Milam	WV Privacy Officer	Sallie.H.Milam@wv.gov
Debra	Martin	WVSBDC	Debra.K.Martin@wv.gov
C&TC			
Sarah	Tucker	WVC&TC	tucker@wvctcs.org
Nancy	Ligus	WVC&TC	ligus@wvctcs.org
Bob	Hayton	BridgeValley C&TC	bob.hayton@bridgevalley.edu
Matthew	Demaria	Pierpont C&TC	matthew.demaria@pierpont.edu
Rob	Linger	Pierpont C&TC	Rob.Linger@Pierpont.edu
Mary	Butler	New River C&TC	mbutler@newriver.edu
Jerry	Wallace	New River C&TC	jwallace@newriver.edu
Wendy	Patriquin	New River C&TC	w.patriquin@newriver.edu
Gary	Thompson	WVU-P C&TC	gary.thompson@wvup.edu
Stephen	Smoot	Eastern C&TC	stephen.smoot@easternwv.edu
K-12 Education			
Kathy	D'Antoni	WV Dept. of Education	
Lori	Whitt	WV Dept. of Education	lwhitt@k12.wv.us
Tim	Elliott	WV Dept. of Education	tbelliott@k12.wv.us
Amelia	Courts	Education Alliance	amelia@educationalliance.org
Todd	Ensign	NASA/WV Robotics Alliance	todd.i.ensign@nasa.gov

WV Cybersecurity Workforce Working Group

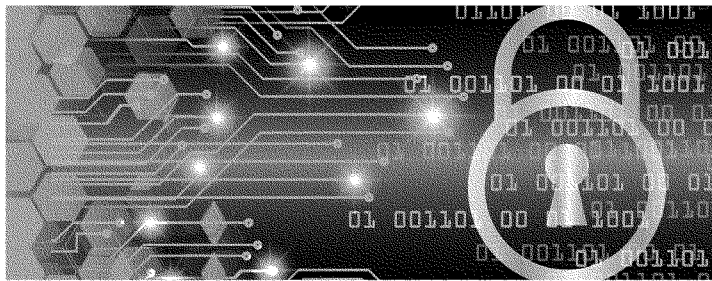
Industry			
Jim	Estep	WV High Tech Foundation	jestep@wyhtf.org
Steve	Morris	IBM	Stephen.L.Morris@ibm.com
Martin	Laird	IBM	lairdmar@us.ibm.com
Craig	Bury	Retired (IBM)	craig.bury@rcn.com
James	Sharpe	CSRA	James.Sharpe@csra.com
Jeff	Tucker	Leidos	Jeffrey.Tucker@leidos.com
Rebecca	Hall-Herndon	NOAA	rebecca.hall-herndon@noaa.gov
Jeffery	Bowmar	US Dept. of Commerce	jbowmar@doc.gov
Daniel	Bollinger	NOAA	daniel.bollinger@noaa.gov
Richie	Wilbur	Advantage Tech	rvilbur@advantagetech.biz
Rob	Dixon	Advantage Tech	rdixon@advantagetech.biz
Jack	Shaffer	Advantage Tech	jshaffer@advantagetech.com
Timi	Hadra	IBM	thadra@us.ibm.com
Trey	Clark	IBM	tclark@us.ibm.com
Cecelia	Schartiger	IBM	schartig@us.ibm.com
Brian	Moats	MPL	bmoats@mpl.com
Brian	Stolarik	Northrop Grumman	Brian.Stolarik@ngc.com
Norm	Gundersen	Global Science and Tech	norman.gundersen@gst.com
Glenn	Copen	Key Logic	gcopen@keylogic.com
Edward	Abraham	FBI/CGIS	elabraham@fbi.gov
Greg	Blaney	NASA IV&V	Gregory.D.Blaney@nasa.gov
Ken	Rehm	NASA IV&V	Kenneth.D.Rehm@nasa.gov
Donald	Ohl	NASA IV&V	Donald.C.Ohl@nasa.gov
Liam	Bowers	Blue Stone Analytics	lbowers@bluestoneanalytics.com
Lindell	Alderman	F5 Networks	lindell.alderman@gmail.com
Jason	Rolleston	McAfee	jrolleston78@gmail.com
Karen	Goodwin	Service Members Opportunities Colleges	karen.goodwin@us.ibm.com
Jim	Spencer	City of Bluefield	jspencer@cityofbluefield.com
Gerard	Eldering	InnovateTech Ventures, LLC	gerard@innovatetech.com
John	Sedoski	National White Collar Crime Ctr.	JSedoski@nw3c.org
Ryan	Thorn	Senator Manchin's Office	Ryan_Thorn@manchin.senate.gov
Aaron	Sporck	Senator Capito's Office	Aaron_Sporck@capito.senate.gov

CYBERSECURITY



1900 Kanawha Boulevard, East, Building 6 • Charleston, WV 25305
wvde.us

WV Cyber Workforce Plan - WVDE Component



The West Virginia Department of Education is committed to providing cyber security preparation to WV students in both K-12 and in Career and Technical Education. The WVDE plan includes an assessment of current policies related to cyber security in K-12, teacher resources and professional development related to cyber security, club and camp activities for students related to cyber security, and a commitment to developing new academic opportunities for students in cyber security. In CTE, the cyber security pathway is clearer, and information related to those programs are included in this plan.

Reaching students with the issues and practices related to cyber security needs to begin in the elementary grade levels, so that students are prepared to understand the problems and solutions related to cyber security as they enter middle- and high-school and become true digital users and producers.

Assessment of current policies related to Cyber Security

Policy 2520.15 contains the West Virginia College- and Career-Readiness Standards for Technology and Computer Science. The language of these standards describes security and privacy as a component of Computer Science, and thus is required to be taught by WV K-12 teachers. "Computer science has a wide range of specialties. These include computer architecture, software systems, programming and coding, graphics design, music technology, robotics & artificial intelligence, web design, security & privacy, computational science, and software engineering. Drawing from a core of computer science knowledge, each specialty area focuses on particular challenges."

CYBERSECURITY

In K-2, the focus is more related to Digital Citizenship.

Digital Citizenship	
TCS.K-2.15	Demonstrate responsible use of technology (i.e., seek guidance and appropriate support when selecting digital content, understand how to be safe online, follow safety rules when using media, etc.).
TCS.K-2.16	Practice using safe, legal, and ethical behavior when using technology.

In 3-5, the focus is still on Digital Citizenship, but deepens to include topics such as online identities, appropriate online interactions, and the importance of keeping personal data private.

Digital Citizenship	
TCS.3-5.20	Practice using safe, legal, and ethical behavior when using technology and interacting online.
TCS.3-5.22	Demonstrate an understanding of the role an online identity plays in the digital world and learn the permanence of decisions made when interacting online.
TCS.3-5.23	Demonstrate appropriate methods of sharing personal data online and how to keep personal data private.

With the move to Middle- and High-School, Digital Citizenship again deepens and begins to include an introduction to Cyber Security which includes, but it not limited to standards such as:

TCS.6-8.16	Demonstrate an understanding of what personal data is and how to keep it private and secure, including the awareness of terms such as encryption, HTTPS, password, cookies and computer viruses; they also understand the limitations of data management and how data-collection technologies work.
------------	---

And

TCS.9-12.16	Keep personal data private and secure, including the awareness of terms such as encryption, HTTPS, password, cookies and computer viruses; understand the limitations of data management and how data-collection technologies work.
-------------	---

In middle- and high-school, however, students also begin to take specific courses in Computer Science, which all include some component of cyber security. The current courses listed in policy include:

Middle School: *Discovering Computer Science*

Discovering Computer Science is designed for students in grades 6-8 and will provide them with opportunities to explore the many facets of Computer Science. This may be taught in a single class in one grade level or divided into sections and taught over a three-year period.

CYBERSECURITY

Standards related to cyber security:

TCS.DCS.25	Demonstrate good practices in personal information security, using passwords, encryption, and secure transactions.
TCS.DCS.34	Describe the major components and functions of computer systems and networks.
TCS.DCS.37	Demonstrate legal and ethical behaviors when using information and technology and discuss the consequences of misuse.

High School: *Computer Science in the Modern World*

Computer Science in the Modern World is a course designed for all students in grades 9-12 and includes the essential skills that all high school students should have upon graduation.

Standards related to cyber security:

TCS.MW.24	Explain the principles of security by examining encryption, cryptography, and authentication techniques.
TCS.MW.35	Explain the basic components of computer networks (e.g., servers, file protection, routing, spoolers and queues, shared resources, and fault-tolerance).
TCS.MW.47	Describe security and privacy issues that relate to computer networks.

High School: *Computer Science & Mathematics*

Computer Science & Mathematics may be counted as a fourth math elective credit course and must be taught by a certified 9-12 math teacher.

Standards related to cyber security:

TCS.M.43	Describe security and privacy issues that relate to computer networks.
TCS.M.44	Explain principles of network security and techniques that protect stored and transmitted data (e.g., encryption, cryptography, authentication).

CYBERSECURITY

Standards related to cyber security:

TCS.GIS.20	Demonstrate an awareness of the ethical and social implications of the use of GIS and GPS system, including system reliability, privacy, legal issues, and the social and ethical ramifications of their use.
TCS.GIS.21	Identify the impacts GIS and GPS systems have on individuals, society, commercial markets, and innovation.

Complete standards for these courses can be found in policy at <http://wvde.state.wv.us/policies/>.

K-12 Plan – Support for Student Opportunities in Cyber Security

K-2 - Promote Cyber Security Resources for young children such as:

- the literature series from Cyber Patriots that includes pre-K books such as *Sarah the Cyber Hero*
- *Cyber Patriots interactive learning module* Security Showdown 2, geared at K-2 students and teaches students about Personal Information

L-5 - Promote Cyber Security Resources for intermediate children such as:

- *Cyber Patriots interactive learning module*, JeffOS is for grades 3-6 and teaches about phishing, malware and firewalls.
- *Cyber Patriots interactive learning module*, Packet Protector is also geared at grades 3-6 and teaches about malware, defenses and passwords.

M-8 - Promote Cyber Security Resources for secondary students such as:

Cyber Patriots middle school competition (<http://www.uscyberpatriot.org/>)
 GenCyber Camps - <https://www.gen-cyber.com/>
 The Cyber Security Lab – activity found at <http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/educator-guide/>

9-12 - Promote Cyber Security Resources and courses for secondary students such as Cyber Start -

<https://www.sans.org/CyberStartUS/>
 Girls Go Cyber Start - <https://www.sans.org/CyberStartUS/additional-resources>
 Cyber Patriots high school competition (<http://www.uscyberpatriot.org/>)
 GenCyber Camps - <https://www.gen-cyber.com/>
 The Cyber Security Lab – activity found at <http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/educator-guide/>

High School Optional Course Offerings Containing Cyber Security Components:

AC Informatics 3 – Database in the Cloud

CYBERSECURITY

Fundamentals of Computer Systems
 AP Computer Science Principles
 Cisco Networking
 Networking Essentials
 Wireless Networking Essentials
 Security +
 Server Essentials
 Digital Computer Concepts

K-12 Plan – Support for Teachers - Resources and Professional Development in Cyber Security

WVDE will disseminate resources to educators, and will provide opportunities for teachers to receive professional development in cyber security.

Current resources to be distributed include:

Free Resources for Teaching Students about Cyber Security - <http://www.oriontech.com/free-resources-teaching-students-cyber-security/>

NICCS Educational Resources:

[Cybersecurity Workforce Planning Diagnostic \(PDF\)](#) – see workforce planning section

[Students' Guide to Cybersecurity Careers \(PDF\)](#)

[Teachers' Guide to Engaging Students in Cybersecurity \(PDF\)](#)

NICE – National Institute for Cybersecurity Education -<https://www.nist.gov/itl/applied-cybersecurity/nice>

Cyber career pathway information -<https://www.cyberseek.org/pathway.html>

US-CERT - the United States Computer Emergency Readiness Team <https://www.us-cert.gov/ncas/tips>

Potential Future Plans for Developing Academic Opportunities in Cyber Security

- Develop courses for students via WV Virtual School to fill the gaps due to scheduling conflicts, non-certified teachers, etc.
- Develop training for teachers so they may develop a deeper understanding of cyber security
- Host Cyber Security Camps for students

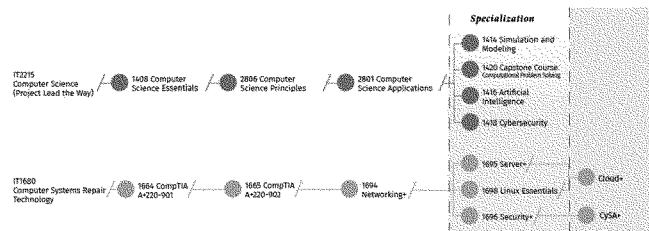
CYBERSECURITY

Career and Technical Education Component

The West Virginia Department of Education Office of Career Technical Education is implementing two programs of studies to meet the needs of the workforce Cyber Security shortage.

- The Project Lead the Way Computer Science program of study will focus on the coding / software side of Cyber Security.
- The Computer System Repair program of study will focus on the hardware / networking aspect of Cyber Security.

These programs offer a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and cybersecurity-related careers in the Information Technology career cluster.



CYBERSECURITY

National Governors Association Report on State Cyber Workforce Initiatives

State	Initiative	Reference URI	Summary
Virginia			
	Cyber Virginia	https://cyber.virginia.gov/	Initiative to help create/develop a pipeline of skilled cybersecurity workers to meet the demand of cyber jobs. Through the VA Cyber Commission, an education-centric approach was developed and included in the Governors budget to increase CAE's, SFS, and other programs to the development of cyber skills and/or capabilities.
	Cyber Initiatives included in 2017-18 Budget bill		Increase Cyber Centers of Excellence, VA scholarship for service, Veterans Pathway in Cyber Security (GWU), VA Cyber Range, etc.
	CyberCamps	http://www.doc.virginia.gov/instruction/career_technical/cybersecurity/cybercamps/index.shtml	Through the Virginia Department of Education the CyberCamps program serves as a pipeline for students K-12 to help bring awareness to cybersecurity, focusing on cyber literacy, problem driven projects related to cyber, and cyber opportunities in the workforce. This program involves 32 public schools within 8 regions.
	Adoption of the NICET Framework	https://governor.virginia.gov/newsroom/news/article/articleId/21073	The new framework will provide state agencies and educational institutions with a common, consistent lexicon that categorizes and describes cybersecurity jobs by category, specialty area, and work role. It is also a resource for firms and/or industry sectors with shared needs for a cyber workforce. Employers can use the framework to provide guidance for Virginia's workforce education and training partners to support more strategic workforce development efforts statewide.
	Virginia Cyber Security Commission	https://governor.virginia.gov/newsroom/news/article/articleId/4817 ; http://www.doc.virginia.gov/instruction/career_technical/cybersecurity/cybersecurity-whitepaper.pdf	The VA Cyber security Commission was established as part of the Executive order (EOR) and is focused on building public-private partnerships in an effort to help strengthen cybersecurity in Virginia. The responsibilities of the committee are to help identify cyber issues, bring awareness to cyber hygiene, provide recommendations to improve the workforce pipeline, and etc. The committee is comprised of academia, industry, and government.

CYBERSECURITY

State	Initiative	Reference URL	Summary
Maryland			
	Maryland Cybersecurity Council	http://www.umms.edu/visitors/president/maryland-cybersecurity-council.shtm	The Maryland Council was created help improve the cyber standards and practices in Maryland by fostering a common guidance to addressing cybersecurity issues. This council is comprised those in the public and private sector.
	Cyber Maryland		This is a yearly, two-day conference that is focused on bringing together thought leaders in academia, industry and government. There are recognized speakers and panelists, break-out sessions on various cyber-related topics, cyber job fair, industry showcase of products/services, and a networking social. The purpose is for information sharing and building of collaborations for the development of cyber assets - human and technological.
	CyberWorks	http://www.cyberworksmd.org	Organization focused on helping build the cybersecurity workforce in Maryland by using a industry-led approach. Using an model involving a two-week-sprint, candidates are vetted and screen for a perfect fit for a business. Funded by State of Maryland's EARN/Maryland Grant Program, administered by Maryland's Labor, Licensing and Regulation. http://www.cyberworksmd.org/model.html
Maryland			
	EARNMaryland	http://www.dltc.state.md/eearn/	EARN Maryland is a new state-funded, competitive workforce development grant program that is industry-led, regional in focus and a proven strategy for helping businesses cultivate the skilled workforce they need to compete. This program aims to address workforce shortages, establish career paths, and skills development.
Indiana			
	Career Makers	https://politechinc.purdue.edu/understem/careermakers	CareerMakers is an industry-led workforce education and training program that is addressing the critical workforce development needs of companies, government and agencies located in the State of Indiana and beyond.
	Cyber Academy	http://www.therepublic.com/2018/06/03/cyber-academy-partnership-provides-key-hints/	Ivy Tech Community College is working collaboratively with the Indiana National Guard to launch a cyber academy.
	Working Groups of the Indiana Executive Council on Cybersecurity	https://www.in.gov/cybersecurity/3827.htm	A focus on various Cybersecurity-related topics. One working group focuses on Workforce Development for building educational programs and pipelines.

CYBERSECURITY

State	Initiative	Reference URL	Summary
Texas	Texas Cybersecurity Council	http://dir.texas.gov/Views/About/DIR/InformationSecurity/Pages/Content.aspx?id=113	The Texas Cybersecurity Council was created by the Department of Information Resource as to establish and develop private-public partnerships. The council focuses on developing strategies and solutions for building the cyber workforce, promote innovation and collaboration to increase awareness and products to cybersecurity, evaluate program requirements, and etc.
	Cyber Texas	https://www.cybertexas.org/	The CyberTexas Foundation is focused on cyber workforce development, economic development, and preparedness. They hold a conference that help bring together experts in government and private sectors to bring attention to and help address cybersecurity issues.
	National Security Collaboration Center	https://www.monmouth.com/texas/2/18/25/08/san-antonio-university-takes-aim-at-grip-on-cybersecurity-workforce/	National Security Collaboration Center, it will be a physical space that aims to be a central gathering place for government agencies and businesses who are seeking both future cybersecurity workers, as well as contemporary research by students that might aid the organizations' existing projects.
	(San Antonio) Chamber's Cybersecurity Industry Council Task Force	https://www.sachamber.org/news/2017/08/30/chamber-cybersecurity-council-tackles-issue-around-san-antonio-searbo-workforce/	The Chamber's Cybersecurity Industry Council, the driving force behind CyberSecurity San Antonio, has launched a new task force that aims to better quantify and promote the talent transitioning out of post-secondary education providers with security skillsets.
Michigan	Michigan Cyber Initiative 2015	http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11_13_2014_web_474127_7.pdf	Michigan Cyber Initiative is focused on people, policy, and technology to address cybersecurity issues and concerns. This public-private partnership looks to develop ongoing efforts for education and cyber awareness, Cyber industry opportunities, and building a cyber ecosystem for a more holistic approach.
		http://www.michigan.gov/cybersecurity	

CYBERSECURITY

State	Initiative	Reference URI	Summary
California			
	CyberCalifornia	http://cybercalifornia.ca.gov	Initiative that supports and helps to promote the California Cybersecurity Task Force by helping to foster connections between public and private institutions with the goal of encouraging innovation, education, and workforce development. In connection with this is iHubs with is a innovative platform administered by Governor's Office of Business and Economic Development.
	Cybersecurity Task Force	http://www.caloes.ca.gov/for-individuals-families/cybersecurity-task-force	Directed by Gov. Jerry Brown, the California Cybersecurity Task Force was created to help foster and promote a culture of cybersecurity through education, information sharing, workforce development and economic growth. The task force has 8 goals that support the building of California's cybersecurity position and resiliency. To achieve these goals, the Task Force is made up of 7 committees that are comprised of volunteers from industry, academia, and government.
	Hi Tech Initiative - TechEd	http://www.biredexchange.com/tech-ed-partnerships	Bired Exchange in partnership with LA Hi-Tech, helps to bridge the skills gap by connecting industry and academia. Through mentorships, fairs, hackathons, internships, and classroom visits students are provided with formal and informal educational opportunities. Currently, there are 8 community colleges, 30 high schools, and 4,000+ students. This sponsored by the LA Chamber of Commerce.
	LA Chamber of Commerce Recruitment and Training Strategy by Bired Exchange		Bired Exchange won a contract with LA to provide Recruiting and Training strategies with a focus on number of jobs, best practices, awareness, case management, and building connections. Th areas of interest are IT, Logistics, Manufacturing, and Biotech. This is still being developed
Florida			
	Supervisors of Elections Training and Key Personnel	https://news.uwf.edu/university-of-west-florida-partners-with-state-and-local-election-officials-to-enhance-cybersecurity-preparations/	The University of West Florida Center for Cybersecurity recently partnered with the Florida Department of State and election officials across Florida to provide training for supervisors of elections and key personnel to enhance cybersecurity resiliency ahead of the 2018 elections.
	Florida Center for Cybersecurity (FC2)	http://florci2.org	The Florida Center for Cybersecurity is a shared resource for academia, government, and industry to help expand educational offerings, increase research capabilities, and and foster partnerships to address cybersecurity. This state initiative is focused on creating more jobs, enhancing the cybersecurity workforce, bringing more innovation, and being a hub for the community.

CYBERSECURITY

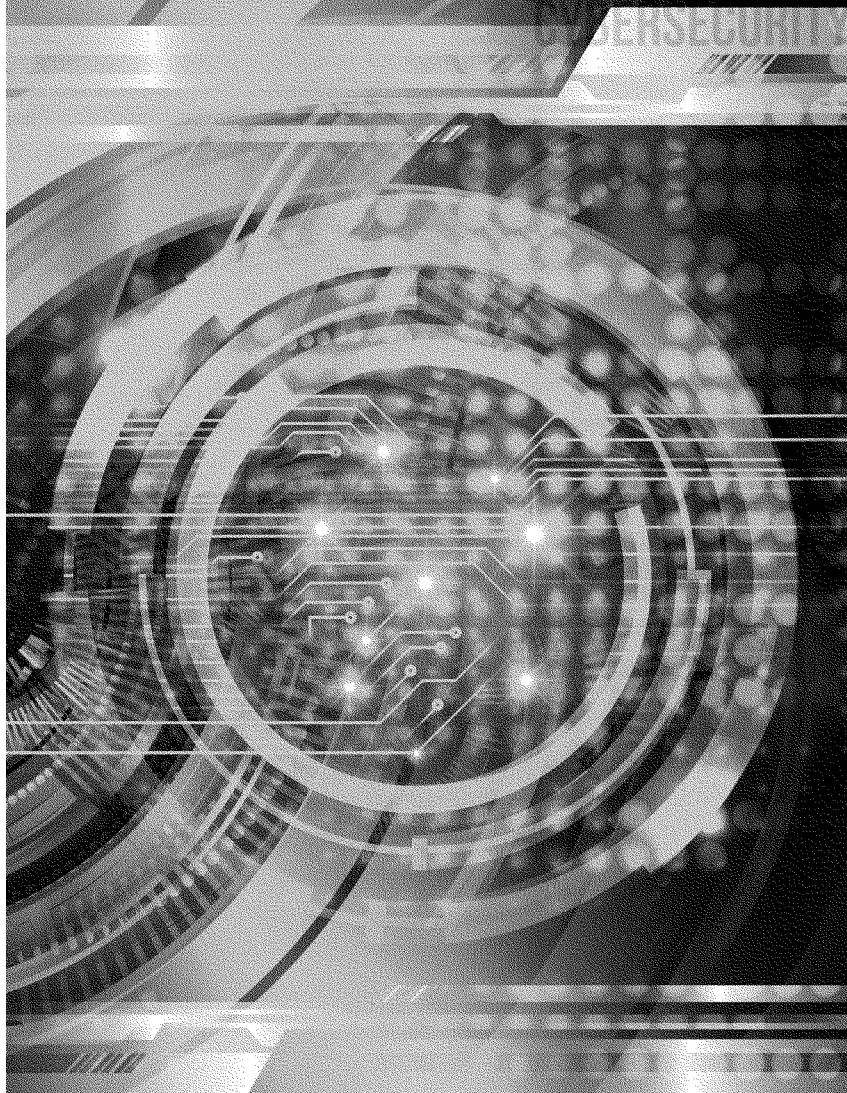
State	Initiative	Reference URL	Summary
Maine			
	Maine Cybersecurity Cluster (MCSC)	http://mainescybersecurity.github.io/	The Maine Cyber Security Cluster (MCSC) is an academic and research center bringing together government, industry, and academia dedicated to workforce and economic development in the field of cyber security. Its focus is project oriented that involves students experimenting and being innovative with cyber related activities, helping them gain practical experience. They have simulations, various tools for project development, and resources - IT professionals.
	Student projects	http://mainescybersecurity.github.io/what-we-do-student-projects	
North Carolina			
	iCenter	https://icenter.nc.gov/	iCenter is a innovative center created by the NC Department of Information Technology to promote strong collaborations and connect academia, government, and industry, for developing technologies, provide training capabilities for state employees, information sharing, and etc. The vision of iCenter is to provide a simple way to interact with government and develop technology solutions in a creative way.
North Dakota			
	Cybersecurity and Computer Networks Program	https://www.nd.govisd/news/5834/north-dakota-and-palo-alto-networks-collaborate-cybersecurity-education	North Dakota Gov. Doug Burgum, Chief Information Officer Shawn Riley and Bismarck State College (BSC) President Dr. Larry Skogen announce an educational collaboration with Palo Alto Networks that will grow the college's Cybersecurity and Computer Networks Program.
Arizona			
	Workforce pipeline for Cybersecurity at EMCC - DoL Grant	https://www.esandlmesonito.edu/prog/ame/cybersecurity	To help reduce this critical workforce shortage, the Arizona San Corridor-Get Into Energy Consortium (ASC-GIEC), which received a \$13.5 million Department of Labor (DOL) grant to advance the training and development of a workforce pipeline for the energy industry, is creating an energy-related cybersecurity program through Estrella Mountain Community College (EMCC), the consortium's lead institution.
Oklahoma and surrounding states			
	Cyber security Education Consortium (CSEC). Formally known as Oklahoma Center for Information Assurance and Forensics Education.	https://cseccenters.org/about-us/	CSEC is a cohesive partnership of community colleges and career and technology centers in Oklahoma, Arkansas, Colorado, Kansas, Louisiana, Missouri, Tennessee and Texas and the University of Tulsa, which serves as the principal training entity and mentor to the two-year institutions. Funded by a NSF grant

CYBERSECURITY

State	Initiative	Reference URL	Summary
Colorado	House Bill 16-1453 signed by Gov. John Hickenlooper	http://pressreleases.aces.edu/?p=2851	Identifies Colorado Springs as the location for the National Cyber Intelligence Center to respond to cyber-attacks, to train government and private sector leaders to respond to them, and to do workforce development and research. The bill supports a partnership of academics at UCCS and other higher educational institutions to leverage military, state, federal, local government as well as private sector resources.
Delaware	Delaware Cyber Aces (SANS)	http://aces.delaware.gov/2013/09/10/governor-launches-delaware-cyber-aces-program/	Delaware Cyber Aces targets high schoolers, college students, veterans, and jobseekers in an effort to identify and develop top talent.
	UD Cybersecurity Initiative	https://sa.udel.edu/missem/statement/	The Cybersecurity Initiative (CSI) was established in 2014 as a partnership among the state, University of Delaware, federal agencies, and the private sector to address a problem that costs billions of dollars a year through education, training, and research.
Missouri	Missouri Governor's Cybersecurity Summit Initiative	http://www.gov.missouri.gov/missouri-governors-cybersecurity-summit.html https://www.missouri.gov/missouri-announces-statewide-cybersecurity-preparedness-initiative/	Currently a yearly summit that focuses on engaging public, private, and academia for Information Sharing, Training Exercises, Workforce Development, Hardening Critical Infrastructure, and Incident Response. Two topics that are very relevant to NICE is "solving the personnel gap" and "the role of education in cybersecurity."
New Mexico	Center for Cyber Defenders	http://www.sandia.gov/careers_students_posdocs_internships_institutes/cyber_defenders.html	Program to train cyber defenders who can move into computer security jobs at Sandia. Learn to combat cyberattacks, while gaining practical experience in understanding computer systems, network operations, and information protection. CCD interns are part of a Sandia program, Technical Internships to Advance National Security (TITANS).
	Western Cyber Exchange (Colorado, New Mexico, and Wyoming)	http://www.wcyb.org/About.aspx	Public-Private partnership (including DHS, MITRE, and Advanced Cyber Security Center - ACSC) that focuses on security of the cyber domain for communities and industry within the critical infrastructure through the sharing of threat intelligence and data, education and training for workforce development, and supporting the advancement of cyber related technology through research and development activity.
New York	New York State Cyber Security Conference and Symposium on Information Assurance	https://www.nys.gov/news/13thannual-cyber-security-conference	Northeast conference for cyber security education, the event is co-hosted by the New York State Office of Information Technology Services, the NYS Forum, Inc., and the University at Albany's School of Business.

CYBERSECURITY

State	Initiative	Reference URL	Summary
Massachusetts			
	Masse Skills Capital Grant Program	http://www.mass.gov/eolc/government/executive-office-of-education/grants-information/massachusetts-skills-capital-grant-program.html	The Skills Capital Grant Program awards grants to support vocational technical training, upgrades and expansion of career technical education, and training of high-quality career pathway programs that are aligned with regional economic and workforce development priorities for in-demand industries, such as information technology.
Connecticut			
	Cyber Security Strategy	http://portal.ct.gov/media/Office-of-the-Governor/Connecticut-Cybersecurity-Resource-Pages/Connecticut-Cyber-Security-Strategy.pdf	High level main points, more collaboration with businesses and higher education institutions, more communication with executive leadership, HR change for better recruitment, and more matching of cybersecurity demands with training and personnel resources.
Georgia			
	Hull McKnight Georgia Cyber Center for Innovation and Training	https://go.georgia.gov/hull-mcknight-georgia-cyber-center-innovation-and-training	A state-owned facility designed to promote modernization in cybersecurity technology for both the private and public sectors through unique education, training, research, and practical applications.
	Cybersecurity Workforce Academy	https://go.georgia.gov/georgia-cybersecurity-workforce-academy	Provide cybersecurity awareness, training, and education. Will take place in the Hull McKnight Georgia Cyber Center for Innovation and Training.
Vermont			
	Workforce Growth Initiatives	http://go.vermont.gov/press-release/governor-phill-scott-appoints-degass-and-huxton-lead-workforce-growth-initiatives	Focused on increasing the WF. There is a Workforce Development Board, a 58-member panel charged with coordinating workforce training and education programs and engaging the state's employers, workers and other partners.



FOR MORE INFORMATION CONTACT:



U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Questions for the Record Submitted to Mr. James B. Robb

Questions from Chairman Lisa Murkowski

Question 1: NERC appears to be addressing the risk of supply chain attacks, where foreign adversaries target utilities via vendors and other third parties that have an established business relationship with the utility. How will NERC's mandatory standard on supply chain management address this threat?

In August 2017, NERC's Board adopted CIP-013, Cyber Security - Supply Chain Risk Management, in response to FERC Order No. 829. FERC approved the standard in October 2018. The supply chain standards will require entities to implement security controls addressing supply chain risks during the planning and procurement of industrial control system hardware, software, and computing and networking services. Entities are required to develop and implement supply chain risk management plans to (1) identify and assess the security risks associated with any particular vendor, product, or service, and (2) address specific security issues in their procurement processes for products and services. The supply chain risk management Reliability Standards focus on the following security objectives: (1) software integrity and authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls. Collectively, the requirements in the supply chain risk management Reliability Standards are designed to:

- Address the risk that entities could enter into contracts with vendors who pose significant risks to their information systems, as well as the risk that products procured by an entity fail to meet minimum security criteria.
- Address the risk that entities could unintentionally plan to procure and install unsecure equipment or software within their information systems, or could unintentionally fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions.
- Address the risk that a compromised vendor would not provide adequate notice of security events and vulnerabilities, and related incident response to entities with whom that vendor is connected.
- Reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches.
- Address vendor remote access-related threats, including the threat that vendor credentials could be stolen and used to access a cyber system without the entity's knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into an entity's operational environment.

Question 2: Under the FAST Act, DOE has authority to issue emergency orders to industry for grid security emergencies. The effectiveness of this authority will require close coordination with

U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Questions for the Record Submitted to Mr. James B. Robb

industry and NERC. What is the status of DOE's work with industry and NERC to ensure this coordination?

NERC is a member of the Electricity Subsector Coordinating Council (ESCC), which is working with the North American Transmission Forum on a range of "templated orders" that will be shared with DOE for their consideration. Templated orders will provide information and context to help inform the basis for orders following a presidential declaration of a Grid Security Emergency. NERC is contributing technical subject matter expertise of the bulk electric system and its operation to the drafting team, and participating in regular discussions on this effort. This effort will be finalized as a report to DOE, expected by the end of summer 2019. NERC intends to exercise the findings with DOE during GridEx V in November 2019.

Question 3: As you know, one of the best ways to be prepared for an attack is training.

- **What type of cyber training are the operators in our control rooms receiving? Is it sufficient?**

CIP-004 is the NERC standard focused on the human element of cyber security. CIP-004 requires operators to implement a cyber security training program; implement a cyber security awareness program; conduct background checks for any individual (employee, vendor, contractor, etc.) seeking electronic or unescorted physical access to BES Cyber Systems; implement an access management program for authorizing electronic and unescorted physical access; and implement an access revocation program to ensure individuals that should no longer have access to BES Cyber Systems do not continue to have access.

- **Is this training reaching down to all grid operators? Or is it only reaching the biggest companies with the greatest resources?**

Reliability standards apply to all users, owners, and operators of the bulk power system. Accordingly, NERC's training requirements under CIP-004 apply to all entities covered by the standard regardless of size. From the specific perspective of a system operator, practical cybersecurity has become an increasingly common topic at system operator training events across North America. In June 2018, NERC's Operating Committee published a Reliability Guideline¹ on Cyber Intrusion for System Operators to enhance the preparedness of operating personnel.

- **Since the Ukraine attacks are real-world events where control room operators were forced to handle the incursion, are the lessons learned about Ukraine being taught in training classes here in America?**

¹ https://www.nerc.com/comm/OC_Reliability_Guidelines_DL/Cyber_Intrusion_Guide_for_System_Operators_approved.pdf

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. James B. Robb

NERC has worked extensively to communicate lessons learned from the Ukraine attacks. NERC's Electricity ISAC collaborated with DOE's Office of Electricity in the months following the December 2015 Ukraine attacks to compile tailored lessons learned and knowledge transfer materials. In March and April following the attacks, NERC participated with government partners in conducting a series of unclassified in-person briefings for asset owners and operators. These briefings included details about the events surrounding the attack, techniques used by the threat actors, and strategies for mitigating risks and improving the cyber defensive posture of an organization.² In addition, this information is incorporated into the Cyber Strike Workshop³ training provided by Idaho National Laboratory. In 2016, NERC issued a Level 2 alert related to the cyber security event in Ukraine. NERC also issued a Level 1 alert on June 13, 2017, "Modular Malware Targeting Electricity Industry Assets in Ukraine." The alert details the capabilities of the malware involved with the December 2016 attack on Ukraine's electricity assets. In July 2017, the E-ISAC and SANS Industrial Control System (ICS) Team released a joint product summarizing analysis of the modular malware framework associated with the 2016 attack. The report consolidated open source information, clarified important details surrounding the attack, offered lessons learned, and recommended approaches to help the ICS community search for and repel similar attacks. The report is available on the E-ISAC website. The E-ISAC continues to be a resource for information sharing and analysis to combat emerging threats to cyber security and help ensure the reliability of the BPS.

Question 4: According to NERC's antitrust compliance guidelines located on its website, "the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition."

- **How are the antitrust laws impacting the ability of the energy industry to properly defend its assets against cyberattack?**

NERC routinely reminds stakeholders participating in NERC activities of the need to adhere to all antitrust laws. NERC is not aware of any specific instances in which antitrust law has been an impediment to industry efforts to enhance the security of their systems and prepare for a cyber attack. Because of the interconnected nature of the grid, it is important to note that the electricity industry has a long tradition of working together to support operational needs. As cyber threats became more complex and pervasive, industry has carried this tradition into the security arena. NERC plays a critical role in convening industry stakeholders to address security issues, including supply chain risk management, partnerships with government agencies, and information sharing through the E-ISAC. NERC's GridEx exercise identified a need for companies to work together to respond to and recover from cyber events.

² See https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf.

³ See https://inl.gov/wp-content/uploads/2018/02/18-50019_Cyber_Strike_Workshop_R0-2.pdf.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. James B. Robb

This led to industry's cyber mutual assistance program which is modeled after the highly effective mutual assistance program for natural disaster recovery. NERC is also a member of the Electricity Subsector Coordinating Council (ESCC) which has proven to be an effective collaboration between industry and government. In 2015, a collaboration among executives of the ESCC directed a strategic review of the E-ISAC. This initiative led to creation of the Member Executive Committee (MEC), an advisory body comprised of industry executives to provide direct strategic input to enhance the value of the E-ISAC to industry. With input from the MEC, the E-ISAC is implementing a five-year strategic plan to further expand capabilities. As these collective efforts continue to evolve, all stakeholders must remain mindful of anti-trust laws while working to address security risks.

- **Should Congress consider holding a hearing or taking other action?**

NERC respectfully defers to the committee's judgment concerning additional congressional attention to this subject.

Questions from Ranking Member Joe Manchin III

Question 1: We discussed concerns about the information sharing process not working quickly enough, especially for component manufacturers. What do you think the solution is?

Addressing this challenge will require a concerted effort and must be done in a public-private partnership between the government, owners and operators, and the vendor community.

The E-ISAC is working on a number of fronts to develop and deploy rapid, actionable information sharing processes to address potential vulnerabilities from component manufacturers and other elements of the supply chain. To share threat detection and intelligence for operational technology (OT) used in the electric grid, the E-ISAC is partnering with the government (DOE, Idaho National Lab) and private sector partners on the Neighborhood Keeper⁴ project. The project team will develop and demonstrate a low-cost cloud-enabled sensor network within the OT domain to enable integration of available technologies that will facilitate real time and actionable information to reduce cyber risk. The E-ISAC will work with Neighborhood Keeper partners to then disseminate this information via the E-ISAC Portal to enhance OT risk mitigation, to include potential component vulnerabilities.

The E-ISAC is also addressing supply chain and component vulnerabilities information sharing through cross-sector partnerships. The E-ISAC is looking at common equipment and adversary tactics, techniques, and procedures across the sectors. The information is shared with industry with added electricity-specific context from our analysts through the E-ISAC Portal and through Critical Broadcast Program calls to

⁴ For more information please visit:
<https://www.energy.gov/sites/prod/files/2018/09/f56/FINAL%20CEDs%20Awards%20fact%20sheet%20October%202018.pdf>
 and <https://dragos.com/neighborhood-keeper/>. Accessed February 27, 2019.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. James B. Robb

inform asset owners on risk and mitigation strategies. Our partners in this important activity include the National Council ISACs (NCI), as well as specific critical interdependent ISACs, such as the Downstream Natural Gas, Multi-State, and Water ISACs, as well as the U.S. and Canadian governments.

Finally, the E-ISAC is cultivating partnerships with major electricity sector component vendors to develop trusted methods to share critical security-related information. The goal is to keep equipment secure and resilient in the face of determined adversaries by providing additional electricity industry context to the vendors, and timely and credible updates to asset owners and operators. This type of sharing is the next evolution in the grid resilience partnership as it relates to cyber threats against critical infrastructure. We all need to work together, and get to a point where known vulnerabilities are disclosed and mitigations are quickly shared by vendors.

Question 2: The interactions between information technology and operational technology systems present significant vulnerabilities for our grid infrastructure.

- **What defenses, security measures, or detection measures are best to employ between informational technology networks and operation technology networks in order to defend the electric grid's physical infrastructure from attacks by hackers, insider attacks, negligence, or mistakes?**

As discussed in my testimony, CRISP provides timely bi-directional sharing of unclassified and classified threat information and develops situational awareness tools to enhance the electricity sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure. Building off the success of CRISP, the E-ISAC is working with DOE on a more OT-focused pilot project called Cybersecurity for the Operational Technology Environment (CYOTE).⁵ The pilot looks at the specifics of OT networks, and evaluating the types of data, collection processes, and the procedures to share the information. The E-ISAC appreciates DOE's leadership on the project and looks forward to continuing its partnership with the government on this and other initiatives.

Technology alone is inadequate to defend the electric grid's infrastructure. All the recommendations below must be supported by effective governance that factors in security considerations into the overall risk management policy and practice of asset owners and operators.

A well-designed network architecture with security and defensibility as explicit design criteria provides an important foundation. Noting that NERC is technology agnostic, there are a variety of commercial devices and capabilities, both for general IT and increasingly for OT environments, from which the system can be built. Detailed asset inventory and management, and configuration change control provide visibility of the defended assets. Monitoring system performance by system operators for unexplained abnormalities and indications of malicious activity is a detective control to identify external or internal attacks, technical errors, or mistakes. Each of these can then be appropriately remediated to incrementally improve the security and reliability of the systems.

⁵ <https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity>

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. James B. Robb

An effective and appropriately resourced security awareness program will strengthen the capabilities of human users, who can be the first opportunity for detection and who are also often the last line of defense against advanced adversaries. As mentioned in response to the Ranking Member's first question, the E-ISAC's participation in the Neighborhood Keeper project will help share threat detection and intelligence for operations technology (OT) used in the electric grid. Research by the partnership is already underway to develop new methods to make industrial control system (ICS) threat analytics and information available to the electricity and other industries. Key to this project is the focus on smaller critical infrastructure owners and operators who may not have the financial resources to procure this type of technology and service. Neighborhood Keeper is designed to make these insights available to those operators, and provide information through the E-ISAC Portal, thereby extending the project's benefit widely.

In addition, operations technologies in critical control centers are protected at the highest level in the CIP standards, requiring not only physical and electronic access controls, monitoring, and logging, but also background checks, cyber security awareness training programs, vulnerability assessments, and drills of restoration procedures.

- **How should utilities mitigate the risks of connecting information technology systems to operational technology systems?**

NERC's critical infrastructure protection standards provide essential cybersecurity protections for BES cyber systems. CIP-005-5 addresses the electronic security perimeter (ESP) of BES cyber systems. The standard requires all applicable BES cyber systems that are connected to a network via a routable protocol to have a defined ESP. CIP-005-5 requires segmenting of BES cyber systems from other systems by requiring controlled electronic access points between the different trust zones. Electronic security perimeters are also used as a primary defense layer for some BES cyber systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability. Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System. If there is routable connectivity across the ESP into any cyber asset, then an electronic access point (EAP) must control traffic into and out of the ESP. Utilities must know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. David Edward Whitehead

Questions from Chairman Lisa Murkowski

Question 1: SEL appears to be addressing the risk of supply chain attacks, where foreign adversaries target utilities via vendors and other third parties that have an established business relationship with the utility.

As a vendor selling critical equipment to the utility industry, how is SEL addressing this threat?

A secure supply chain is critical not only to a company's success but also to national security. At SEL, we select only the highest quality components and follow the best-known security practices, many of which have been created by us and have been endorsed and publicized by the National Institute of Standards and Technology (NIST).

SEL would like to submit for the record a link (and PDF attachment) to our 2016 supply chain document which outlines the processes SEL follows to ensure a safe and dependable supply chain for the products we deliver to customers around the world.

https://cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/SecureSupplyChain_PF00551.pdf?v=20161219-191622

We take a comprehensive approach to evaluating the risks to our supply chain. Our R&D division uses a rigorous design and component qualification process. Our approach consists of eight basic steps. We've highlighted certain aspects in each step and we hope Congress will consider our model as they continue to drive the discussion on how to improve supply chain risk management.

- *Step 1: Build Trusted Supply Networks* – This includes annual supplier conferences, onsite audits, and cross-functional collaboration.
- *Step 2: Rate Suppliers' Risks* – This includes a supplier rating system based on PQFIDS (price, quality, features, innovation, delivery and services), tracking our suppliers' suppliers, preferences for domestic suppliers and shipping supplier qualifications.
- *Step 3: Ensure Component Integrity*: This includes a component qualification process, direct procurement through a prescribed process, and continuous testing of materials.
- *Step 4: Keep Track of Components and Products* – This includes keeping detailed records of every product and creating an outstanding warranty.
- *Step 5: Ensure Component Availability* – This includes tracking at risk parts and keeping sufficient inventory of specialty parts.
- *Step 6: Collaborate with Customers and Industry* – This includes customer visits to SEL facilities to test products and participation in government-led initiatives including standards development.
- *Step 7: Build Security into Company Practices* – This includes developing our own source code, testing the performance of equipment, practicing need to know policies, never releasing a product's bill of materials or design schematics, creating robust designs, and embracing cybersecurity at every step of product development.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. David Edward Whitehead

- *Step 8: Ongoing Risk Management* – This includes tracking emerging threats, and vertically integrating our manufacturing capabilities as necessary.

SEL looks forward to continued work with government agencies, NERC, and industry partners to continuously implement and improve supply chain risk management practices. We hope that our processes are used to inform how industry manages its vast supply chain. They have been used and refined by SEL over decades and helped us maintain layered security throughout our organization and within the products we manufacture.

Should Congress be taking action on supply chain threats?

The U.S. Government should *teach the threat* related to supply chain challenges to technology developers, manufacturers, logistics companies, and service providers. The U.S. Government has the resources to understand what threats may exist. Asset owners and manufacturers have the specific expertise to know how those threats may impact their products or supply chain.

SEL offers to serve as a resource on supply chain threats, should Congress need information or a private sector perspective on how a regulation or standard affects the innovation, manufacturing, or distributing of our products.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. David Edward Whitehead

Question 2: You state that information sharing among the government and electric grid asset owners and equipment manufacturers is critical to protecting the grid from cyber-attacks. To that end, you recommend building out a more robust system of communication for government agencies to quickly share information with industry.

What are your thoughts on existing government-industry information sharing programs, such as DOE's Cybersecurity Risk Information Sharing Program, NERC's Electricity Information Sharing and Analysis Center, and the Department of Homeland Security's National Cybersecurity & Communications Integration Center? How can these programs be improved?

SEL does not participate in the Cybersecurity Risk Sharing Program or Electricity Information Sharing and Analysis Center. Technology developers and manufacturers, like SEL, would benefit from participation in such public-private information sharing frameworks using the information gained to improve the security of our products. We believe SEL, and likeminded companies, could help mitigate vulnerabilities and implement security solutions faster if brought into the conversation in real time.

SEL coordinates with DHS' National Cybersecurity & Communications Integration Center (NCCIC) and when appropriate, postindustrial control system vulnerability advisories. We also monitor NCCIC advisories to track vulnerabilities affecting the electric sector.

U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Questions for the Record Submitted to Mr. David Edward Whitehead

Question 3: I understand that SEL manufactures most of its products within the United States, but many other suppliers to the energy sector are either foreign companies or have manufacturing or research facilities abroad.

Does foreign manufacturing present any cybersecurity risks? If so, how big is this problem? And what should be done about it?

SEL designs and manufactures our electronic devices in the U.S. SEL sources domestically to the greatest extent possible. For both domestically and internationally sourced parts we use only trusted, reputable suppliers, while delivering on our commitment to offer the lowest price anywhere in the world. We are able to deliver on this promise because SEL risk managers possess tremendous detail about the path of every component – through fabrication, packaging, testing, warehousing, shipping, and distribution. When we do source foreign components, we test and verify that they are of the highest standard and put in place stringent requirements to ensure our risk management strategy is effectively implemented. We track and test every component and sub-component. We control the source code in our products. We never release a product's bill of material. Rather, we buy individual components and then using those components, assemble products in the U.S. – suppliers have zero knowledge of where and which components are installed in a particular product. And, as you point out, we develop most of our materials in-house or in the U.S. to avoid foreign manufacturing issues.

At SEL, we believe that the cybersecurity threat is ever present, whether it is from a foreign or domestic vendor. That is why we take a holistic approach to integrity and have established tight requirements for all vendors to prevent cybersecurity incidents – from embedding cybersecurity at the earliest stages of product development, to strict physical security requirements for employees and visitors alike, and stringent rules on maintenance and upgrade services by their vendors. Anyone, employees included, coming on-site with USB keys are required to run them through a company-designed scanning system prior to use on SEL systems. Additionally, personal devices are prohibited from connecting to SEL's network. This is a manageable issue if companies will commit to continual audits and inspections of their suppliers, exchange industry best practices and innovative ideas and provide mutual guidance. Collaborating with our suppliers on manufacturing process improvements helps SEL improve quality, efficiency, cost, and security. These are practices that we believe the entire industry could benefit from.

Even with companies entirely located within the United States, there is no guarantee that every employee will protect American interests—how do you protect against insider threats?

An essential element of the SEL insider threat mitigation program is rigorous employee vetting, which begins on day one of the hiring process. All candidates undergo extensive pre-hire background checks, which includes a full examination of any criminal history. All employees are required to report negative interactions with the criminal justice system. Periodic background checks are required for certain categories of employees throughout their careers.

At time of hire, employees undergo an intensive training program that reinforces the need for security at every level of the enterprise, the concept of least privilege, and the critical role of each employee as the last and first line of defense in SEL's security infrastructure. SEL's security program includes frequent

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. David Edward Whitehead

training through a variety of mediums, including segments at a weekly, company-wide business meeting called Friday Lunch.

Finally, the SEL Human Resources, Security, and Legal teams operate collaboratively, to detect and quickly provide support to employees in difficulty, which may present an incipient insider threat from developing. This collaboration also serves as a deterrent to malicious behavior and increases the probability that insiders who pose a risk SEL will be quickly detected. At all times, SEL's insider threat detection program safeguards employee privacy and the dignity of work in keeping with our long-standing Principles of Operation which set forth the philosophies and values that guide all SEL operations.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. David Edward Whitehead

Questions from Ranking Member Joe Manchin III

Question 1: We discussed concerns about the information sharing process not working quickly enough, especially for component manufacturers. What do you think the solution is?

Bringing together relevant government agencies, asset owners and operators, and component manufacturers in real time would be of tremendous value for public and private entities to quickly assess and mitigate cyber threats. To date, the majority of critical infrastructure protection work is segmented by industry or sector. For example, SEL is not a member of the Electricity Sector Coordinating Council or the Electricity Information Sharing and Analysis Center and therefore is not part of the collective discussion regarding cybersecurity preparedness, information sharing, and incident response activities with our customers. Bringing these entities together in a public-private partnership is important so we are all working together to share information. If asked, SEL would gladly participate as a member of the ESCC and E-ISAC.

I proposed the idea of an '8:00 AM call' where security vulnerabilities are reported on and coordinated between government and industry. This is the kind of coordination that FEMA conducts daily in preparation for and in response to Hurricanes. I believe that government and industry could work together on something similar. We understand that there are challenges to conduct a call like this, including multinational corporations listening to potentially sensitive information, liability protections, and sharing of business sensitive information. However, there are ways to address all of these issues if we come together and develop a more coordinated process with rules of engagement.

SEL possesses the appropriate security clearances to hear real-time, sensitive information. We commit to act on intelligence and provide solutions to the government and our customers when needed. All we ask is that we are informed in a timely matter when serious threats are posed to our customers and our products.

U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Questions for the Record Submitted to Mr. David Edward Whitehead

Question 2: The interactions between information technology and operational technology systems present significant vulnerabilities for our grid infrastructure.

What defenses, security measures, or detection measures are best to employ between informational technology networks and operation technology networks in order to defend the electric grid's physical infrastructure from attacks by hackers, insider attacks, negligence, or mistakes?

The major difference between an informational technology (IT) network and an operational technology (OT) network is that an IT network is dynamic, e.g. user, devices, and network flows are continually changing, while an OT network, for the most part, is static—designed, put into service, and expected to run in that configuration for a long time. The static nature of the OT network provides a significant advantage over IT networks for the following reasons:

- White-listing is possible on OT networks. Because OT networks run a fixed function, only explicitly defined networks should be permitted to transit the network, i.e. white-listed, and all unauthorized traffic is disallowed.
- OT networks lend themselves to a layered approach to network security. For example, most OT network devices are machine-to-machine communications. Because of this firewall and other security gateways can be implemented to segregate the machine-to-machine communication from the human-to-machine communication and IT networks.

At the end of 2018, SEL published a book on power system cybersecurity. *Sensible Cybersecurity for Power Systems* which is a collection of 28 technical papers by industry experts offering an overview of challenges, opportunities, and solutions for modern power system cybersecurity.

Electric power systems rely on secure communications. Dependability, determinism, network recovery, and cybersecurity are fundamental concerns. Recent events, such as the Ukraine cyberattacks show that electric utility protection and control systems are vulnerable to electronic intrusion when proper cybersecurity controls, processes, and procedures are not used. This book, written by research and development engineers; field application engineers; and protection, control, and communications practitioners from the power industry, provides modern solutions to address these challenges.

The book goes into many of the technologies and approaches SEL and others employ to ensure risk management and security solutions are implemented from designing layered defenses with appropriate security controls to securing networks and communications through applications like software-defined networking.

There are too many technologies and approaches to pinpoint a silver bullet. In addition, it also depends how technologies are configured, which features are turned off or on, and how they are tied to other technologies in the system, to understand the full network security. Lastly, we have hundreds of engineers at SEL already creating next generation security solutions that will replace any list provided.

How should utilities mitigate the risks of connecting information technology systems to operational technology systems?

U.S. Senate Committee on Energy and Natural Resources
 February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
 Questions for the Record Submitted to Mr. David Edward Whitehead

There are many mitigations SEL and our customers continue to use to address IT-OT connection vulnerabilities. SEL's Cybersecurity Solutions document provides some insights, in brief.
https://cdn.selinc.com/assets/Literature/Product%20Literature/Flyers/PF00250_CybersecuritySolutions_20151013_Pubs.pdf?v=20170307-194819

Overarching is implementing defense-in-depth cybersecurity solutions that mitigate threats with sustainable, proactive solutions, including:

- Network segregation between IT and OT systems. Network segregation within OT systems between human-to-machine networks and machine-to-machine networks.
- Security controls and encryption to maximize confidentiality and integrity of communications.
- Integrated user access controls to support centralized single or multifactor authentication to intelligent electronic devices (IEDs).
- Logs and alerts to provide detailed audit trails that identify all activity on electrical systems.
- Cybersecurity experts to help design, engineer, and maintain effective cybersecurity systems.

SEL welcomes the opportunity to discuss this Congress and Federal employees about our technology toolkit and maintain and open and active dialogue on the issues.

Question from Senator Debbie Stabenow

Question: It is deeply troubling that key parts of our energy system are made in other countries – like China – raising the potential for tampering, theft, or the insertion of malware in our energy supply chain.

Would you please speak to the vulnerabilities within our energy supply chain, and to whether our growing dependence on foreign-made energy components presents a potential national security threat?

Any long supply chain represents risk. The U.S. would certainly be in a more secure position if we were able to source critical energy sector components within our country.

Presently it is not feasible to source energy sector equipment entirely from U.S. manufactures. Given this reality, we should focus on supply chain risk management practices outlined above that help us monitor and verify our security posture and enable industry to deploy technologies and experts to isolate, fix, and further protect our systems in real time.

SEL goes to extreme lengths to ensure our suppliers and their technologies and parts are vetted, especially foreign-owned entities. We also vet the suppliers' suppliers and test and track all our technologies and business arrangements. We then repeat these processes regularly to maintain a constant understanding of the evolving supply chain.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. David Edward Whitehead

Questions from Senator Mazie Hirono

Question 1: As industrial control systems in the power grid, pipelines, and other infrastructure become more complex, more connected and potentially more vulnerable. On the other hand, however, technical advances could potentially make these systems easier to protect because they can incorporate the latest state of the art security technology such as advanced encryption algorithms and other measures. In your opinion, are industrial control systems in the energy industry more secure as the technology becomes better, or are we losing ground because these systems are becoming more complex and inherently more vulnerable to advanced persistent cyber threats?

While SEL has always taken cybersecurity as key component of the products we build, I have seen a significant increase in the electric sector to deploy new technologies that incorporate cybersecurity. Offensive and defensive technologies and approaches are constantly evolving and so must our solutions. The operational tempo for cyber defense needs to be in near real time. We at SEL want to stress the importance of a nimble, innovative and collaborative public-private workforce that can handle real and evolving cyber threats and does not focus on compliance which will certainly slow us down, and potentially focus us on fixing yesterday's problems.

U.S. Senate Committee on Energy and Natural Resources
February 14, 2019 Hearing: *The Status and Outlook of Cybersecurity Efforts in the Energy Industry*
Questions for the Record Submitted to Mr. David Edward Whitehead

Question 2: In your view, are the Administration and Congress investing enough resources to counter and respond to cyber threats, and are the resources sufficiently well-targeted? Also, in your view, are electric utilities and other owners of energy-sector critical infrastructure investing enough resources and correctly targeting them to adequately address cyber threats?

I don't have an intimate knowledge of how much investment the U.S. is spending on cyber threats. I do believe that the role of the U.S. government is to teach the threat. If asset owners and equipment suppliers understand the threat, they will address it because it is in their best interest to do so.

We can tell you that our customers, including utilities, take cybersecurity very seriously. It's at the top of every executive's mind in the electricity industry. More resources are being applied to cybersecurity measures in industry. My recommendation is for the U.S. government to be resource for the electric sector, but not select any one particular technology and mandate it across the sector. Allow each asset owner to develop cyber security systems that meet their needs based on good cyber intelligence from the U.S. government.



Securing Your Supply Chain

Best Practices From SEL



Society depends on critical infrastructure.

Critical infrastructure depends on supply chain security.

SEL's culture of quality, continuous improvement, and innovation drives us to create the safest, most reliable, and most economical products for critical infrastructure. To do this, we select only the highest quality components and follow the best known security practices, many of which have been created by us and have been endorsed and publicized by the National Institute of Standards and Technology (NIST) and the U.S. Resilience Project.

SEL understands that secure supply chains are critical not only to a company's success but also to national security. Supply chains feed our critical infrastructure operations, which in turn power our society. As the focus on supply chain security continues to intensify, infrastructure operators are asking their suppliers for details about what they are doing to address this issue. This document outlines the processes SEL follows to ensure a safe and dependable supply chain for the products we deliver to customers around the world.



How SEL Ensures a Dependable Supply Chain

SEL's supply chain is global and complex. We take a comprehensive approach in evaluating the risks to our supply chain. Our R&D division uses a rigorous design and part qualification process to evaluate potential variables. This approach consists of eight basic steps.

Step 1: Build Trusted Supply Networks

ANNUAL SUPPLIER CONFERENCES

Every year, SEL hosts a Supplier Conference for vendors who supply us with component parts, equipment, and services. During this event, more than 200 companies come to our headquarters in Pullman, Washington, where we share our technical needs and strategic objectives for the coming year and identify ways of partnering to ensure a continuous supply of quality parts.

ONSITE AUDITS

This relationship-building continues throughout the year as we conduct onsite audits of our suppliers to verify that their quality and security processes meet our required specifications.

ORGANIZATIONAL APPROACH TO SUPPLIER SELECTION AND MONITORING

At SEL, supply chain risk management relies on cross-functional collaboration. The process begins with the selection of vendors, which is a team effort between product development, quality, and purchasing. Similarly, different teams weigh in on component selection, ongoing monitoring of vendors and parts, and onsite vendor audits. The approach makes risk management everyone's responsibility.

PRIVACY

We do not share our bills of materials (BOMs). We provide forecasts by part number, unrelated to the product. We never send out design schematics in order to avoid disclosing other vendor product and part information.

Effective Security Depends on Awareness, Speed, and Flexibility

Companies need freedom to:

- Use all available tools.
- Improve upon available tools through innovation.
- Proactively mitigate risks.
- Quickly resolve potential vulnerabilities.

To Keep Pace With Technology, Security Should Be Dynamic

SEL knows our own business better than anyone else. Because of this, we understand that what's "required" may not always be enough. To achieve our own high security standards, we challenge ourselves to exceed the status quo and constantly invent new ways to mitigate risks and improve quality.

Step 2: Rate Suppliers' Risks

PQFIDS

At SEL, we employ a supplier rating system that evaluates every supplier based on price, quality, features, innovation, delivery, and service (PQFIDS). To arrive at this rating, we assess the following supplier risks:

- Manufacturing locations
- Material lead times
- Financial health
- Replenishment methodologies
- Technology type
- On-time delivery performance

OUR SUPPLIERS' SUPPLIERS

It's not enough to know our first-tier suppliers. We ask our suppliers to identify their first-tier suppliers, along with their key risks, mitigation strategies, and replenishment methodologies.

PREFERENCE FOR DOMESTIC SUPPLIERS

To the greatest extent possible, we source within the United States.

TRANSPORTATION AND SHIPPING SUPPLIER QUALIFICATION

To help ensure the secure delivery of our products to our customers, we apply the same supplier qualification processes to our transportation and shipping suppliers.



Step 3: Ensure Component Integrity

COMPONENT QUALIFICATION PROCESS

To ensure the integrity of our products, we verify the performance of all purchased components against supplier product specifications.

DIRECT PROCUREMENT

We procure components directly from the manufacturer or official distributors. If components must be purchased outside of this prescribed process, we take additional steps to ensure their integrity: we use x-ray, inspect packaging, and consult the manufacturer's design drawings.

CONTINUOUS TESTING

Throughout the manufacturing process, we are constantly testing our products. If variations in performance are found, we work to understand the root cause of that variation. We have also developed methods to detect counterfeit products.

FINAL DELIVERY

When requested, we support our customers with installation and commissioning, further ensuring component and product integrity.

Step 4: Keep Track of Components and Products

EASY-TO-ACCESS INFORMATION

We keep a detailed record of every product we manufacture so we know where our products are installed and can notify customers about potential quality or security issues.

OUTSTANDING WARRANTY

Offering the best warranty in the industry provides an incentive for our customers to return products to us when they fail. We can then examine these products and find the root causes of defects, which in turn enables us to identify problems with our design process or with our suppliers and thus allowing us to improve our product designs. SEL provides a ten-year warranty at no cost on all products.



Step 5: Ensure Component Availability

IDENTIFYING AT-RISK PARTS

Because SEL keeps a detailed record of every product we manufacture, in the aftermath of the 2011 Japanese earthquake and tsunami, we were able to quickly identify which parts were at risk of becoming depleted. We immediately moved to purchase additional inventory from existing or alternative suppliers to ensure the uninterrupted flow of SEL products to customers.

MINIMIZING THE IMPACT OF DISRUPTIONS

SEL works with suppliers to ensure we and they keep sufficient inventory of specialty parts.

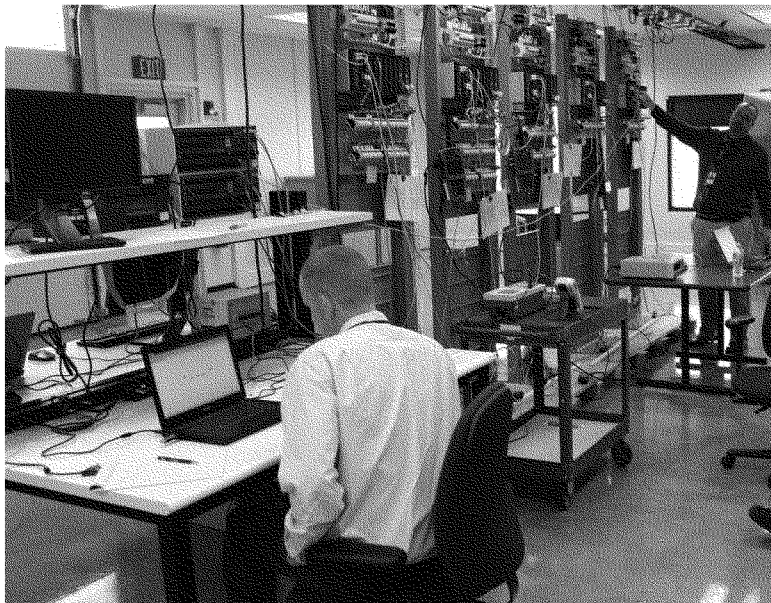
Step 6: Collaborate With Customers and Industry

CUSTOMER INSPECTION AND FEEDBACK

We regularly invite our customers to our facilities so they can inspect our supply chain security risk management practices, our product testing, and our quality processes. Throughout the procurement process, SEL works to understand the supply chain security and compliance needs of our customers so we can help them achieve their specified goals and/or requirements.

INDUSTRY INVOLVEMENT

We participate in various government-led initiatives and standards development activities so we can be aware of the current best practices of others, contribute to industry best practices, and stay attuned to the evolving demands placed on our customers. Similarly, we contribute to and use guidance documents, such as the NIST Cybersecurity Framework, to improve our own processes and controls and help shape agreed upon industry best practices.



Step 7: Build Security Into Company Practices

SOURCE CODE

We own every line of our source code, and we do not share source code or schematics.

INTERNAL TESTING

SEL has a robust process that uses both standards and special testing. All testing is performed onsite at SEL by SEL employees.

NEED TO KNOW

We compartmentalize projects and do not share information internally unless there is a need to know.

ROBUST ARCHITECTURES

We embrace simplicity of design and apply this to create resilient control system and product architectures.

CYBERSECURITY

We embed cybersecurity from the earliest stages of product development and enforce strict security practices for employees and visitors.

ROOT CAUSE

Every failure is significant. We get to the root cause of every problem.

Step 8: Ongoing Risk Management

EMERGING RISK MONITORING

Executives at SEL include risk management as part of their daily activities. They stay informed of emerging threats to the supply chain and make adjustments accordingly.

IN-HOUSE SOFTWARE DEVELOPMENT

We develop the majority of the software that our products use. If we use third-party software, we acquire the source code. Products go through numerous peer reviews. We also use automated tools for inspecting code in order to identify potential issues developers may have missed.

VERTICAL INTEGRATION

SEL makes many of our product components in-house. This allows us to ensure high quality as well as grow our expertise with that component.

SEL—Who We Are

SEL partners with utilities and industries around the world to ensure the safe, reliable, and economical delivery of electric power to critical infrastructure. In 1984, SEL introduced the world's first commercially available digital relay, revolutionizing the protection of electrical systems. Since then, we have developed and manufactured products for the protection, monitoring, control, automation, measurement, and metering of electric power systems. We are 100 percent employee-owned and have been manufacturing our products in the United States since we were founded.

Managing supply chain risks is fundamental to ensuring the quality of our products. SEL's Quality Management System is certified to the International Organization for Standardization (ISO) 9001 Quality Management Systems Standard. This certification is evidence that our critical design, manufacturing, and business processes meet the exacting requirements of this internationally recognized standard. Our manufacturing processes comply with the workmanship standard IPC-A-610 Class 3 for products requiring high reliability, such as those used in life-support and aerospace systems.

At SEL, our objective is not to just comply with existing standards, but to exceed them. We constantly identify, measure, and improve our processes so we can consistently surpass our customers' expectations.



SEL's Quality Policy

At SEL, our quality policy is to "Understand, Create, and Simplify." This represents our relentless pursuit of understanding opportunities and challenges, creating innovative solutions, and ensuring those solutions are simple and robust.



Making Electric Power Safer,
More Reliable, and More Economical

Schweitzer Engineering Laboratories

Tel: +1.509.332.1890 | Email: info@selinc.com | Web: www.selinc.com

© 2016 by Schweitzer Engineering Laboratories, Inc.
PF00551 • 20161219

