

**PRIVATE SECTOR AND GOVERNMENT  
CHALLENGES AND OPPORTUNITIES TO  
PROMOTE THE CYBERSECURITY AND  
RESILIENCY OF OUR NATION'S  
CRITICAL ENERGY INFRASTRUCTURE**

---

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON**  
**ENERGY AND NATURAL RESOURCES**  
**UNITED STATES SENATE**  
ONE HUNDRED FIFTEENTH CONGRESS  
SECOND SESSION

—————  
MARCH 1, 2018  
—————



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

WASHINGTON : 2019

COMMITTEE ON ENERGY AND NATURAL RESOURCES

LISA MURKOWSKI, Alaska, *Chairman*

JOHN BARRASSO, Wyoming	MARIA CANTWELL, Washington
JAMES E. RISCH, Idaho	RON WYDEN, Oregon
MIKE LEE, Utah	BERNARD SANDERS, Vermont
JEFF FLAKE, Arizona	DEBBIE STABENOW, Michigan
STEVE DAINES, Montana	JOE MANCHIN III, West Virginia
CORY GARDNER, Colorado	MARTIN HEINRICH, New Mexico
LAMAR ALEXANDER, Tennessee	MAZIE K. HIRONO, Hawaii
JOHN HOEVEN, North Dakota	ANGUS S. KING, JR., Maine
BILL CASSIDY, Louisiana	TAMMY DUCKWORTH, Illinois
ROB PORTMAN, Ohio	CATHERINE CORTEZ MASTO, Nevada
SHELLEY MOORE CAPITO, West Virginia	TINA SMITH, Minnesota

BRIAN HUGHES, *Staff Director*

PATRICK J. McCORMICK III, *Chief Counsel*

BRIANNE MILLER, *Senior Professional Staff Member and Energy Policy Advisor*

MARY LOUISE WAGNER, *Democratic Staff Director*

SAM E. FOWLER, *Democratic Chief Counsel*

DAVID GILLERS, *Democratic Senior Counsel*

SCOTT MCKEE, *Democratic Professional Staff Member*

# CONTENTS

## OPENING STATEMENTS

	Page
Murkowski, Hon. Lisa, Chairman and a U.S. Senator from Alaska .....	1
Cantwell, Hon. Maria, Ranking Member and a U.S. Senator from Washington .....	3
Duckworth, Hon. Tammy, a U.S. Senator from Illinois .....	5

## WITNESSES

Walker, Hon. Bruce J., Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy .....	6
Matheson, Hon. Jim, Chief Executive Officer, National Rural Electric Cooperative Association .....	17
Endicott-Popovsky, Dr. Barbara, Executive Director, Center for Information Assurance and Cybersecurity, University of Washington .....	30
Sanders, Dr. William H., Donald Biggar Willett Professor of Engineering, and Head, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign .....	59
Lee, Robert M., Chief Executive Officer and Co-Founder, Dragos, Inc. ....	67

## ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

Cantwell, Hon. Maria: Opening Statement .....	3
Duckworth, Hon. Tammy: Opening Statement .....	5
Endicott-Popovsky, Dr. Barbara: Opening Statement .....	30
Written Testimony .....	32
Responses to Questions for the Record .....	167
Lee, Robert M.: Opening Statement .....	67
Written Testimony .....	70
Responses to Questions for the Record .....	205
Matheson, Hon. Jim: Opening Statement .....	17
Written Testimony .....	19
Responses to Questions for the Record .....	164
Murkowski, Hon. Lisa: Opening Statement .....	1
Sanders, Dr. William H.: Opening Statement .....	59
Written Testimony .....	61
Responses to Questions for the Record .....	202
Walker, Hon. Bruce J.: Opening Statement .....	6
Written Testimony .....	9
Responses to Questions for the Record .....	154



**PRIVATE SECTOR AND GOVERNMENT  
CHALLENGES AND OPPORTUNITIES TO  
PROMOTE THE CYBERSECURITY AND  
RESILIENCY OF OUR NATION'S  
CRITICAL ENERGY INFRASTRUCTURE**

---

**THURSDAY, MARCH 1, 2018**

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

The Committee met, pursuant to notice, at 10:00 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, everyone. The Committee will come to order as we begin our hearing on the cybersecurity and resiliency of our critical energy infrastructure.

Cyberattacks are a well-documented and continuing threat. Every day we seem to hear of yet another incident. Increasingly, it appears that the bad actors are nation-states and sophisticated entities, such as organized crime or terror groups. These attacks are across-the-board and not limited, of course, to energy infrastructure.

Just last week, according to the news reports out there, U.S. intelligence identified efforts by Russian military spies to attack computers used by Olympic officials during this year's games. Reportedly, their goal was to make it look as if North Koreans were leading the cyberattack. Acts of cyber intrusion such as these can jeopardize diplomatic relations and could have more serious repercussions.

Just a couple days ago, the Director of the Division of Elections in my home State of Alaska again informed the public that Russian cyber actors made a failed attempt to access the Division's public website prior to the 2016 election. Apparently they merely scanned the state's system so this was not a 'breaking and entering' scenario, but it clearly underscores the persistence of the problem.

Here in the United States, the energy sector is clearly a high value target for cyberattacks. Earlier this month Entergy's security monitoring system detected a cyber intrusion on the company's corporate network. Thankfully, the intrusion was on the corporate side and did not affect energy delivery or reliability, but again, bad

actors will test any available avenue in an attempt to infiltrate energy networks.

Our Committee has spent a lot of time, many hours, examining the threats to energy infrastructure. We have learned about the potential challenges of increased digitalization of the energy sector and opportunities to improve cybersecurity by engineering in protections and developing strong cybersecurity protocols.

We have repeatedly heard how protection of our nation's critical assets is a shared responsibility, with federal, state and private sector partners working together to improve cyber defenses and sharpen responses to cyberattacks. We know there is more work to be done to improve that collaborative work. We are alert to the danger that "shared responsibility" can, in practice, be the hardest responsibility to consistently and accountably discharge.

Now we have also legislated to help address the cybersecurity problem. In the Energy Policy Act of 2005, Congress imposed mandatory reliability standards, including cyber standards, on the electric industry. And today we will hear testimony that these standards have led to meaningful improvements. The electric sector is still the only sector that has such stringent requirements, but we will also hear that keeping the nation safe from major cyber threats goes well beyond regulation.

Last Congress, in the FAST Act, we enacted provisions authored by this Committee to codify the Department of Energy as the sector-specific agency for the energy sector and we provided the Secretary with the authority to address grid-related emergencies, including cyberattacks. We also sought to facilitate greater information sharing by protecting sensitive information from disclosure. I am pleased to report that public and private sector efforts not only to identify threats and share information but also to improve the capabilities for detecting and responding, are intensifying.

So the question this morning is, "What do we do next?" What should the Federal Government do, or refrain from doing, to meet this dynamic and evolving threat? And how can the government help improve the cyber resiliency of critical energy infrastructure if a threat becomes a reality?

Mr. Walker's testimony states that Secretary Perry is establishing a distinct "Office of Cybersecurity, Energy Security, and Emergency Response." This new office, which will be known by the acronym C.E.S.E.R.—we are already referring to it I guess as Caesar, big shoes here.

[Laughter.]

But much of CESER's lineage is from the Department's current office, the Office of Electricity Delivery and Energy Reliability, which was established after the 2003 Northeast Power Blackout.

Mr. Walker, we appreciate the Department's attention to this important topic and certainly look forward to learning more about this new office and how you intend it operate and function.

Protecting our nation's energy infrastructure, we all agree, is critical to maintaining so much of the American way of life. We must determine what the next appropriate steps will be to further identify and prevent cyber intrusions and increase resiliency in the event of an attack. Those solutions may not require more regulation, but rather more common sense and cooperation.

I appreciate the expert witnesses that we have before us today, that you have made time to be before the Committee. I will introduce them after Senator Cantwell's opening comments, but we appreciate you being here.

Senator Cantwell.

**STATEMENT OF HON. MARIA CANTWELL,  
U.S. SENATOR FROM WASHINGTON**

Senator CANTWELL. Thank you, Madam Chair, and thank you for holding this important hearing. I am sure that the Chair has probably grown weary of how many times I bring up cybersecurity.

[Laughter.]

Both in our negotiations on an energy bill, now almost two years ago, the need to be more expeditious about the process, and my continued concern about it from the perspective of one of the greatest threats facing our nation.

So I am delighted to have the panelists before us today to focus on what our nation needs to do to be more expeditious in our agenda on cybersecurity.

Obviously, cybersecurity, as it impacts our energy infrastructure, is one of the key issues for this Committee. We used to say that we were worried about foreign entities entering our airspace, our shipping lanes, or any kind of unwanted provocations. Now they come in the form of cyberattacks.

So make no mistake, our nation's energy infrastructure is under that attack from Russians and other state actors. We know, according to the Ukrainians, Russia took out part of the Ukraine electricity grid in 2015 and 2016 through cyber means. WIRED magazine, at the time, chillingly suggested that the entire nation of the Ukraine was becoming a Russia test lab for cyber war.

As one of our witnesses will say today—Dragos has said that the Russian government has devised a cyber weapon that has the potential to be one of the most disruptive yet against our electricity system. So we look forward to hearing more on that.

In the last year, the Washington Post reported that Russian government hackers were behind cyber intrusions into a nuclear power plant's business system. We know from our own northwest lab that the firewall that protects much of our information, they have communications of something like 25,000 a day, cyberattacks against that system.

We know what is happening and, as the Chair mentioned, we know that the Administration has set up a cyber office which we appreciate but we want the Administration to be much more aggressive.

We have been pushing for over a year now asking for a threat assessment to our electricity grid. I think it was June 22, 2017, that we wrote the White House asking them to perform a required assessment on protecting the grid from cyberattacks.

I know, Mr. Walker, you are here today and you will try to enlighten us on the work that you have been doing in your short period of time, which is a lot given the Puerto Rico situation, so we appreciate that. Nonetheless, we want the Department of Energy to respond to this letter of a year ago asking them what we are doing to protect the reliability of our electricity grid from Russian

hacking. This was sent by many U.S. Senators and we have yet to have a response.

Why is this so important? We saw just this morning the German government was hacked by Russian actors. According to the German Interior Ministry, we can confirm that the Federal Office of Information Security and Intelligence Services were part of a cyber hack.

So this issue is not going away. It is only growing in incredible importance. We don't want to have an Administration asleep at the computer terminal while we are sitting here worrying about American business and government interests and national security interests being attacked by state-owned actors.

I also hope that we can see, as we specifically asked Secretary Perry during his confirmation hearing, that the Administration will support a robust infrastructure investment as it relates to cybersecurity. I know he told the Committee at the time that he believed that we should do that and we want to see in this next budget legislation, that commitment. I know that the Chair and I had a chance to talk to the President at an infrastructure discussion a couple weeks ago, and we emphasized how much energy infrastructure needed to be part of a national infrastructure investment bill. So now is the time for action.

We also discussed, and the Chair and I have in legislation, a clear focus on how important workforce is to a critical energy infrastructure for the future, including cybersecurity.

Our state, the State of Washington, has been a leader in developing a cyber workforce training, and I would like to welcome Professor Barbara Endicott-Popovsky to testify today. She is the Executive Director at the Center for Information Assurances and Cybersecurity at the University of Washington, a national leader in pioneering cyber education.

We were able to have a forum there recently to see how business, education and the cybersecurity community was coming together to try to focus on cybersecurity solutions. She has been shaping cybersecurity education policy and has authored more than 100 peer-reviewed articles. So we welcome what you have to say today on this issue.

She recognizes, as I do, that one of the biggest challenges to the nation's cyber preparedness is a skilled workforce and that by 2020 IBM estimates that there will be 1.5 million unfilled cybersecurity positions across all industries. That is mind boggling, mind boggling, to think about but not hard to imagine given that we live in an information age and how connected everything is going to be and how every layer will also need security and reinforcement.

I hope that today's hearing will help illuminate for us how much investment we really need to make to make that part of our energy infrastructure work cost-effectively.

We know that some of the challenges that we face is getting that curriculum well established and also making sure that different aspects of the cybersecurity challenge are addressed everywhere from two-year degrees to PhDs. I do think the Department of Energy has a role to play here in defining for individuals interested in this area, the partnerships that will be necessary to skill that workforce in a timely fashion.

All in all, Madam Chair, thank you so much for the hearing today. Thank you for the attention to this issue. I know you and I keep hoping that there will be some cybersecurity legislation that moves through the Full Congress as it has already moved through the Senate. So, maybe, I don't know if the third time is the charm, but hopefully we will be able to use these very important events that have transpired across the entire world to get our colleagues to see the urgency of the situation.

So again, thank you for the hearing.

The CHAIRMAN. Thank you, Senator Cantwell, and thank you for your persistent push on the cybersecurity piece of it.

As you mention, we think we have a good, strong, bipartisan bill. We would like to see that be more than just a bill. We would like to see it be law and to put in place some of these protections that we have been working on so hard, but I greatly appreciate your continued focus on this.

We have a good, strong panel with us this morning. Again, welcome.

We have our Assistant Secretary for the Department of Energy, Mr. Bruce Walker. It is good to have you back before us.

We are also joined by former Congressman Jim Matheson. Congressman Matheson represented Utah from 2001 to 2015. He is now the CEO of the National Rural Electric Cooperative Association (NRECA). It is good to have you before the Committee.

Dr. Barbara Endicott-Popovsky with the Center for Information Assurance and Cybersecurity at the University of Washington has just been introduced by Senator Cantwell. We are very pleased that you could join us this morning.

Dr. William Sanders is from the University of Illinois, and I will let Senator Duckworth introduce him.

But let me also welcome Mr. Robert Lee, who is the CEO of Dragos Incorporated. It is good to have you with the Committee.

Senator Duckworth, if you would like to introduce your fine constituent.

**STATEMENT OF HON. TAMMY DUCKWORTH,  
U.S. SENATOR FROM ILLINOIS**

Senator DUCKWORTH. Thank you, Chairwoman Murkowski.

I would like to extend a very warm welcome to Dr. Sanders, who is joining us from the University of Illinois at Urbana-Champaign. They have some great farm-to-table restaurants there, by the way.

I am proud that the University of Illinois was one of the very first universities to recognize the importance of ensuring that cybersecurity and cyber resiliency of our energy infrastructure.

Dr. Sanders serves as the head of the Department of Electrical and Computer Engineering and is an expert on computing and critical infrastructure, such as the power grid.

Over the past several decades, Dr. Sanders has published over 270 technical papers in these areas and received the 2016 IEEE Innovation and Societal Infrastructure Award.

He has used his expertise to assist the government's efforts to make the grid more secure and resilient. This work includes leading an initiative of the Department of Energy and the Department

of Homeland Security on building a better, more secure and resilient power grid.

Dr. Sanders, I am thrilled that you are able to join us today. I think your voice will be a very valuable one to today's discussion.

We all know that future battles will increasingly exist in cyberspace and that cybersecurity is a critical aspect of our national security, and I look forward to hearing your testimony and your recommendations concerning this very important issue.

Welcome.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator.

Again, thank you all.

I would ask that you try to keep your comments to about five minutes. Your full statements will be included as part of the record.

I will note for colleagues that we are scheduled to have votes. I think it is 11:45 when we have a series of three votes that are set up. My intention this morning is to try to move as quickly as we can so that we can get in as many questions as we can to this fine group of experts.

Assistant Secretary Walker, if you would like to lead off.

Thank you.

**STATEMENT OF HON. BRUCE J. WALKER, ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, U.S. DEPARTMENT OF ENERGY**

Mr. WALKER. Thank you. Good morning.

Chairman Murkowski, Ranking Member Cantwell, and distinguished members of the Committee, thank you for the opportunity to discuss the continuing cybersecurity threats facing our national energy infrastructure and the Department of Energy's role in protecting it.

Establishing a resilient energy infrastructure is a top priority of the Secretary and a major focus of the Department; hence, our focus on cybersecurity is paramount.

Our national security and economy depend on the availability of a reliable and resilient energy infrastructure. The mission of the Office of Delivery and Energy Reliability, OE, is to strengthen, transform and improve the resiliency of energy infrastructure to ensure access to reliable and secure sources of energy.

The Secretary and DOE are committed to working with our public and private sector partners to protect the nation's critical energy infrastructure from physical security events, natural and man-made disasters and cybersecurity threats.

To demonstrate our focus on the aforementioned mission, the Secretary announced last month he's establishing an Office of Cybersecurity, Energy Security and Emergency Response, better known as CESER. This organization change will strengthen the Department's role as the energy sector-specific agency for cybersecurity thereby supporting our national security responsibilities.

The creation of this office will build upon what we do today, significantly increase the Department's focus on energy infrastructure protection and will enable more coordinating preparedness and response to physical and cyber threats as well as natural disasters.

Furthermore, the CESER Office will play an essential role in coordinating government and industry efforts to address these energy sector threats.

The President has requested slightly more than \$95 million in FY2019 for CESER with a focus on early stage R&D activities, working with our national labs to improve cybersecurity and resilience, to harden and evolve critical grid infrastructure. These activities will develop the next generation of cybersecurity control systems, components and devices, including enhancing our ability to share time-critical data with industry to detect, prevent and recover from cyber events.

Our national intelligence agencies have noted the increasing number and sophistication of cyber threats. Our adversaries understand the energy sector is a valuable target because of the assets that the sector controls, including our defense critical energy infrastructure.

DOE's role in energy sector cybersecurity was codified by Congress under the FAST Act. That legislation designated DOE as the sector-specific agency for cybersecurity. As a result, the Secretary of Energy is authorized upon the 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.

In order to properly plan for this type of occurrence, it is critical that we continue to work closely with our energy, industry and federal agency partners. In the energy sector, the core of critical infrastructure partners consists of the Electricity Subsector Coordinating Council, the Oil and Natural Gas Subsector Coordinating Council and the Energy Government Coordinating Council.

The Energy Government Coordinating Council is led by CESER and DHS and it is where the interagency partners, states and international partners come together to discuss the important security and resilience issues for the energy sector. Collectively, we all work together under DHS' Critical Infrastructure Partnered Advisory Council which provides a mechanism for industry and government coordination.

As a part of the Comprehensive Energy Cybersecurity Resiliency Strategy, the Department of Energy, working with our industry partners, is focusing cyber support efforts to enhance visibility and situational awareness of operational networks, increase alignment of cybersecurity preparedness and planning across local, state and federal levels and leveraging the expertise of our national labs to drive cybersecurity innovation.

In conclusion, cyber threats continue to evolve and DOE is working diligently to eliminate and mitigate the potential consequences of these threats. Establishing the CESER Office is a result of our laser-focused attention to cyber and physical security.

Our long-term vision is significant and will positively impact our national security. The establishment of this office will be the first step in the transformational change necessary to meet the ever-changing cyber landscape highlighted by our national intelligence agencies.

Finally, I would like to highlight that the risk of physical and cyber threats is continually exacerbated by a set of circumstances

that are increasingly interdependent of the various energy systems throughout the nation. This significantly increases our overall risk due to the increased number of penetration points that can significantly impact national security and economy.

As always, 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.

Thank you.

[The prepared statement of Mr. Walker follows:]

**Written Testimony of Assistant Secretary Bruce J. Walker**  
**Office of Electricity Delivery and Energy Reliability**  
**U.S. Department of Energy**  
**Before the**  
**U.S. Senate**  
**Committee on Energy and Natural Resources**

**March 1, 2018**

**Introduction**

Chairman Murkowski, Ranking Member Cantwell, and distinguished Members of the Committee, thank you for the opportunity to discuss the continuing cybersecurity threats facing our national energy infrastructure and the Department of Energy's (DOE's) role in protecting it. Establishing a resilient energy infrastructure is a top priority of the Secretary and a major focus of the Department; hence, our focus on cybersecurity is paramount.

Our national security and economy depend on the availability of a reliable and resilient energy infrastructure. The mission of the Office of Electricity Delivery and Energy Reliability (DOE-OE) is to strengthen, transform, and improve the resiliency of energy infrastructure to ensure access to reliable and secure sources of energy. The Secretary and DOE are committed to working with our public and private sector partners to protect the Nation's critical energy infrastructure from physical security events, natural and man-made disasters, and cybersecurity threats.

**Office of Cybersecurity, Energy Security, and Emergency Response**

To demonstrate our focus on the aforementioned mission, the Secretary announced last month that he is establishing an Office of Cybersecurity, Energy Security, and Emergency Response (CESER). This organizational change will strengthen the Department's role as the sector-specific agency (SSA) for cybersecurity in the energy sector, supporting our national security responsibilities.

The CESER office will play an essential role in coordinating government and industry efforts to address these energy sector threats. Initially, the office will be comprised of work we currently do in DOE-OE's Infrastructure Security and Energy Restoration (ISER) division and Cybersecurity and Emerging Threats Research and Development (CET R&D) division.

The President has requested slightly more than \$95 million in FY 2019 for CESER with a focus on early-stage activities that improve cybersecurity and resilience to harden and evolve critical grid infrastructure. These activities include early-stage R&D at National Laboratories to develop the next generation of cybersecurity control systems, components, and devices including a greater ability to share time-critical data with industry to detect, prevent, and recover from cyber events.

The creation of the CESER office will build on all that we do today and elevate the Department's focus on energy infrastructure protection and will enable more coordinated preparedness and response to cyber and physical threats and natural disasters. This must include electricity delivery, oil and natural gas infrastructure, and all forms of generation. The Secretary's desire to create dedicated and focused attention on these responsibilities will provide greater visibility, accountability, and flexibility to better protect our Nation's energy infrastructure and support asset owners.

*The Unique Nature of Energy Sector Cybersecurity*

During a hearing last month before the Senate Select Committee on Intelligence on Worldwide Threats, the Director of National Intelligence testified that the growing cyber threat is "one of my greatest concerns." At that same hearing, the Director of the National Security Agency and head of U.S. Cyber Command stated that "if you look at the internet of things, if you look at the security levels within those components . . . if we think the problem is a challenge now; just wait. It's going to get much, much worse." As the Intelligence Community Worldwide Threat Assessment indicates, cyber threats will only continue to increase and the criticality of DOE's role as the sector-specific agency necessitates a more focused approach to cybersecurity.

Our National Intelligence Agencies have noted the increasing number and sophistication of cyber threats. Cyber attacks targeting "information technology," or IT, including computing and business applications, to cause disruptions, obtain access to email accounts and personal information, exfiltrate data to release to the world at large, and exploit information for private gain are growing increasingly common. The energy sector is not immune to such attacks.

Moreover, our adversaries understand that the energy sector is a valuable target because of the assets that the sector controls; including, our defense critical energy infrastructure. Accordingly, we have seen an increased interest in vulnerabilities of the "operating technology," or OT, of energy delivery systems and other critical infrastructure as well. OT systems consist of industrial control systems (or ICS), programmable logic controls, and their associated supervisory control and data acquisition software (known as SCADA). The heavy use of OT systems has made electric utilities, oil and natural gas providers, hydro and nuclear facilities, and water utilities prime targets for OT-related cyber attacks. The disruption of any one of these is not only inherently problematic, it also hampers the ability to respond to other types of emergency events.

The Department of Homeland Security's (DHS's) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) coordinates control systems-related security incidents and information sharing with Federal, state, and local agencies and organizations, the intelligence

community, and private sector constituents. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community. ICS-CERT responded to 295 incidents in FY 2015, 46 of which were in the energy critical infrastructure (CI) sector. And while only 290 incidents were responded to in FY 2016, the energy CI sector accounted for 59 of the events.<sup>1</sup>

*DOE's Roles and Responsibilities for Energy Sector Cybersecurity*

In preparation for, and response to, cybersecurity threats, 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 a cyber incident 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: 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 the National Cyber Investigative Joint Task Force, respectively. In the event of a cybersecurity emergency in the energy sector, closely aligning DOE's activities with those of our partners at DHS and DOJ ensures DOE's deep expertise with the sector is appropriately leveraged.

DOE's role in energy sector cybersecurity was codified by Congress through the Fixing America's Surface Transportation (FAST) Act. That legislation designated DOE as the Sector Specific Agency for Energy Sector Cybersecurity. In extreme cases, the Department can use its legal authorities such as those in the Federal Power Act, as amended by the FAST Act, to assist in response and recovery operations. Congress enacted several important new energy security measures in the FAST Act as it relates to cybersecurity. The Secretary of Energy was provided a 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 respond as needed to the threat of cyber and physical attacks on the grid. The Grid Security Emergency authority is unique to DOE and an important element in partnering with DHS and DOJ to fully address the cybersecurity risks to the energy sector.

---

<sup>1</sup> DOE also collects information on electric incidents and emergencies through the Electric Emergency Incident and Disturbance Report (Form OE-417). Electric utilities that operate as Control Area Operators and/or Reliability Authorities, as well as other electric utilities as appropriate, are required to file the form whenever an electrical incident or disturbance is sufficiently large enough to cross reporting thresholds. In the case of cybersecurity, reporting is required for a cyber event that causes interruptions of electrical system operations or an event that could potentially impact electric power system adequacy or reliability. In 2016, five of the 141 events reported were cyber-related, compared with three of 150 events in 2017. For the month of January this year, two of the 18 reported events were cyber-related. [https://www.oe.netl.doe.gov/OE417\\_annual\\_summary.aspx](https://www.oe.netl.doe.gov/OE417_annual_summary.aspx)

In the energy sector, the core of critical infrastructure partners consists of 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 co-chaired with 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 that we are working together in a whole-of-government response.

As defined in the National Infrastructure Protection Plan, the industry coordinating councils or “SCCs” are created by owners and operators and are self-organized, self-run, and self-governed, with leadership designated by the SCC membership. The SCCs serve as the principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience coordination and planning, as well as a range of sector-specific activities and issues.

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 Strategy for the Energy Sector**

DOE plays a critical role in supporting energy sector cybersecurity to enhance 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 an ecosystem of resilience: a network of producers, distributors, regulators, vendors, and public partners, acting together to strengthen our ability to prepare, respond, and recover.

As part of a comprehensive energy cybersecurity resilience strategy, the Department is focusing cyber support efforts to enhance visibility and situational awareness of operational networks; increase alignment of cyber preparedness and planning across local, state, and Federal levels; and leverage the expertise of DOE’s National Labs to drive cybersecurity innovation.

##### *Enhance Visibility and Situational Awareness of Operational Networks*

It is necessary for partners in the energy sector and the government to share emerging threat data and vulnerability information to help prevent, detect, identify, and thwart cyber attacks 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.

The purpose of CRISP is to share information among electricity subsector partners, DOE, and the Intelligence Community to facilitate the timely bi-directional sharing of unclassified and classified threat information to enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the Intelligence Community to better inform the energy sector of the high-level cyber risks.

Current CRISP participants provide power to over 75 percent of continental United States electricity customers. If CRISP has demonstrated one finding to DOE, it is 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.

DOE's 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.

Advancing the ability to improve situational awareness of OT networks is a key focus of DOE's current activities. The Department is currently in the early stages of 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 – and having the ability to store and retrieve network traffic from the recent past – can be the first step in stopping an attack in its early stages.

#### *Increase Alignment of Cyber Preparedness and Planning Across Local, State, and Federal Levels*

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-OE 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 resilient to cyber threats. This document is publicly available on the NARUC Research Lab website, benefitting not only regulators, but state officials as well.

We are continuing to work with the NARUC Research Lab to support regional trainings on cybersecurity throughout the year, with the goal of building commissioner and commission staff

expertise on cybersecurity so they ensure cyber investments are both resilient and economically sound.

DOE also continues to work closely with our public and private partners so our response and recovery capabilities fully support and bolster the actions needed to help ensure the reliable delivery of energy. We continue to coordinate with industry through the SCCs to synchronize government and industry cyber incident response playbooks.

DOE-OE engages directly with our public and private sector stakeholders to help ensure we all are prepared and coordinated in the event of a cyber incident to the industry. Innovation and preparedness are vital to grid resilience. DOE and the National Association of State Energy Officials (NASEO) co-hosted the Liberty Eclipse Exercise in Newport, Rhode Island, which focused on a hypothetical cyber incident that cascaded into the physical world, resulting in power outages and damage to oil and natural gas infrastructure. The event featured 96 participants from 13 states, and included representatives from state energy offices, emergency management departments, utility commissions, as well as Federal partners, such as FEMA, and private sector utilities and petroleum companies.

And late last year, DOE participated in GridEx IV, a biennial 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. This and other similar large scale exercises continue to highlight the interdependencies between our Nation's energy infrastructure and other sectors.

While the after-action report has yet to be released, during GridEx IV, it was clear that collaboration between industry and the Federal government has strengthened greatly since Superstorm Sandy and GridEx III. The executed coordination in response to this year's hurricane season also is evidence of this strengthening.

Communication capabilities that are survivable, reliable, and accessible, by both industry and government, will be key to coordinate 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 industry, Federal, and state partners now to further shape the types of orders that may be executed under the Secretary's authority, while also clarifying how we communicate and coordinate the operational implementation of these orders.

Continued coordination with Federal and industry partners and participation in preparedness activities like GridEx enables DOE to identify gaps and develop capabilities to support cyber response as the SSA.

*Leverage the Expertise of DOE's National Laboratories to Drive Cybersecurity Innovation*

Beyond providing guidance and technical support to the energy sector, DOE-OE also supports a R&D portfolio designed to develop advanced tools and techniques to provide enhanced cyber protection for key energy systems. Intentional, malicious cyber threat challenges to our energy

systems are on the rise in both number and sophistication. This evolution has profound impacts on the energy sector.

Cybersecurity for energy control and OT systems is much different than that of typical IT systems. 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 be difficult.

DOE-OE'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 research and development effort. DOE-OE co-funds industry-led, National Laboratory-led, and university-led projects with 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 (S&T).

To select cybersecurity R&D projects, DOE constantly examines today's 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 cyber attack.

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 the commands would result in damage to the system or 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 which passively monitors all network traffic with and 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 they have the tools and resources needed to address security challenges. 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.

### **Conclusion**

Cyber threats continue to evolve and DOE is working diligently to eliminate and mitigate the potential consequences of these threats. Establishing the CESER office is a result of our laser focused attention to cyber and physical security. Our long-term vision is significant and will positively impact our national security. The establishment of this office will be the first step in the transformational change necessary to meet the ever changing cyber landscape highlighted by our National Intelligence Agencies.

Finally, I would like to highlight that the risk of physical and cyber threats is continuously being exacerbated by a set of circumstances that are increasing the interdependence of the various energy systems throughout the Nation. This significantly increases our overall risk due to the increased number of penetration points that can significantly impact national security and the economy.

As always, 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, Secretary Walker.  
Congressman Matheson, welcome.

**STATEMENT OF HON. JIM MATHESON, CHIEF EXECUTIVE OFFICER, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION**

Mr. MATHESON. Good morning, Chairman Murkowski and Ranking Member Cantwell, members of the Committee. I appreciate the invitation to testify before you on what is a very important topic.

I'm testifying today on behalf of more than 900 electric cooperatives who are working together to protect our U.S. electricity system from cyber threats. I just returned last night from the NRECA annual meeting with our membership and we also had a TechAdvantage conference, and I'm happy to share with you that cybersecurity was a significant topic of discussion of both of those meetings.

We had several breakout sessions on cybersecurity to share information with our members about the latest in policy and technology, and our members shared with each other examples of what they are doing to keep their systems secure. That peer-to-peer learning is a hallmark of the electric cooperative program.

Protecting the nation's complex interconnected electric power system while ensuring reliable, secure and affordable electricity has always been a top priority for electric co-ops and, quite frankly, for the entire electric power industry. Maintaining the resilience and security of the electric grid requires a flexible approach that draws upon a variety of tools, resources and options.

As threats and threat actors continue to evolve, so must the industry's capability to defend against them. The possibility of a cybersecurity attack affecting grid operations is something for which the electric sector has been preparing for years.

These preparations are built on the need for a flexible approach and they include implementing security standards and technologies to protect systems, forging close partnerships to identify threats and solutions and to respond to incidents, engaging in active information sharing about threats and vulnerabilities, participating in industry and cross sector disaster planning exercises such as DOE's clear path and the North American Electric Reliability Corporation's Grid X biannual exercise. We also partner with DOE, the National Labs and other federal agencies on cybersecurity research to improve tools and resources needed by the industry to address these threats.

Protecting the electric grid from threats that could affect national security and public safety is a responsibility shared by both the government and the electric power sector. As we continue working together to protect the electric system from cyber threats, there are a couple of areas that can benefit these partnerships and the sector that I'd like to highlight in these comments.

First, these efforts can be enhanced through continued cybersecurity research and development, including support for developing resources for small and medium-sized utilities. The Rural Electric Cooperative Association is active in cybersecurity research programs and initiatives supported by the DOE's Office of Electricity Delivery and Energy Reliability. Strong research and development

programs are essential to developing new technologies to keep pace with the rapidly changing cybersecurity threats that our industry faces. The DOE is our industry's primary source for federal funding to develop cybersecurity tools and resources.

Currently, one of the most valuable research programs for electric cooperatives is the funding partnership between DOE and the Rural Electric Co-ops, called the Rural Cooperative Cybersecurity Capabilities Program, or we call it RC3 for short. This partnership is specifically focused on addressing the unique cybersecurity needs of small and mid-sized distribution utilities. And in addition to developing cybersecurity resources and tools appropriate for these utilities, we have provided cybersecurity training to more than 150 of our members through the RC3 program.

The second area I'd mention in these comments is the need to continue improving information sharing between the government and electric utilities. In some circumstances, there are situations where the government possesses information on intelligence on a particular threat or vulnerability that could be timely and actionable for the industry. We support efforts aimed at increasing electric cooperatives access to this type of information thereby helping us to do an even better job of protecting the grid. The FAST Act and Cyber Information Sharing Act from last Congress were excellent and appreciated steps in this direction.

Information sharing, of course, is a bidirectional issue and assurances that sensitive information shared from industry to government will be properly protected and free of liability concerns when shared in good faith is also necessary. In addition, the government also holds information on terrorist activities. A voluntary process that allows utilities to have the FBI perform enhanced background investigation screening for critical employees in our industry could go a long way in helping to address some of the potential insider threat concerns.

So again, thank you for inviting me to testify today. We look forward to working with Congress on these issues and continuing in our successful partnerships with the DOE and other federal agencies.

I'm happy to answer any questions.

[The prepared statement of Mr. Matheson follows:]



**Testimony of The Honorable Jim Matheson  
Chief Executive Officer  
National Rural Electric Cooperative Association**

**to the Committee on Energy and Natural Resources  
U.S. Senate**

**March 1, 2018**

Jim Matheson, CEO  
National Rural Electric Cooperative Association  
March 1, 2018 Testimony

### **Introduction**

Chairwoman Murkowski, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to testify before you on this very important topic. I am Jim Matheson, the chief executive officer at the National Rural Electric Cooperative Association (NRECA) and I am testifying today on behalf of more than 900 electric cooperatives that are working together to protect U.S. energy delivery systems from cybersecurity threats.

I have served in that capacity since 2016 after serving in the U.S. House of Representatives for 14 years, including serving on the Energy and Commerce, and the Transportation and Infrastructure Committees. I also was a principal at Squire Patton Boggs in Washington, D.C., and worked in the energy industry for several years before my years of government service.

NRECA is the national service organization for America's electric cooperatives. Member-owned, not-for-profit electric co-ops constitute a unique sector of the electric utility industry and provide electricity to more than 42 million people in 47 states. Electric cooperatives are driven by their purpose to power communities and empower their members to improve their quality of life. Affordable electricity is the lifeblood of the American economy, and electric co-ops have provided energy and other services that grow their communities. Because of their critical role in providing affordable, reliable, and universally accessible electric service, electric cooperatives are vital to the economic health of the communities they serve.

America's electric cooperatives serve 56 percent of the nation's landmass, 88 percent of all counties, and 12 percent of the nation's electric customers, while accounting for approximately 13 percent of all electricity sold in the United States. NRECA's member cooperatives include 63 generation and transmission (G&T) cooperatives and 834 distribution cooperatives. The G&Ts are owned by the distribution cooperatives they serve. The G&Ts generate and transmit power to nearly 80 percent of the distribution cooperatives, and those distribution cooperatives provide power directly to the end-of-the-line member-owners. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. NRECA members account for about five percent of national generation and, on net, generate approximately 50 percent of the electric energy they sell. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

In my leadership role at NRECA, I represent electric cooperatives on the Steering Committee of the Electric Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between leadership in the federal government and in the electric power sector, with the mission of coordinating efforts to prepare for national-level incidents or threats to critical infrastructure. Protecting the electric grid from threats that could impact national security and public safety is a responsibility shared by both the government and the electric power sector. The ESCC supports policy- and public affairs-related activities and initiatives designed to enhance the reliability and resilience of the electric grid. The ESCC coordinates with senior Administration officials from the White House, Department of Energy (DOE), Department of

Jim Matheson, CEO  
 National Rural Electric Cooperative Association  
 March 1, 2018 Testimony

Homeland Security (DHS), the Federal Energy Regulatory Commission (FERC), the Federal Bureau of Investigation (FBI) and others as needed.

#### **Addressing Cybersecurity in the Electric Sector**

Protecting the nation's complex, interconnected network of generators, transmission lines, and distribution facilities that make up the electric power system, while ensuring a supply of reliable, secure and affordable electricity is a top priority for electric co-ops and other segments of the electric power industry.

The U.S. electric system was originally designed with a focus on safety, reliability and affordability. Today, there are new considerations for the electric system, including intentional physical- or cyber-attacks. Fortunately, our normal preparations to prevent damage from severe weather and equipment failure serve us well in limiting the potential impact of intentional actions. To protect against extreme weather events, vandalism and major equipment failure, a high level of redundancy is built into the power supply system. This includes multiple layers of protection to safeguard assets from cyber threats. The grid is designed to reliably meet the highest possible summer or winter load demand even when our most critical facilities are out of service. That is our industry standard. Because of this, our industry has withstood intentional attacks, such as the 2013 California substation and Arkansas transmission line attacks, with no loss of customer service, despite severe damage to our infrastructure. This approach to protecting critical assets is known as defense-in-depth.

The electric power industry continuously monitors the electric grid and responds to events large and small. Consumers are rarely aware of these events because of system resilience supported by effective planning, coordination and response/recovery efforts. In rare cases where an event does impact electric service, industry resilience and preparedness ensures service is promptly restored in most cases.

The possibility of a cybersecurity attack impacting grid operations is something for which the power sector has been preparing for years. These preparations include:

- Implementing security standards and technologies to protect systems,
- Forging close partnerships to identify threats and solutions, and to respond to incidents,
- Engaging in active information sharing about threats and vulnerabilities,
- Participating in industry and cross-sector disaster planning exercises such as DOE's Clear Path and the North American Electric Reliability Corporation's (NERC) GridEx biannual exercise, and
- Partnering with the DOE, the National Laboratories and other federal agencies on cybersecurity research to improve the tools and resources needed by industry to address cyber threats.

As threats and threat actors continue to evolve, so must the industry's capability to defend against them. Maintaining the resilience and security of the electric grid requires a flexible approach that draws on a variety of tools, resources and options.

Jim Matheson, CEO  
National Rural Electric Cooperative Association  
March 1, 2018 Testimony

Much of the public discourse around cyber- or physical- threats to the electric grid often focuses on far-fetched scenarios, sensationalized claims or misunderstandings of the bulk electric system (BES) function. Facilities that are part of the BES are considered to be the ones that could potentially impact the reliability of the nationwide flow of electricity. The scenarios most publicized are rarely reflective of the real threat environment, and disproportionately emphasize the highest consequence scenarios that are the least likely to occur. Many of the more dramatic scenarios would constitute acts of war on the United States and would directly impact more than just the electric sector. In addition, these scenarios do not always take into account our expertise and planning to ensure reliable and resilient electricity delivery.

That is not to say there are not legitimate threats to the grid. They exist. Rather than being reactive or fearful, the electric sector considers the entire threat landscape to ensure grid operations meet high reliability standards. The electric power industry continuously monitors the bulk electric system and responds to events large and small. Consumers are rarely aware of these events, primarily because of the sector's planning and coordinated response to manage these threats. In the cases where an event impacts the consumer, these same activities, in addition to the decades of lessons learned from supplying power, have helped ensure there are hazard recovery plans in place for working within the sector and with government partners to get the power back on.

Defense in depth and system redundancies are helping electric utilities keep the grid reliable and secure. This approach will continue to be our first and best defense to any event.

#### **Mandatory and Enforceable Standards**

To maintain and improve upon the high level of reliability consumers expect, electric cooperatives work closely with the rest of the electric industry, the North American Electric Reliability Corporation (NERC), DHS, DOE and FERC on matters of critical infrastructure protection, including sharing needed information about potential threats and vulnerabilities related to the bulk electric system. FERC delegated authority from the Energy Policy Act of 2005 to NERC, a private not-for-profit entity, to develop and enforce reliability and cybersecurity standards that protect the BES. The Electric sector today is the only one with mandatory and enforceable standards when it comes to cybersecurity.

Approximately 60 generation and transmission cooperatives and an equal number of distribution cooperatives must comply with some portion of NERC's reliability standards, based on the critical bulk electric system assets they own and operate. Since NERC reliability and cybersecurity standards became mandatory, electric cooperative representatives have participated in NERC standard development activities. Those cooperatives with compliance responsibilities have been working both to comply and demonstrate compliance through scheduled NERC audits. If covered entities are found to have violated cybersecurity and/or other NERC standards, they can be subjected to fines as high as \$1 million per day per violation. As the CEO for the association that represents America's electric cooperatives, I can tell you that compliance with the NERC standards is taken very seriously.

Jim Matheson, CEO  
National Rural Electric Cooperative Association  
March 1, 2018 Testimony

The NERC standards development process begins with input from industry experts. After approval by industry, the NERC Board of Trustees is asked to approve the standards which, if approved, are then submitted to FERC for approval. Upon FERC approval, the standards become mandatory and enforceable. The electric utility industry recently developed standards on physical security and geomagnetic disturbances (GMDs) and continues to revise and develop additional cybersecurity and GMD standards. Geomagnetic disturbances are initiated by events on the surface of the sun where masses of electrically charged particles of varying levels are hurled toward the Earth, creating the potential for ground-based disturbances due to their interaction with the Earth's magnetic field. When the particles interact with the Earth's magnetic field, especially in certain geographic regions, they can cause ground-induced currents (GIC) and other potentially disruptive phenomena.

NERC also has an "alert system" that provides the electric sector with timely and actionable information when a standard may not be the best method to address a particular event or topic.

#### **Cybersecurity for Electric Cooperatives**

Electric cooperatives with NERC compliance responsibilities are subject to scheduled NERC audits. Entities that can impact the BES, our national supply and transmission of electricity tend to have larger IT departments and therefore more resources at their disposal. Those who own or operate components of the BES like electric generation resources, transmission lines or interconnections with neighboring systems must be concerned about the operations technology (OT) used to support these assets. However, those who are not part of the BES still take cybersecurity very seriously, though often with more of an emphasis on the business or information technology (IT) platforms, which encompass employees, consumers, architecture, and sensitive data. Most states have laws enforcing data security that require compliance from all entities. NRECA is playing a leading role in nurturing a culture of cybersecurity with electric co-ops to help prepare for and respond to cybersecurity challenges – operations and business systems alike. Assessments, awareness, and training are key for helping these entities engage and protect their assets. NRECA's cybersecurity programs provide cybersecurity support and resources to our members at all levels – technical, regulatory, legislative, and legal. In fact, during our Annual Meeting and TechAdvantage event this week we had an opportunity to discuss cybersecurity with our membership and highlighted a number of efforts and resources available for electric cooperatives.

NRECA thanks DOE Secretary Perry and Assistant Secretary Walker for the partnership between the Office of Electricity Delivery and Energy Reliability and electric co-ops to protect our system against cyber threats. DOE provided funding to NRECA and the American Public Power Association to implement programs that will specifically help small- and mid-sized utilities improve their cyber and physical security capabilities. NRECA used this funding to create the Rural Cooperative Cybersecurity Capabilities Program (RC3), which assists cooperatives in advancing their cybersecurity posture. RC3 provides cybersecurity training, services and tools to help our members build stronger cybersecurity programs.

Jim Matheson, CEO  
 National Rural Electric Cooperative Association  
 March 1, 2018 Testimony

A major priority of the RC3 Program is developing a self-assessment maturity model to enable small- and mid-sized utilities to assess and benchmark their cybersecurity capabilities, and to build a culture of security within their organization. This effort builds on existing work using the DOE's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), a Risk Mitigation Guide NRECA developed with funding from the Office of Electricity in 2011, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. For the past year, NRECA has been field testing this maturity model in a Self-Assessment Research Program.

Cybersecurity is not just the responsibility of IT staff. All employees have the ability—and responsibility—to impact their organization's cybersecurity posture. The Self-Assessment Research Program works with the executive team of a cooperative and helps each member of that team take a hard look at where their cybersecurity efforts are strong and where they can be improved. Through this program, NRECA provides intensive two-day cybersecurity training and has used it to evaluate programs at 36 small- and mid-sized cooperatives in 13 states.

As NRECA continues our work with cooperatives, we are already seeing measureable progress. For example, we are documenting improvements in securing network access, strengthening physical security, and integrating cybersecurity awareness into negotiations with third-party vendors. With continued DOE support, NRECA is working to expand this program to more of our members.

In addition, the RC3 Program held six Cybersecurity Summits in 2017 that provided staff representing 151 cooperatives cybersecurity training. "Every presentation provided something I could take home to benefit our company," said one attendee. The most valuable aspect of the summits was the opportunity for co-ops to come together and discuss cybersecurity challenges and solutions. With continued support from DOE, NRECA will hold another round of Cybersecurity Summits this year.

#### **It Takes a Toolbox: Resources for Rural Electric Cooperatives**

When it comes to cybersecurity, a flexible toolbox with many different resources and options is necessary. There are no "silver bullets." For the electric sector, this includes, but is not limited to: standards, cyber assessment, guidance, tools and resources for small and medium entities, cyber mutual assistance programs, and a national industry playbook. Below is a summation of some of the cybersecurity resources available for rural electric cooperatives, either directly from government or through NRECA. Many of these have been alluded to earlier in the testimony.

**Tools and resources for small and medium entities:** In addition to the Self-Assessment Research Program and the Cybersecurity Summit Series, the RC3 Program is developing:

- cybersecurity training and guidance resources to assist co-op employees to understand their roles and their ability to help protect their cooperative;
- increased awareness of existing information sharing resources and opportunities; and

Jim Matheson, CEO  
National Rural Electric Cooperative Association  
March 1, 2018 Testimony

- new technologies to identify, prevent and/or mitigate cyber incidents.

Though the RC3 Program is specifically focused on developing resources for those utilities with limited resources, all of the resources developed through the RC3 Program will be available to all NRECA members.

**Examples of Cyber Assessments for Industry Broadly:** The industry has decades of experience working together to protect our shared infrastructure and is constantly reevaluating threats and taking steps to protect the system as well as plan for its recovery. One example is the ES-C2M2, developed by the Office of Electricity through a public-private partnership that supports the adoption of the NIST Cybersecurity Framework by assisting organizations to improve their cybersecurity capabilities. The Office of Electricity is in the process of updating the ES-C2M2, and NRECA will be involved in ensuring that this tool continues to meet the needs of electric cooperatives. The continued development of cybersecurity programs and tools, like the ES-C2M2—combined with access to actionable relevant information, both classified and unclassified—is vital to strengthening security postures in critical infrastructures.

**NRECA Guidance for Electric Cooperatives:** To further bolster the efforts of ES-C2M2 specifically for electric cooperatives, NRECA developed a “Guide to Developing a Cybersecurity and Risk Mitigation Plan,” which includes tools and processes cooperatives (and other utilities) can use today to strengthen their security posture and chart a path of continuous improvement. All co-ops participating in NRECA’s Regional Smart Grid Demonstration Project used these tools to develop a smart grid cybersecurity plan. The most recent version of the guide was published in 2014. This resource, developed by NRECA with funding from the Office of Electricity, is available to all utilities and is posted on DOE’s website

**Cyber Mutual Assistance programs:** Given the extensive experience they have responding to storms and natural disasters, electric cooperatives have an effective approach to emergency management and disaster recovery. Following a disaster, cooperatives rapidly deploy crews and equipment to impacted areas to assist other cooperatives with the restoration of power. The foundation of this program is a standard Mutual Assistance Agreement, signed by the vast majority of NRECA member electric cooperatives. Cooperatives help each other and other electric utilities as needed. Individual co-ops typically coordinate mutual assistance efforts through their statewide organizations, which lead efforts to identify in-state and cross-state needs and resources. This culture of mutual assistance can be found across the electric sector and is being applied to the implementation of the ESCC’s recommendation for the formation of a Cyber Mutual Assistance (CMA) program, a natural extension of the electric power industry’s longstanding approach of sharing critical personnel and equipment when responding to emergencies. The CMA program has 141 members, including 35 cooperatives, participating—covering more than 80% of all U.S. electricity customers.

**ESCC Playbook:** Most events impacting electric power supply tend to impact a community or a region – not the bulk power system as a whole. However, planning for response and recovery at a national level for widespread events is necessary in a world where terrorists and nation states may target elements of our critical infrastructure. By coordinating with the government and providing mutual assistance to address cyber threats, the electric power industry

Jim Matheson, CEO  
National Rural Electric Cooperative Association  
March 1, 2018 Testimony

is greatly enhancing our nation's ability to protect against and recover from threats to our systems. The ESCC Playbook provides a framework for senior industry and government executives to coordinate response and recovery efforts and communicating to the public when such a situation arises. The playbook is an evergreen document that can be updated by industry when lessons are learned from an exercise or real-world experiences.

It is important to note that with a national level event, while our society depends on electricity to function; our electricity systems are reliant on other systems, including transportation systems for our fuel, water systems for cooling, and telecommunications for operations. When dealing with national events, coordination across all these systems is imperative.

#### **Importance of Partnerships & Information Sharing**

As mentioned earlier, the ESCC serves a vital role by providing the venue for the sector to work with government to coordinate policy-level efforts to prevent, prepare for, and respond to national-level incidents affecting critical infrastructure. The major trade associations and industry work together with government to improve cybersecurity through the ESCC.

These efforts by industry CEOs from all segments of the electric sector and their government counterparts include: planning and exercising coordinated responses, ensuring that information about threats is communicated quickly among government and industry stakeholders, and deploying government technologies on utility systems that improve situational awareness of threats.

In addition to industry and government collaboration throughout the year, the ESCC serves in an advisory role with the Electricity Information Sharing and Analysis Center (E-ISAC). The E-ISAC collects and promptly disseminates threat indicators, analyses and warnings from a variety of private sector and government resources to assist electric sector participants in taking protective action. The information is managed confidentially and distributed through the NERC secure internet portal directly to electric industry asset owners and operators.

The E-ISAC also manages the Cybersecurity Risk Information Sharing Program (CRISP), a public-private partnership co-funded by DOE and industry that facilitates the timely bidirectional sharing of actionable unclassified and classified threat information, using advanced collection, analysis, and dissemination tools to identify threat patterns and trends across the electric power industry with near real-time exchange of machine to machine information. This is an excellent example of efforts to bridge the divides between the classified realm and sharing actionable, relevant information with private industry.

We appreciate the continued efforts of the administration in coordinating with the ESCC and we stand ready to continue our work with government counterparts to ensure a secure, reliable and resilient grid.

Jim Matheson, CEO  
 National Rural Electric Cooperative Association  
 March 1, 2018 Testimony

Additionally, NRECA and our members look forward to working with the leadership and staff that will be assigned to the recently announced DOE Office of Cybersecurity, Energy Security and Emergency Response.

#### **How Congress Can Continue to Help**

In the previous Congress, several pieces of legislation were passed that assist efforts in securing the grid. Congress passed the Consolidated Appropriations Act of 2016 (P.L. 114-113), which included long-sought legislation to promote robust, multidirectional voluntary information-sharing about cybersecurity threats between and among federal agencies and critical infrastructures, including the electric utility industry. This legislation provided additional confidence in sharing information safely through existing channels, such as the E-ISAC, between the federal government and private sector. Congress also enacted into law the Fixing America's Surface Transportation (FAST) Act (P.L. 114-94), which included these provisions:

- Clarification of roles and authorities when there is an imminent threat to the bulk power system, as well as identifying DOE as the official lead Sector-Specific Agency (SSA) for cybersecurity for the energy sector. DOE was already the SSA for the sector, but this was appropriately clarified to include cyber issues; and
- Freedom of Information Act exemptions for "critical electric infrastructure information" submitted by industry to FERC and other federal agencies.

Congress should recognize that the electric utility industry is the only one with mandatory and enforceable cybersecurity standards. As such, we ask that lawmakers keep this in mind when considering broad cybersecurity proposals to ensure that they do not conflict with existing standards within our industry. With that being said, here are some areas for how Congress can and should help:

1. **Information Sharing:** One of the best examples of how government can improve its information sharing with industry is the December 2015 Ukraine cyber breach. While the content of the classified and unclassified information from our government was helpful, the timeliness of getting specific, actionable information to industry after an event must be improved so that electric utilities can respond as quickly as possible. In addition, assurances that sensitive information shared from industry to government is properly protected and free of liability concerns when shared in good faith would improve the information-sharing environment.
2. **Insider Threats:** The owners and operators of critical infrastructure understand that the most significant threats tend to be those that are hardest to identify – including the insider threat. We urge Congress to consider legislation giving the FBI the statutory authority to assist industry on a voluntary basis in performing enhanced background checks for terrorist activity for industry-determined personnel that perform critical functions. This would assist industry in further mitigating risks in a way we cannot accomplish at the local and state levels.

Jim Matheson, CEO  
 National Rural Electric Cooperative Association  
 March 1, 2018 Testimony

3. **Continue Assistance for Small and Medium Utilities:** A one-size-fits-all cybersecurity strategy simply does not work in the electric sector. For example, security issues relevant for an entity on the BES may be very different from another BES entity due to geography, engineering architecture and redundancies. Similarly, security issues relevant for the BES are not necessarily the same as issues facing the local distribution system. As such, Congress should protect funding for DOE's "Improving the Cyber and Physical Security Posture of the Electric Sector" initiative, which supports NRECA's RC3 Program and is funded by the Office of Electricity Delivery and Energy Reliability's Cybersecurity for Energy Delivery Systems program (CEDS). This is the only program where DOE and NRECA are specifically focused on addressing the unique cybersecurity needs of small- and mid-sized distribution utilities. The RC3 Program emphasizes collaboration and personalized training and is helping distribution cooperatives build stronger cybersecurity programs.
4. **Supply Chain:** The language of the SAFETY Act of 2002 and the accompanying rule always have made clear that protections under the law apply to cyber events and would apply regardless of whether a terrorist group conducted such an attack. In practice, there has been some hesitancy on the part of industry to utilize the SAFETY Act to protect against federal claims arising from cyber attacks due to the requirement that the attack be deemed an "act of terrorism" by the Secretary of Homeland Security before liability protections become available. Senator Daines' legislation—S. 2392, the Cyber Support for Anti-Terrorism by Fostering Effective Technologies Act of 2018 (Cyber SAFETY Act)—would explicitly allow for the liability protections of the SAFETY Act to become available when the Secretary deems that an act of terrorism or a "qualifying cyber incident" has occurred. Without the need to link a cyberattack to an "act of terrorism," more companies would take advantage of the SAFETY Act program, thereby fulfilling the law's original intent of promoting the widespread deployment of products and services that mitigate malicious events, including those related to cybersecurity.
5. **Continued Support for Cybersecurity Research and Development:** Fundamental research is needed within the electricity sector to develop the tools and technology necessary to strengthen our cybersecurity posture and ensure the ability to rapidly recover from a cyber incident. NRECA works collaboratively with the DOE's Office of Electricity on many research projects, electric cooperatives partner with the DOE's National Laboratories to advance research efforts, and NRECA and our members provide industry input into the department's research priorities. NRECA is an active member supporting the Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS) research consortium, an initiative located at the University of Arkansas and supported by the Office of Electricity. Without a strong research and development program, many industry vendors will not be able to keep pace in developing solutions to address the rapidly changing cybersecurity threats that our industry faces.

#### Conclusion

Thank you for holding today's hearing on this very important issue. I am proud of the efforts electric cooperatives and the broader electric sector make to continually improve our

Jim Matheson, CEO  
National Rural Electric Cooperative Association  
March 1, 2018 Testimony

cybersecurity posture. Even though our sector is comprised of various business models, we work together to secure our nation's reliable electricity supply. I hope that my testimony provides the Committee insight regarding a few of the many activities and collaborative efforts among electric cooperatives and the broader industry and our federal government partners. We share your goal of protecting this nation's critical infrastructure from cyber threats and appreciate your efforts to address this important national security issue.

Electric cooperatives believe building and investing in partnerships is vital as the industry navigates this dynamic environment. We are implementing a coordinated and collaborative effort across the electricity sector to respond to threats and to vigilantly modify our security tactics as needed to keep pace with these threats.

The CHAIRMAN. Thank you, Congressman Matheson.  
Dr. Endicott-Popovsky, welcome.

**STATEMENT OF DR. BARBARA ENDICOTT-POPOVSKY, EXECUTIVE DIRECTOR, CENTER FOR INFORMATION ASSURANCE AND CYBERSECURITY, UNIVERSITY OF WASHINGTON**

Dr. ENDICOTT-POPOVSKY. Thank you.

Good morning, Chairman Murkowski and Ranking Member Maria Cantwell and distinguished members of the Committee. I want to thank you for the opportunity to speak with you today about examining cybersecurity in our nation's critical energy infrastructure.

My name is Dr. Barbara Endicott-Popovsky. I'm the Executive Director of the Center for Information Assurance and Cybersecurity at the University of Washington, and we are an NSA Center of Academic Excellence in cybersecurity as well as a regional resource center for dissemination of best practices. We convene industry, government and military around shared problems, but to provide context for my remarks, we're driven by four major ideas.

First of all, in cyberspace everyone is your neighbor. This is going to require new ways of thinking about partnerships with military, industry and government.

Secondly, cybersecurity involves rules and tools. While it came from technology, there are still humans in the system and there's no firewall for stupid. So, it's going to require policies, procedures, awareness training that's going to really deal with that human element.

Thirdly, all of this is exacerbated by not enough talent. And I can't emphasize that enough. This is a systemic problem, and it is not going to be fixed with a Band-Aid. This is going to be equivalent to the moon shot project that we had back in the Kennedy era. Now, we were able to do it back then. We should be able to pull the resources together to do it now, but this is a serious problem.

And besides that, cybersecurity is becoming a profession and I want to caution the Committee about balkanizing the field with its own definitions and its own educational procedures. There are differences, infrastructure to infrastructure, yes.

I would refer the Committee to work that was done by the FCC CSRIC that was designed to look at how they could leverage existing NIST and NSA, DHS, work that's been done on cybersecurity educational standards and I think you'll find that much is already there, but there will be a delta.

How did we get here? Certainly, cyberattacks are daunting. We're living through digital transformation. That's what's going on. And we're still clinging to mental models from the physical world and the information world that simply don't work. Cross sector collaboration, for example, is something we talk about, but it's not easily done because all sectors have their own missions. It's very difficult to get everyone on the same page.

However, there's one thing we can all agree on. There is no cyber fire department. There is no cyber 911. In a cyber disaster the DoD is prepared to protect its own networks and maintain its mission, but who is there on the civilian side and the private sector side? No one.

This vacuum is a national security threat. And toward this end H.R. 3712 has been proposed by our delegation that deals with proliferating the Cyber Civil Support teams across the country which is going to require extensive education of the National Guard so that they're prepared to do what's necessary in the event of an attack.

The case of cyber war is a case of mutually assured destruction. Make no mistake. At some point, we're going to need the equivalent of the Kennedy and Khrushchev red phone and nuclear disarmament talks, but getting everybody to agree on enforcement is going to be a problem and I'm not sure that nation-states right now have an appetite for stepping up to the table. But this will have to happen so we don't mistake each other. This is a tragedy of the commons where a shared resource is used individually by users to the detriment of the whole and to the ruination, perhaps, of the whole.

In addressing the talent deficit, this is a problem across all sectors and, in particular, with utilities. We need to be mindful that industry is competing for the same talent and their salaries are much higher. So I suggest that we consider ways to incentivize students to go to work for utilities through, perhaps, funded scholarship programs. The bottom line, again, is that this is no easy fix. This is no Band-Aid. We need commitment over the long haul to really develop what's necessary to transform our educational processes so that we prepare people adequately and quickly to do what's necessary to protect our vital infrastructure.

Thank you.

[The prepared statement of Dr. Endicott-Popovsky follows:]

**Written Testimony of  
Dr. Barbara Endicott-Popovsky**

Executive Director, Center for Information Assurance and  
Cybersecurity  
University of Washington

**Full Committee Hearing to:  
Examine Cybersecurity in our Nation's Critical Energy  
Infrastructure**

before the United States  
Senate Committee on Energy and Natural Resources

March 1, 2018

Good morning, Chairman Murkowski and Ranking Member Cantwell, and distinguished Members of the Committee. Thank you for the opportunity to speak with you today about examining cybersecurity in our Nation's critical energy infrastructure, specifically about the public and private interplay in protecting the grid. My name is Dr. Barbara Endicott-Popovsky, and I am the Executive Director of the Center for Information Assurance and Cybersecurity (CIAC) at the University of Washington. Founded in 2004, CIAC is an NSA/DHS designated Center of Academic Excellence in Cybersecurity Defense Education and Research and an NSA CAE Regional Resource Center named to disseminate best practices in cybersecurity education and to mentor other colleges and universities. We convene industry, government and military around shared problems.

**CYBERSECURITY CONTEXT**

To provide context, four big facts about cybersecurity drive our work and our views on cybersecurity:

- 1) ***In cyberspace, EVERYONE is our neighbor.***  
This requires new deeper relationships between the military, government, industry, and citizens.



3) **Not enough talent**

There is a systemic shortage of well-trained talent (and of qualified teachers)

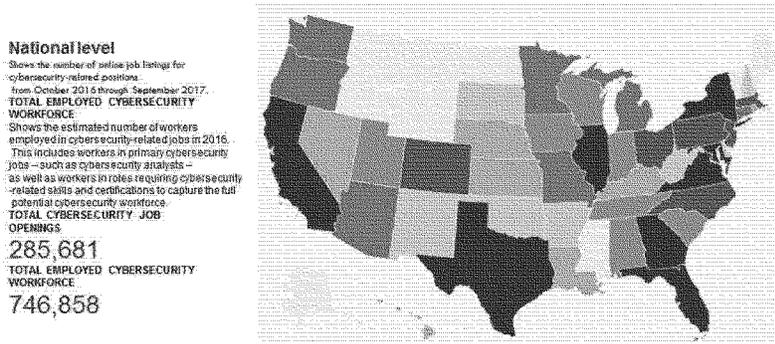
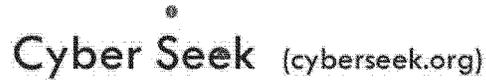


Figure 3: Operational environment for managing cybersecurity

4) **Cybersecurity is becoming a profession**

It's not one thing--32 separate career paths have already been identified.

**The National Initiative for Cybersecurity Education (NICE)  
Cybersecurity Workforce Framework**  
NIST Special Publication 800-181

**FRAMEWORK**

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. The NICE Framework supports thoughtful organizational and sector communication for cybersecurity education, training, and workforce development.

**DEVELOPMENT PROCESS**

The National Initiative for Cybersecurity Education (NICE) Framework progresses communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or work that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

1. Conducted initial research and analysis, including identifying job tasks and analysis, and identifying the government entities to work with on this project.
2. Conducted focus groups with current federal agencies (effort to identify user-defined specialty areas not noted in previous sections of the Framework (i.e., Cybersecurity Management and Language Analysis).
3. Conducted focus groups to shape categories, specialty areas, and work role definitions and also identified tasks and KSAs for each work role.
4. Identified tasks and associated KSAs for each work role.
5. Revised Framework as necessary through workshops, meetings, and stakeholder input (ongoing).

**2. Reflected existing distribution of cybersecurity specialty areas based on sector**

**3. Conducted focus groups with current federal agencies (effort to identify user-defined specialty areas not noted in previous sections of the Framework (i.e., Cybersecurity Management and Language Analysis)).**

**4. Conducted focus groups to shape categories, specialty areas, and work role definitions and also identified tasks and KSAs for each work role.**

**5. Identified tasks and associated KSAs for each work role.**

**6. Revised Framework as necessary through workshops, meetings, and stakeholder input (ongoing).**

**CYBERSECURITY WORK CATEGORIES**

Category 1	Category 2	Category 3	Category 4	Category 5	Category 6	Category 7	Category 8
------------	------------	------------	------------	------------	------------	------------	------------

**CONTACT:**  
The NICE Framework  
NICE@nist.gov

**WHAT IS THE CYBERSECURITY WORKFORCE?**

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

**CATEGORIES:** A high-level grouping of common cybersecurity functions.

**SPECIALTY AREAS:** Represent an area of concentrated work, or function, within cybersecurity and related work.

**WORK ROLES:** The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role.

**TASKS:** Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles.

**KSAs:** Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.

**BUILDING BLOCKS FOR A CAPABLE AND READY CYBERSECURITY WORKFORCE**

The NICE Framework provides employers, current and future cybersecurity workers, training and certification providers, education providers, and technology providers with a national standard for organizing the way we define and talk about cybersecurity work, and what is required to do that work.

**NIST**  
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Figure 4: NICE framework standardizing cybersecurity workforce specialties

<https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

## CYBERATTACKS: HOW DID WE GET HERE?

At least weekly we hear about significant data breaches or cyberattacks that threaten the financial health and privacy of millions of online users, or describe attacks by nation states or terrorist groups with a political or propagandistic agenda. To the citizen observer, it must appear that those responsible for managing networks are helpless to do anything about rising online crime and threats. To a certain extent that assumption is true. We will never have 100% secure systems. Technologies

alone won't fix things. Users assume a certain amount of risk online. Many just don't realize it. The idea shatters our comfortable sense of security we've developed over decades of experiencing reliable infrastructure. It's no wonder the public is disturbed by what they are reading in the news. There is no cyber 911 we can call if things don't work.

How did we get here? How did our online interconnectedness, that has created so many benefits, resulted in so many challenges? Have we been so enamored of creating the next new digital device or online service that we didn't take time to consider the unintended consequences that we've introduced into our lives?

We're living through digital transformation that's challenging how we think and breaching the silos that used to organize our lives and our thinking. We have been clinging to mental models from the physical world and the industrial age that blind us to the changes around us. The embrace of technology is moving so fast, it's difficult to keep up with the unintended consequences of what this has done to our daily reality and how society as a whole functions.

In one sense, we are rapidly smashing our Industrial Age mental models where organizations are structured in hierarchies, knowledge is structured by discipline, our work is in discrete silos—departments and sectors: military, government, industry, academia—replacing it with interconnectedness that, as a by-product, also enables online fraud, online voting scams, illegal downloads, and continuing threats to network security. But who saw this coming? Like Mickey Mouse as the Sorcerer's Apprentice in *Fantasia*, we have assumed the wizard's powers without anticipating the risks! What was meant for good has ushered in unexpected problems. The Internet has brought convenience, savings, and

productivity, but it also has created troubling dislocations that we didn't anticipate.

## **NEW MENTAL MODELS NEEDED**

### **1. Cross Sector Collaboration: Public Private Partnerships**

Civilians are used to calling 911 for emergencies of all kinds, but who do you call in the event of a major cyber outage? There are no cyber fire departments. The DoD is prepared to defend their own networks to support their missions, but who will step in on the civilian and private sector sides to restore power, to assist with maintaining our communities? There is no one. This vacuum is a national security threat.

In Washington State we've benefited from a National Guard whose leadership, coming from the tech industries, have created cyber civil support teams that assist government agencies and utilities to assess their vulnerabilities through penetration test exercises.

Working across civilian and military boundaries is not so easy, given the legal authorities issues that arise. Their lessons learned about how to manage crossing authorities in nanoseconds is preparing organizations locally and could be disseminated across the country for maximum preparedness.

Public and private, we have two very different missions: the mission of the military is to protect the Homeland, and the mission of private sector to innovate and maintain profitability for the Board and shareholders. Blending missions is not an easy task, but the time has come where the cost of not integrating resources significantly outweighs the

benefits of maintaining independent response plans. This is especially true given the workforce shortage of cyber specialists.

One very important nexus between these missions – public, private, federal, military – is the primary role of providing life safety. Profitability becomes secondary to protecting critical infrastructure. A unifying component is the legal obligation that critical infrastructure partners have to maintain continuity of operations. Two recent studies on this topic are: the 2017 Rand “Cyber Power Potential of the Army Reserve Component” and the 2017 PNNL report on Public/Private/Civilian/Local/Federal partnerships (draft only). These reports create an excellent case for greater training, but they need a framework to operationalize the teams necessary for comprehensive cyber response. Critical infrastructure private sector partners have an opportunity to leverage the work of the Guard to increase their surge capacity through efforts to expand the existing cyber civil support teams to include the Cyber mission. One of the most impactful contributions that could come from private sector critical infrastructure cyber response and threat intelligence teams would be the coordination of credentialing, training, and funding of area command centers to respond to a cyber disaster.

For this reason, Rep Kilmer from Washington State has joined with colleagues in the House to propose proliferation of cyber civil support teams across the country through all National Guard, modeled after the work being done by the Washington National Guard. Appendix 2 and 2b provide insight.

## **2) Cyberwar: A New Case of Mutually Assured Destruction**

In this country we have had the luxury of two oceans on either side, left and right, with two ‘soft’ countries above and below us that are basically

cooperative and 'like us.' This can inure us to what we have done by becoming virtual next door neighbors with all of our friends online. I'm fond of telling my students that my mother named six kids that I was absolutely to avoid like the plague when I was growing up. I still remember the name of the boy at the top of the list. These were perennial trouble-makers in the neighborhood; if you hung around them, you were assured of no-good. (I can attest to it, having smashed a church window, by accident, playing softball with a couple of them!) Now we are side-by-side with cultures and countries radically different from our own, with very different world views about IP (Intellectual Property), freedom, ethics, etc. Why do we expect them to behave like us? They don't and they won't,

At some point we will need, for cyberspace, 1) the equivalent of the Kennedy/Khrushchev era 'red phone' to ensure we don't misread each other's online actions and 2) the equivalent of nuclear disarmament talks to define the rules and tools of acceptable online activities for civil societies. There is no doubt in my mind that cyberwarfare can be as deadly as nuclear war and result in mutually assured destruction, as Admiral Rogers testified this week.

### **3) Tragedy of the Commons**

This is a case of 'tragedy of the commons,' in which a shared-resource, the Internet, is accessed by users who act independently according to their own self-interest, behaving contrary to the common good, thus spoiling that resource for all. Many users have placed reliance on that resource and will be lost without it.

Again this argues for agreed to behavior standards for all, but there would need to be a means of enforcement. This has not proven easy in the case of individuals and in the case of nation states there seems to be no appetite. We are left, perhaps, with the need for a catastrophic failure before a solution can be developed. I don't see a solution in my lifetime. I do see a need for thoughtful interim behaviors on the part of all users, individually, during this interesting period while we shed the industrial age infrastructures we grew up with for something as yet to be developed.

## **TALENT DEFICIT**

To deal with all of this change and its significance and impacts, we have a huge deficit in talent to handle the cyber problems we face. The lack of talent in the field of cybersecurity is keenly felt across all sectors of the economy—industry, government, military, the academy. While cybersecurity education has been called a national priority by some, there still are hundreds of thousands of cybersecurity jobs going unfilled, and the gap will take a long time to close.<sup>1</sup> Of further concern, we have gathered anecdotal evidence that employers in both government and industry consider many recent cybersecurity graduates woefully unprepared for the realities of the workplace, taking too long to become effective. For that reason, CIAC has adopted an approach to address both the supply and preparedness problems, with the application of a lightweight cooperative learning model—designed specifically to develop and graduate 'breach-ready' cybersecurity professionals.

---

<sup>1</sup> [cyberseek.org] and this is just the US view. There is a deficit worldwide that at least doubles their numbers.



Figure 5: Cybersecurity Cooperative Learning Model

Because imposing a cooperative learning structure (such as European countries have, or a few universities in the United States and Canada, where a year of work interleaves a year of school) would be costly and disruptive to most academic institutions, CIAC devised a cybersecurity cooperative learning pilot where students maintain their current academic load in the last year of their degree programs and, in addition, opt into an integrated program of professional instruction and half-time industry employment. The additional professional education includes: 1) an information security and risk management certificate that covers all the necessary knowledge units required to meet NSA/DHS/NIST standards and 2) a professional seminar conducted in partnership with industry to help students triage their work experience with what they've learned formally in the classroom. The addition of the professional seminar and certificate elements in the pilot accelerate student readiness for work when they formally graduate, based on employer and student data collected.

T-Mobile served as our initial industry partner and collaborator in developing this cooperative learning program. In addition to their support, government is also a partner. The National Information Assurance Education and Training Program (NIETP) is interested in the dissemination of the cooperative learning model and the lessons learned during the pilot period. This is conceived as a two-year pilot. This first year 10 students, constituting one cohort, were engaged with one employer. Students were selected based on technical foundation, interpersonal skills, team participation, and collaborative problem-solving abilities. Certificate scholarships were provided. A second year of the pilot is currently being conducted with more industry partners for the purposes of incorporating lessons learned from the first year and refining and generalizing the model.

In the second year, data collected will provide insight into several questions: 1) /how this program will be scaled, 2) how and to what degree this kind of a program accelerates cybersecurity job readiness, 3) what are best practices for conducting such a program.

## **PROFESSIONALIZATION OF CYBERSECURITY: STANDARDS**

Cybersecurity is and must professionalize. The Manning and Snowden incidents argue for professional standards of behavior and selection, like we see in other professions (medicine, dentistry, law, etc.) We also see education standards taking hold with more NSA CAE's adopting the curricular standards laid out by NIST/NSA/DHS and the emergence of ACM guidelines and ABET accreditation on the technical side.

We've also seen one of the infrastructure sectors, telecommunications,

become the first to step up to exploring whether or not new or additional educational standards need to be created for cybersecurity specific to that sector. Telecommunications supports virtually all of our critical infrastructure. For this reason, CIAC joined the Communications Security, Reliability and Interoperability Council (CSRIC), led by T-Mobile, to address this and other workforce issues specific to telecommunications cybersecurity professionals.

We learned that much of the existing work by NIST, NSA, DHS on workforce development, work roles, education standards, etc., could be leveraged by the telecommunications sector and we posit by other critical infrastructures, as well, saving time and resources. For this reason, CSRIC findings are located in an appendix to this testimony for the committee's reference in the hopes that these findings could be informative.

Please note that we will need specific incentives for students to work in critical infrastructure cybersecurity. Critical Infrastructure is competing with industry for the same scarce talent pool and they can be salaries that are much higher. For that reason, CSRIC recommended a scholarship for service program for critical infrastructure.

#### **ANOTHER MOON SHOT PROJECT**

With commitment to truly solve the cybersecurity talent problem systematically, and provide the stable, steady funding that that would imply, it will require the kind of effort that turned the education system around during the project to put a man on the moon. It took 10 years, but we did it.

## **ACKNOWLEDGEMENTS**

I wish to acknowledge the following organizations and individuals—representing military, industry and government respectively—for their contributions to the appendices that follow: The Washington National Guard led by Col. Gent Welsh, the Communications Security, Reliability and Interoperability Council (CSRIC) led by Bill Boii, Senior VP, T-Mobile, and the National Initiative for Education and Training Program (NIETP) at NSA led by Chief Lynne Clark.

These are offered for your further research efforts. More material is available upon request.

## APPENDIX 1 (pp 14-17)

### EXAMPLE INDUSTRY COLLABORATION

**Communications Security, Reliability and Interoperability Council (CSRIC) final report recommendations** (Executive Summary below) apply equally to other critical infrastructure like the energy sector and could be leveraged to accelerate workforce development initiatives therein. University of Washington CIAC collaborated with the T-Mobile on this project. The full report is available on request.

*Courtesy Bill Boni, Sr.VP T-Mobile*

---

March 2017 WORKING GROUP 7 Cybersecurity Workforce  
 Communications Security, Reliability and Interoperability Council (CSRIC)  
 Final Report –  
 Cybersecurity Workforce Development Best Practices Recommendations

Bill Boni (Co-Chair)  
 Drew Morin (Co-Chair)  
 Bill Newhouse

T-Mobile  
 T-Mobile  
 NICE Program Office at NIST

### **Executive Summary (excerpted)**

The mission of the Communications Security, Reliability and Interoperability Council (CSRIC or Council) is to provide recommendations to the Federal Communications Commission (FCC) to ensure, among other things, optimal security and reliability of communications systems.<sup>4</sup>

Furthermore, the Council's recommendations specifically address the prevention and remediation of detrimental cyber events. Working Group 7 of the CSRIC V is specifically chartered to provide recommendations for the

CSRIC's consideration regarding any actions the FCC should take to promote improvements in cybersecurity workforce development. 5

The CSRIC V Working Group 7 was tasked to examine and develop recommendations for the CSRIC's consideration regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field.

Specifically, this working group leveraged existing work in this context to enhance the volume and quality of the workforce, including 6:

- (1) **demonstrating the application of the National Cybersecurity Workforce Framework (NCWF)** to the common and specialized work roles within the communications sector;
- (2) **identifying any gaps or improvements in the NCWF** for evolving work roles or skill sets that should be included in sector members' workforce planning; and
- (3) **identifying, developing, and recommending best practices and implementation thereof** to mitigate insider threats, including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities within the communications sector and particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. In this respect, the working group should consider means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

In order to manage the scale of the task, Working Group 7 chose to segment the information gathering and analysis process with targeted findings specific to each segment. We then identified best practices based on our analysis for each segment for consideration. This Final Report presents those Best Practices deemed to be most appropriate and impactful for consideration by the CSRIC V as recommendations to the FCC and the Communications Industry as a whole.

The National Cybersecurity Workforce Framework (NCWF)<sup>7</sup> provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Competencies, and KSAs.

1. **Categories** are common major functions regardless of job titles or other occupational terms.
2. **Specialty Areas** are common types of cybersecurity work which are grouped with similar areas under a specific Category.
3. **Competencies** are areas of expertise required for the successful performance of a job function; these are defined in the framework through the association of specific KSAs.
4. **Knowledge, Skills and Abilities (KSAs)** are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training experience, education, or training.

Working Group 7 (WG7) leveraged the prior NCWF analysis and process completed by the Financial Sector as a best practice to accelerate our task of evaluating the NCWF. The summary conclusions are that the NCWF is a viable, flexible framework that can and should be applied to the Communications Sector for Cybersecurity Workforce Development Planning. Building on this finding by the Working Group members, we proceeded to complete the initial evaluation of the “building blocks” – Categories, Specialty Areas, Competencies, and KSAs – for gaps and improvements that should be included in the application of this dataset to the Communications Sector. Our work product is attached to this Final Report as Appendices 1 and 2. It was also delivered to the FCC as a working database in Microsoft Excel format for unrestricted use.

We recognize that cybersecurity workforce development is undergoing rapid change and evolution.

This Final Report provides a lexicon that can be used to articulate the specific Workforce needs of the Communications Sector for roles involving cybersecurity. However, it is a static dataset and needs to evolve as the NCWF matures and Cybersecurity Workforce Development Planning gains maturity in our respective organizations. As part of the Final Report, WG7 provides specific recommendations for consideration by CSRIC on a process for adaptation and improvement of the sector specific dataset.

## Recommendations

The CSRIC V Working group 7 was tasked to examine and develop recommendations...to improve the security of the nation’s critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. Workforce

Development is not about filling job openings, although that is a source of metrics often used to represent the scale of the challenge. Instead, we chose to base our approach on the simple adage – a rising tide raises all boats. This led us to focus on the following broad based recommendations that would expand the available pipeline of skilled candidates for our industry as a whole.

- 6.1 The FCC Should Support a Process for the Communications Industry to Cooperatively Support Updates to the NICE Cybersecurity Workforce Framework (NCWF)*
- 6.2 Communications Industry can Benefit by Growing Awareness of and Supporting Programs Encouraging K-12 Youth to Study Cybersecurity*
- 6.3 The FCC Should Encourage Communications Industry Development of Cooperative Work-Study Program Partnerships*
- 6.4 The FCC should engage with the Communications Industry to Develop or Expand Scholarship for Service Programs in Industry*
- 6.5 The FCC Should Encourage Communications Industry Cybersecurity Professionals to Help Train the Next Generation*
- 6.6 The FCC Should Encourage the Communications Industry to Participate in the Development of Curriculum Guidelines by the Joint Task Force on Cybersecurity Education*
- 6.7 FCC Should Partner with Communications Industry, Public Safety, and Federal GenCyber to Develop a Cybersecurity Distance Learning Program for Public Safety and Rural Communities*
- 6.8 The Communications Industry Should Support Innovative Cybersecurity Workforce Development Initiatives such as the CyberBlue Program Support to Engage Populations with Disabilities*
- 6.9 Communications Industry Cybersecurity Experts Should Join the National Initiative for Cybersecurity Education (NICE) Working Group or One of its Subgroups*

<sup>3</sup> In November, NIST released for comment an update in partnership between NICE and DHS that changes the nomenclature back to the NICE Cybersecurity Workforce Framework

<sup>4</sup> Charter of the FCC's Communications Security, Reliability and Interoperability Council

<sup>5</sup> CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016

<sup>6</sup> The FCC CSRIC Working Group Description references the NICE CWF; Working Group

<sup>7</sup> has opted to refer to this framework using the April 2014 NICCS designation of the National Cybersecurity Workforce Framework (NCWF) for external consistency

## APPENDIX 2A (pp 18-20)

### EXAMPLE MILITARY COLLABORATION

#### **Major General Tim Lowenberg National Guard**

**Cyber Defenders Act** proposed by Rep. Kilmer to create National Guard Cyber Civil Support Teams.

There are no cyber ‘fire departments’ for civilians to call in the event of a major cyberattack. University of Washington CIAC collaborates with the Guard in cyber preparedness projects.

*Courtesy Col. Gent Welsh, USAF194 WG (US)*

---

### **H.R. 3712 – Major General Tim Lowenberg National Guard Cyber Defenders Act**

**Rep. Derek Kilmer (D-WA) & Rep. Steven Palazzo (R-MS)**

**Cosponsors [19D, 14R]:** Bishop (UT), Bordallo (GU), Brady (PA), Brooks (IN), Carson (IN), Cole (OK), DelBene (WA), Esty (CT), Fortenberry (NE), Gallego (AZ), Graves (GA), Heck (WA), Herrera Beutler (WA), Himes (CT), Jayapal (WA), Jones (NC), Kihuen (NV), Kind (WI), Krishnamoorthi (IL), Larsen (WA), Love (UT), McMorris Rodgers (WA), Mullin (OK), Newhouse (WA), O’Halleran (AZ), Pocan (WI), Reichert (WA), Rice (NY), Rosen (NV), Scott (GA), Shea-Porter (NH), and Visclosky (IN).

**Endorsed:** The National Guard Association of the U.S. & the Enlisted Association of the National Guard of the U.S.

**The Issue:** *“America’s response to the challenges and opportunities of the cyber era will determine our future prosperity and security.”* -2018 National Security Strategy

**The Threat:** In December 2017, hackers remotely controlled an industrial safety control system, the first-ever reported successful attack on safety devices widely-used across U.S. energy, chemical, and utility industries. This hack is just the latest in a growing number of cyber-attacks exposing the gap between the authority of federal cybersecurity forces and the needs of states, tribes, municipalities, and private industry. The 2018 National Military Strategy identifies the cyber domain as the tool of choice for state and malicious non-state actors to use as a weapon of mass disruption.

**The Problem:** Most of the Nation’s critical infrastructure is non-federal, which means existing federal cyber efforts leave states, tribes, and municipalities, as well as private industry, to fend for themselves.

**The Strategy:** The 2018 National Security Strategy promises to work with our critical infrastructure partners to assess their informational needs and to reduce the barriers to information sharing, and to expand collaboration with the private sector so that we can better detect and attribute attacks (Page 13).

“We will work with the Congress to address the challenges that continue to hinder timely intelligence and information sharing, planning and operations, and the development of necessary cyber tools” (Page 32).

**The Proposal:** This bill seeks to improve our nation’s cybersecurity posture by establishing National Guard Cyber Civil Support Teams, of up to 10 members, in every state and territory to bridge the gap between federal and non-federal efforts. Cyber CSTs would serve as first-responders to incidents under the direction of governors and the state adjutant general, building a trusted link between states, critical infrastructure providers, and the federal government.

**Why are National Guard Cyber Civil Support Teams a key part of addressing the cybersecurity gap?**

- The National Guard is the only US military force that can operate across both State and Federal responses. The US Cyber

Command's Cyber Protection Teams are limited by federal Title 10 authority.

- US Cyber Command needs a “point of presence” in every state and territory in order to rapidly effect information sharing up and down the chain during cyber-attacks.
- States need a dedicated cyber response force structure not beholden to DOD or the Cyber Mission Force in order to be successful in response to state, tribal, and local incidents.
- Numerous reports and testimonies have already called for increased National Guard involvement in the U.S. cyber posture to improve DOD support of civil authorities.
- Despite Presidential Policy Directives, GAO recommendations, and Congressional reports, the DOD has yet to define responsibilities for civil support in cyber incidents or for National Guard involvement.
- The best way to build an efficient response protocol *before* an attack happens is to establish local, dedicated teams that train and routinely share information. The Cyber National Guard teams in Washington, Virginia, and Michigan have built successful relationships with their non-federal partners.

Cyber CST's could lead the effort in their states to defend elections against cyberattack.

## APPENDIX 2B (pp 21-25)

**Washington's National Guard** Cyber Civil Support Team (articles below) performs penetration tests of local government agencies as well as utilities upon request. They have pioneered working across public and private sector domains, capturing lessons learned that could be shared across the country in order to prepare for major cyber events.

*Courtesy Lt. Col. Thomas Muehleisen, (ret.)*

---

### Guard attacks on demand

Guardsmen waging war in cyberspace with local agencies at their bidding

By J.M. Simpson on May 14, 2015

You may not be interested in cyber warfare and all that it embodies, but it is certainly interested in you. By the end of 2013, this country entered the era of the mega-breach when Russian-speaking hackers stole 40 million credit-card numbers after penetrating Target Corp. computer systems.

Cyber-attacks are commonplace; companies like Adobe Systems, J.P. Morgan Chase & Company, eBay, Anthem Inc. and others have experienced such attacks. While the specific reasons for these attacks can vary, the end result is the same - serious damage to the infrastructure undergirding this nation's economy.

Eye opening does not describe the challenges this state's computer savvy citizen-soldiers confront in protecting critical entities from an attack. And they are employing those skills to purposely attack willing participants before actual bad guys do the same.

"The threat exists," Lt. Col. Tom Muehleisen, a cyber planner, said. Muehleisen often made allusions to the old Star Trek TV series. "There can be a Romulan war bird parked off the coast." Can this war bird unleash a photon torpedo that can damage if not destroy part of the state's and/or nation's critical infrastructure? "Yes," Muehleisen answered. "Our mission is to assume a defensive position, to protect critical infrastructure from attack."

Where are these attacks coming from? "There is no such thing as a fully secure network," he continued. "In this business, you work under the assumption of a breach." To that end, Muehleisen and his small team of cyber warfare specialists work to defend against cyberattacks. While there is no such thing as a fully secure network, critical agencies must make themselves more secure from a binary borne assault.

A cyberattack is a deliberate exploitation of computer systems employed by individuals or organizations that target - zero in on, if you will - computer information systems, networks and/or personal computing devices through the use of malicious code to alter operations or data.

This attack generally results in a series of disruptive consequences that can compromise data and lead to theft, alteration, manipulation or the destruction of a specific computer system.

If a group of bad actors were to successfully deploy computer technology to destroy a power company's ability to provide power, we all could be living in the dark.

"I believe all utilities have to be concerned about their cyber security," wrote Benjamin Beberness, Snohomish County Public Utility District 1's chief information officer, in an email.

The district, or SnoPUD, is a public utility that provides power to 325,000 customers in Snohomish County and on Camano Island. The utility is the second largest public utility in the Pacific Northwest, and it is the 12th largest in the country.

To bad actors with intent to do harm to this country's power grid, SnoPUD is a prime target.

"Every day someone is knocking on SnoPUD's door trying to see what is inside," continued Beberness. The knocking on the door can and

sometimes does come in the form of a powerful cyberattack. Think of that Romulan war bird parked off the coast of Washington potentially arming a photon torpedo and you're getting the idea.

About two years ago, Beberness asked the Guard if it would create "SnoPUD #1 Cyber Security Defense Assessment" in order to test SnoPUD's ability to defend itself. In conducting the test, the Guard fielded a small but highly intelligent and experienced team of determined aggressors.

Penetration, testing and understanding the vulnerabilities of SnoPUD's computer infrastructure and key resources underscored the team's actions.

The team took its role seriously; it pulled no punches in testing SnoPUD's ability to protect itself.

Just as important, in conducting the test, the Guard's cyber warriors zeroed in on the utilities' "smart grid lab," a perfect replica of SnoPUD's actual computer driven operations center.

The cyber warriors utilized a penetration test, or pen test, to assess SnoPUD's abilities to protect itself. It is the blunt end of the Guard's assessment driven photon torpedo launched into SnoPUD's smart grid lab.

During the test, the Guard's cyber warriors entered the lab and began moving from one section to another. "The goal is to get in, look around, and leave without a trace. This testing is a good way to get the attention of the technicians at SnoPUD," Muehleisen said. "If we touch you, we own you."

The Guard personnel involved in this operation had little trouble leaving their fingerprints behind as they found and exploited SnoPUD's vulnerabilities to an actual cyberattack. "SnoPUD is very good at what it does," Muehleisen continued. "They are a proactive agency when it comes to defending against cyberattacks; SnoPUD pushes this agenda at the national level in order to convince other public utilities to engage with organizations like the Guard."

If agencies critical to the nation's infrastructure don't engage in discussions like SnoPUD and the Washington National Guard have, the Romulans most certainly will.

## **Washington National Guard is on cyber patrol**

### **Joint Forces Defense Assessment Team leads state's cyber-emergency planning**

By [Melissa Renahan](#) on February 18, 2014

Washington was the first state to find a role for the National Guard in its cyber-security efforts.

"The National Guard, through its existing relationships within every state and territory, is in a unique and important position to help solve what I call the 'cyber response capability gap.' That gap is the space that exists between what we acknowledge as a threat and our actual capability to do something about it," explained Col. Gent Welsh, former Chief Information officer for the Washington National Guard.

Enter the Joint Forces Defense Assessment Team. Thus far, Washington has used this team to conduct cyber-emergency planning and to search for vulnerabilities within state networks under the direction of the governor. Per mission, there are typically between five and eight team members, representing the State Guard, Air National Guard and Army National Guard for Washington.

"Right now, there is no agency within the federal or state government that has the mission to protect our nation's critical cyber infrastructure and in my opinion, nowhere in our nation's history has a problem been so acknowledged (cyber threats) but yet no comprehensive effort put forth to resolve it in a meaningful and collaborative way," stated Welsh, who has been in the Washington Air National Guard for more than two decades.

"For example, national leaders have talked about a 'cyber 9/11' but yet the nation still lacks a response force to manage the consequences of a devastating series of attacks which could target our critical infrastructure, not just military infrastructure, and the management and response processes are still in their infancy," Welsh continued.

This is part of the reason why Washington was the first state to find a role for the National Guard in its cyber-security efforts. Given that so many of the state's citizen soldiers work in a technology field in their civilian careers, it made sense to take advantage of that knowledge when they were serving in uniform.

"We want to work on proactive efforts, as well as a response to a cyber attack," explained Russ McRee, who works at Microsoft when he is not serving as a staff sergeant (who is poised to graduate from Officer Candidate School soon) with the Washington State Guard. His job at the software giant is remarkably similar to the role he plays at Camp Murray as both involve him assessing and analyzing threats.

"Where are the gaps? Where a threat meets a vulnerability and then becomes a risk? That's what we're seeking out," said Lt. Col. Thomas Muehleisen, the current Chief Information officer. "I feel fairly good about what we're doing nationally but it starts to break down somewhat at the state level and we're ready to improve that."

Recently, during one such assessment for a large state agency, McRee and his team identified approximately \$800 million in identified risk. That figure is calculated by adding up what said agency would have to do in order to recover and restore any lost records, which could run upwards of \$200 per lost record, per individual.

"We take on the role of the bad guy and try to compromise systems, find ways in and then take that assessment and information and advise the agency with the intent that now they have the weaknesses," McRee explained.

The cyber team has also worked with 25 other government agencies and private sector partners statewide to lead a cyber exercise that resulted in a standardized response if there was a major cyber threat or incident.

Moving forward, the cyber-security team would ideally like to have staff on duty every day to monitor and compare threat data ... but that is still a work in progress.

"Our duty is to defend the citizenry of our state and that's not just during a flood or combat situation - this is the new frontier. It's active threat and not getting better anytime soon," McRee said.

## APPENDIX 3 (pp 26-27)

### EXAMPLE GOVERNMENT COLLABORATION

#### National Centers of Academic Excellence in Cyber Defense



##### About The Program

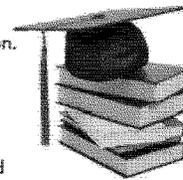
The increasing prevalence of cybersecurity attacks on both individuals and businesses emphasizes the need for cybersecurity professionals to protect and defend our Nation's critical infrastructure and systems. The **National Centers of Academic Excellence in Cyber Defense (CAE-CD)** program, co-sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS), was established to meet this growing need for knowledgeable and skilled cybersecurity professionals within the Federal Government – and ultimately, within state and local governments and industry.



With the CAE designation, colleges and universities are formally recognized by the U.S. Government for their robust cybersecurity-related programs. These institutions have undergone an in-depth assessment and have met rigorous requirements in order to be designated. They are well postured to equip students with expert knowledge and skills to protect and defend against the cyber threat landscape.

##### Program Highlights

- **Receive U.S. Government recognition** for your institution's cyber defense programs and curricula.
- **Map to specified Knowledge Units**, which align with the NICE Cybersecurity Workforce Framework (NCWF, NIST SP800-181), a cybersecurity language employed nationwide by educators, industry workers and government organizations.
- **Ensure student confidence** in your degree programs as a top choice to learn the necessary knowledge and skills to succeed in the cybersecurity workforce.
- **Assist federal agencies** by providing academic insight into cyber-related programs at DHS, NSA, and other federal agencies.
- **Serve** as a potential source and facilitator for government-academic researcher exchanges.
- **Facilitate development** of faculty and research leaders at your institution.
- **Join the CAE Community** of cybersecurity professionals, educators, researchers, and advocates to grow the cyber field.
- **Provide opportunities** for student scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program.

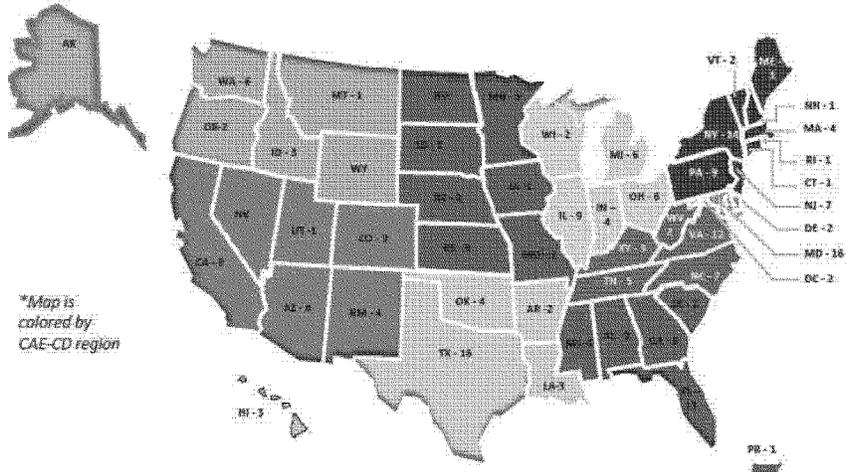


**National Centers of Academic Excellence in Cyber Defense**

**Eligibility**

All regionally accredited two-year, four-year, and graduate-level institutions in the United States can apply for designation as a NSA/DHS CAE-CD. CAE designation is valid for five academic years, after which the school must successfully reapply in order to retain its CAE-CD designation.

**CAE-CD Institutions**



**232 Total Institutions**

In 46 states + District of Columbia & Commonwealth of Puerto Rico

**More Information**

Visit [www.iad.gov/NIETP](http://www.iad.gov/NIETP) for more details on how to apply, download the available tools, and submit your institution's application.

Questions? Email [AskCAEIAE@nsa.gov](mailto:AskCAEIAE@nsa.gov)

For a full list of schools, visit: [https://www.iad.gov/NIETP/reports/cae\\_designated\\_institutions.cfm](https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm)

The CHAIRMAN. Thank you, Doctor.  
Dr. Sanders, welcome.

**STATEMENT OF DR. WILLIAM H. SANDERS, DONALD BIGGAR  
WILLETT PROFESSOR OF ENGINEERING, AND HEAD, DE-  
PARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING,  
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN**

Dr. SANDERS. Good morning, Chairwoman Murkowski, Ranking Member Cantwell and distinguished members of the Committee. Thank you for inviting me to speak today.

My name is Bill Sanders, and I'm the Head of the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. As was also said earlier when I was introduced, I've led or co-lead major centers funded by the Department of Energy, the Department of Homeland Defense and the National Science Foundation for the last 12 years working in this area.

I want to focus my comments today on cyber resiliency. Resiliency is a fundamental concept that differs from traditional metrics, such as reliability or cybersecurity. In the context of electric power, resiliency is not just about being able to lessen the likelihood an outage will occur, but it's about managing and coping with outage events when they do occur.

With resiliency, we attempt, to the greatest extent possible, to avoid a blackout, but understand and accept it may not be possible to totally avoid its occurrence. Thus, we work to respond as quickly as possible to the event when it occurs, preserving critical and individual societal services during the period of degraded operation and over time striving for full recovery and enhanced robustness.

An important new concern for the resiliency of this is the cyber portion of the grid and how it affects overall grid resiliency. The electric power system has become increasingly reliant on its cyber infrastructure to deliver electricity to consumers. A compromise of power grid control systems or other portions of the grid cyber infrastructure can have serious consequences ranging from a simple disruption of service with no damage to the physical components to permanent damage to hardware that can have long lasting effects on the performance of the system. Any consideration of improved power grid resiliency requires consideration of ways to make the grid cyber infrastructure resilient.

Over the last decade, much attention has rightly been placed on grid cybersecurity, but much less has been placed on grid cyber resiliency. It's now, however, becoming very apparent that protection alone by cybersecurity is not sufficient and it can never be made perfect.

Given the relentless attacks and the challenges of prevention, successful cyber penetrations are inevitable and there's evidence in increases of the rates of penetration.

The resiliency goals for the cyber infrastructure thus require a clear understanding of the interaction between the cyber and conventional physical portions of the grid and how impairments on either side, cyber or physical, could impact the other.

Specific guidance about cyber resiliency research that is critically needed comes from a consensus study published in July 2017 by

the National Academies of Sciences, Engineering and Medicine, entitled, Enhancing the Resilience of the Nation's Electricity System.

As one of the co-authors on this report, I helped craft seven overarching recommendations. Overarching recommendation number five is particularly relevant to the concept of cyber resilience. I'll paraphrase. The Department of Energy, together with the Department of Homeland Security, academic research teams, national labs and the private sector should carry out a program of research, development and demonstration activities to develop and deploy capabilities for the continuous collection of diverse, both cyber and physical sensor data, diffusion of sensor data with other intelligence information, visualization techniques, analytics, restoration techniques and the creation of post-event rules. In summary, the cyber threat to grid resiliency is real. The time to act is now.

It is critical that the Committee understand the following:

Number one, grid resiliency is different from cybersecurity and requires a fundamentally new approach.

Two, protection as a cybersecurity mechanism alone is not sufficient and can never be made perfect. The grid can only be resilient if its cyber infrastructure is also resilient. So, research and development are critically needed to provide assured mechanisms to ensure cyber resiliency.

Three, six capabilities—continuous data collection, the fusion of sensor data, visualization, analytics, restoration and post-event tools—are critical to creating an effective strategy for cyber resiliency. Those capabilities can only be achieved if academia, industry and government work closely together in a focused research and development program.

And finally, Congress should continue to fund and increase funding to the Department of Energy and other government agencies to advance this research and development.

Thank you very much. I would be happy to answer any questions.

[The prepared statement of Dr. Sanders follows:]

William H. Sanders, Head, Dept. of Electrical & Computer Engineering, University of Illinois at Urbana-Champaign

Testimony of

**William H. Sanders**

Donald Biggar Willett Professor of Engineering  
Head, Department of Electrical and Computer Engineering  
University of Illinois at Urbana-Champaign

Before the  
United States Senate  
Committee on Energy and Natural Resources

March 1, 2018

### **Introduction**

Good morning Chairwoman Murkowski, Ranking Member Cantwell, and distinguished Members of the Committee. Thank you for the opportunity to speak today.

I am a Donald Biggar Willett Professor of Engineering and the Head of the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. I was the founding director of the Information Trust Institute at the University of Illinois and served as director of the Coordinated Science Laboratory at Illinois. I am a professor in the Department of Electrical and Computer Engineering and in the Department of Computer Science. I am a Fellow of the IEEE, the ACM, and the AAAS; a past chair of the IEEE Technical Committee on Fault-Tolerant Computing; and past vice-chair of the IFIP Working Group 10.4 on Dependable Computing.

I am an expert on secure and dependable computing with a focus on critical infrastructures. I have published more than 270 technical papers in those areas. I was the 2016 recipient of the IEEE Innovation in Societal Infrastructure Award for “assessment-driven design of trustworthy cyber infrastructures for electric grid systems.” Since 2005, I have led or co-led major government-funded academic research centers (TCIP, TCIPG, and CREDC) that work to make the grid secure and resilient. I was also a member of the committee that wrote the National Academies of Sciences, Engineering, and Medicine consensus report entitled “Enhancing the Resilience of the Nation’s Electricity System.” In short, my experiences provide me with a unique perspective to offer the Committee insight and recommendations concerning the impairments to and approaches for providing cybersecurity and cyber resiliency in the nation’s energy infrastructure.

In my remarks today, I will:

- Describe the concept of cyber resiliency and the importance of resiliency in the cyber systems that control the grid,

(Portions of this testimony were taken verbatim from the National Academies of Sciences, Engineering, and Medicine report “Enhancing the Resilience of the Nation’s Electricity System, ISBN 978-0-309-46307-2 | DOI 10.17226/24836, available at <http://nap.edu/24836> and the associated “Report in Brief”)

- Describe the unique contribution universities (including Illinois) play in developing new, innovative technologies and approaches to preventing, detecting, and recovering from cybersecurity threats to the grid,
- Make specific recommendations of research to enhance the resiliency of the cyber portion of the power grid to attacks, and
- Argue that Congress should continue to fund and increase funding to DOE and other government agencies to advance this research.

### **Cyber Resiliency**

“Resiliency” is a fundamental concept that differs from traditional metrics such as reliability or cybersecurity. In the context of electric power, resiliency is not just about being able to lessen the likelihood that outages will occur, but also about managing and coping with outage events when they do occur. The goal is to lessen outage impacts, regrouping quickly and efficiently once an event ends, and, in the process, learning to deal with other events better in the future.

Stephen E. Flynn (2008) has outlined a four-stage framing of the concept of resilience: (1) preparing to make the system as robust as possible in the face of possible future stresses or attacks; (2) relying on resources to manage and ameliorate the consequences of an event once it has occurred; (3) recovering as quickly as possible once the event is over; and (4) remaining alert to insights and lessons that can be drawn (through all stages of the process) so that if and when another event occurs, a better job can be done at all stages.

With resiliency, we attempt, to the greatest extent possible, to avoid a large-scale event (in this case, a long-term blackout), but understand and accept that it may not be totally possible to avoid an event, and thus work to respond as quickly as possible to the event once it occurs—preserving “critical” individual and societal services during the period of degraded operation—and, over time, strive for full recovery and enhanced robustness to further impairments that could result in additional large-scale events.

Because the power system is hierarchical, these same concepts apply at several different levels of the system, including across the high-voltage grid, the regional grids (some of which are operated by regional transmission organizations), local transmission and distribution systems (typically the domain of utilities), and the end-user level (on both the utility and customer sides of the meter), and across both the cyber and conventional physical portions of the power grid. It is also clear that the resiliency of the power grid is critically dependent on other interconnected infrastructures (e.g., oil and gas).

A relatively new concern, and the subject of my core expertise, is the resiliency of the cyber portion of the grid, and how it affects overall grid resiliency. The electric power system has become increasingly reliant on its cyber infrastructure to deliver electricity to the consumers. This infrastructure includes computers, communication networks, other control system electronics, smart meters, and other distribution-side cyber assets. A compromise of the power grid control system or other portions of the grid’s cyber infrastructure can have serious consequences, ranging from a simple disruption of service with no damage to the physical components to permanent damage to hardware that can have long-lasting effects on the

performance of the system. Any consideration of improved power grid resiliency requires consideration of ways to improve the resiliency of the grid's cyber infrastructure.

Over the last decade, much attention has rightly been placed on grid cybersecurity, but much less has been placed on grid cyber resiliency. The sources of guidance on protection as a mechanism to achieve grid cybersecurity are numerous. It is now, however, becoming apparent that protection alone is not sufficient and can never be made perfect. Cybercriminals are difficult to apprehend, and there are nearly 81,000 vulnerabilities in the NIST National Vulnerability Database (NVD). An experiment conducted by the National Rural Electric Cooperative Association and N-Dimension in April 2014 determined that a typical small utility is probed or attacked every 3 seconds around the clock. Given the relentless attacks and the challenges of prevention, successful cyber penetrations are inevitable, and there is evidence of increases in the rate of penetration in the past year.

Fortunately, the successful attacks to date have largely been concentrated on utility business systems, as opposed to monitoring and control systems (termed "operational technology" or "OT" systems), in part because the operational technology systems have fewer attack surfaces, fewer users with more limited privileges, greater use of encryption, and more use of analog technology. However, there is a substantial and growing risk of a successful breach of operational technology systems, and the potential impacts of such a breach could be significant. These risks are growing in part because, as the grid is modernized, there is greater reliance on grid components with significant cyber controls. In addition, further integration of operational technology systems with utility business systems, despite its potential for increased efficiency, also poses serious risks.

Given that protection cannot be made perfect, and the risk is growing, cyber resiliency is critically important. Cyber resiliency aims to protect through established cybersecurity techniques, but acknowledges that such protections can never be perfect, and requires monitoring, detection, and response to provide continuous delivery of electrical service. While some solutions from classical cybersecurity can support cyber resiliency (e.g., intrusion detection and response), the majority of the cybersecurity work to date has focused on preventing the occurrence of successful attacks, rather than detecting and responding to partially successful attacks that occur.

In contrast, a cyber resiliency architecture should implement a strategy for mitigating cyberattacks and other impairments by monitoring the system and dynamically responding to perceived impairments to achieve resiliency goals. The resiliency goals for the cyber infrastructure require a clear understanding of the interaction between the cyber and conventional physical portions of the power grid, and how impairments on either side (cyber or physical) could impact the other. By their nature, such goals are inherently system-specific, but as a general principle they should balance the desires to minimize the amount of time a system is compromised and maximize the services provided by the system. Often, instead of taking the system offline once an attack has been detected, a cyber-resilient architecture attempts to heal the system while providing critical cyber and physical services. Based on the resiliency goals, cyber resiliency architectures typically employ sensors to monitor the state of the system on all levels of abstraction and detect abnormal behaviors. The data from multiple levels are then fused to create higher-level views of the system. Those views aid in detecting attacks and other cyber and

physical impairments, and in identifying failure to deliver critical services. A response engine, often with human input, recommends the best course of action. The goal, after perhaps multiple responses, is complete recovery, i.e., restoring the cyber system to a fully operational state.

#### **TCIP/TCIPG and CREDC**

These findings have grown out of collaborative academic-industry-government settings, including three major research activities that I have led or co-led over the last twelve years. In particular, I served as the Director and Principal Investigator (PI) of the DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center and currently serve as a co-PI of the Cyber-Resilient Energy Delivery Consortium (CREDC), which conducts research at the forefront of national efforts to make the U.S. power grid resilient.

The Trustworthy Cyber Infrastructure for the Power Grid projects (TCIP, 2005–2010; and TCIPG, 2009–2015), which were partnerships of four academic institutions, were conducted to meet the challenge of making the electricity grid resilient. The initial TCIP project (of which I was also Director and PI) was funded primarily by the National Science Foundation, with additional support by the Department of Energy’s Office of Electricity Delivery and Energy Reliability, and by the Department of Homeland Security’s Science and Technology Directorate, HSARPA, Cyber Security Division. The subsequent TCIPG project was funded by the Department of Energy’s Office of Electricity Delivery and Energy Reliability with partial support from the Department of Homeland Security’s Science and Technology Directorate, HSARPA, Cyber Security Division.

In those projects, we collaborated with national laboratories and the utility sector to protect the U.S. power grid by significantly improving the way the power grid infrastructure is designed, making it more secure, resilient, and safe. In both technology and impact, TCIP/TCIPG was a successful partnership of government, academia, and industry, creating multiple startup companies (including Network Perception, Inc., which I co-founded) and transitioning multiple technologies to industry (including First Energy, Schweitzer Engineering Laboratories, ABB, Honeywell, Ameren, Telecordia, GE, Entergy, EPRI, DTE Energy, and PJM, among others). The projects also had a significant positive impact on workforce education, delivering successful short courses, producing graduates, and providing the knowledge necessary to do interdisciplinary work of the same type at other universities.

CREDC (funded by the Department of Energy Office of Electricity Delivery and Energy Reliability with support from the Department of Homeland Security’s Science and Technology Directorate, HSARPA, Cyber Security Division) is a partnership of 10 academic institutions and 2 national labs that performs research and development in support of the Energy Sector Control Systems Working Group’s Roadmap of resilient Energy Delivery Systems (EDS) that focuses on the cybersecurity of EDS. In doing so, CREDC addresses the cybersecurity of power grids, as well as oil and gas refinery and pipeline operations. To do this, CREDC is developing projects with significant and measurable sector impact, involving industry partners (asset owners, equipment vendors, and technology providers) early and often, with activities that range from helping to identify critical sector needs, to performing pilot deployment and technology adoption. In fact, Robert M. Lee, who is also testifying here today, is a CREDC industrial advisory board member.

While progress is being made, further work is critically needed to define cyber resiliency architectures that protect against, detect, respond to, and recover from cyber attacks that occur.

#### **National Academy Recommendation Regarding Cyber Resiliency of the Grid**

Specific guidance about cyber resiliency research that is critically needed comes from a consensus study published in July 2017 by the National Academies of Sciences, Engineering, and Medicine entitled “Enhancing the Resilience of the Nation’s Electricity System.”

The study focused largely on reducing the nation’s vulnerability to large-area, long-duration outages—those that span several service areas or even states and last three days or longer. It found that much can be done to make both large and small outages less likely, but they cannot be totally eliminated, no matter how much money or effort is invested. To increase the resilience of the grid, our report argues that the nation must not only work to prevent and minimize the size of outages but must also develop strategies to cope with outages when they happen, recover rapidly afterward, and incorporate lessons learned into future planning and response efforts.

As one of the co-authors of the report, I helped craft seven overarching recommendations. One of these recommendations is particularly relevant to the concept of cyber resilience:

***Overarching Recommendation 5: The Department of Energy, together with the Department of Homeland Security, academic research teams, the national labs, and the private sector, should carry out a program of research, development, and demonstration activities to develop and deploy capabilities for the***

- *continuous collection of diverse (cyber and physical) sensor data;*
- *fusion of sensor data with other intelligence information to diagnose the cause of the impairment (cyber or physical);*
- *visualization techniques needed to allow operators and engineers to maintain situation awareness;*
- *analytics (including machine learning, data mining, game theory, and other artificial intelligence-based techniques) to generate real-time recommendations for actions that should be taken in response to the diagnosed attacks, failures, or other impairments;*
- *restoration of control system and power delivery functionality and cyber and physical operational data in response to the impairment; and*
- *creation of post-event tools for detection, analysis, and restoration to complement event prevention tools.*

Those six capabilities—(1) continuous data collection, (2) fusion of sensor data, (3) visualization, (4) analytics, (5) restoration, and (6) post-event tools—are critical elements of an effective strategy for cyber resiliency. These capabilities can be achieved only if academia, industry, and government work closely together in a focused research and development program.

**Summary**

The cyber threat to grid resiliency is real, and the time to act is now. It is critical that the committee understands the following:

- 1) Grid resiliency is different from cybersecurity and requires a fundamentally new approach.
- 2) With grid resiliency, we attempt, to the greatest extent possible, to avoid long-term blackouts, but understand and admit that it may not be totally possible to avoid them, and thus we work to respond as quickly as possible to the event once it occurs (preserving “critical” services during the period of degraded operation) and, over time, strive for full recovery and enhanced robustness.
- 3) The grid can be resilient only if its cyber infrastructure is resilient, so research and development are critically needed that provide assured mechanisms to ensure cyber resiliency.
- 4) Six capabilities—(1) continuous data collection, (2) fusion of sensor data, (3) visualization, (4) analytics, (5) restoration, and (6) post-event tools—are critical to creating an effective strategy for cyber resiliency.
- 5) Those capabilities can be achieved only if academia, industry, and government work closely together in a focused research and development program.
- 6) Congress should continue to fund and increase funding to DOE and other government agencies to advance this research.

Thank you for the opportunity to be here with you today. I would be happy to answer any questions that you have.

The CHAIRMAN. Thank you, Dr. Sanders.  
Mr. Lee, welcome to the Committee.

**STATEMENT OF ROBERT M. LEE, CHIEF EXECUTIVE OFFICER  
AND CO-FOUNDER, DRAGOS, INC.**

Mr. LEE. Chairwoman Murkowski, Ranking Member Cantwell and members of the Committee, thank you for providing me the opportunity to present before you today.

I want to briefly explain my background which informs the testimony I bring before you. I started my career at the United States Air Force Academy, was commissioned and then took a position as a cyber warfare operations officer tasked out to the National Security Agency (NSA).

While at the NSA I was tasked with building a mission to identify new nation-state threats breaking into environments. It was there that I built and led a first-of-its-kind mission looking at the nation-states breaking into industrial environments. I did so with the hypothesis that we would find the new threats, and we did. It was there I came to understand that there was a significant collection bias in the U.S. intelligence community and in the larger information security community. That means, as we typically prioritize and report on things where we collect and can see, but we're blind to the environments that we're not collecting like industrial control networks.

I left to build Dragos to gain insights and develop technology to help people.

Over the last three years, we've seen these type of attacks take place: The Ukraine power grid attack of 2015, I was one of the lead investigators there to solve the first-ever cyberattack that could halt grid operations; the Ukraine attack of 2016, where my firm and I helped identify and analyze CRASHOVERRIDE—the software that was purposely built to disrupt electric grids; and, in 2017 in the Middle East a more concerning thing to me is that a first piece of malware that was developed to specifically target human life was deployed. So with my experience in the military and intelligence community, training the world's defenders and leading the world's best against the world's worst, I want to highlight a few points for you today.

First, as scary as all this sounds, our infrastructure is extremely resilient today. We have to do more, but I do want to note that there's a lot of good work happening in the community. My team often strives for nuance in our analysis and reporting on the threats, but we have observed a disservice to the community over the last couple decades, even the most casual phishing email deployed to a corporate network of a nuclear power plant gets headlines about cyberattacks taking down infrastructure and killing people. This is not accurate. These scenarios presented are often nonsense and full of hype and unintended misinformation, but the threats are real.

Today, my firm released three reports detailing the industrial threats of vulnerabilities and our lessons learned and response. We detailed five such threat activity groups or teams specifically targeting industrial control networks. This is in addition to the much

larger number of teams that are targeting the corporate networks of infrastructure companies but this specific trend is worrying.

Equally important though, we must be careful of technologies and approaches which sound like silver bullets and they sound too good to be true. These approaches are often referred to in the industry as buzzwords making immense traction and buzz and attention when used in conversations and they do have an application, but they're obviously and usually extended far past that application. And the context of cybersecurity, block chain, machine speed, automated response and artificial intelligence are three such examples that are thrown around frequently as a panacea for our problems when they are simply not.

On to my second point today which is the role of regulation. The NERC CIP standards are often highly discussed topics, but it is undeniable that the efforts in the community to comply with these standards have made the North American bulk electric system the most resilient and well defended in the world. However, regulations serve as a base level of security. They're obviously on the trailing end of what is going on and they, in no way, can regulate the human adversary. Malware and vulnerabilities are not our threats, the human adversary is our threat.

For that, we must take an approach that also appreciates the workforce development that's required. I recommend for a period of three to four years that no new regulations be imposed under NERC—it would allow companies to catch up with current regulations as well as identify the threat landscape before them and come up with their own best practices for the type of innovation that we need for industrial-specific networks.

On my third point my recommendations for DOE's CESER. First, provide multi-year funding and greater operational support to efforts that are prioritized to make foundational changes to the fundamental risk. Consequence-driven, cyber-informed engineering is one of those programs that's been highlighted that I think very kindly of. It is in no way going to fix everything, but it is foundational and so, our grid security.

Second, CESER should serve as the key team focused on de-duplicating efforts in the DOE and their labs by being keenly aware of what is already taking place in the private sector. There is never malice or intentional overlap, but at the speed and rate of innovation in the private sector as well as the sheer volume, overlap can take place that has unintentional overlaps and competitive issues will emerge.

Third, with a stated mission of focusing on addressing emerging threats, realize and appreciate the best insights and intelligence on threats or in the community and the companies that are being targeted. The private sector companies, like Dragos, as well as the community members like the electric ISAC, the downstream natural ISAC and the others, have a keen insight in that threat landscape today and partnering with teams like CESER will ensure that they do not recreate efforts, but that we all achieve the same goal of providing security to our infrastructure.

I sincerely want to thank the Committee for providing me the opportunity to testify today and will welcome any questions and addi-

tional information to help support the safety of our families, communities and each other.

Thank you.

[The prepared statement of Mr. Lee follows:]



## THE INDUSTRIAL CYBER THREAT LANDSCAPE

### THE ROLE OF THE PRIVATE SECTOR AND GOVERNMENT IN ADDRESSING CYBER THREATS TO ENERGY INFRASTRUCTURE

---

#### HEARING BEFORE THE

#### COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

1 MARCH 2018, DIRKSEN SENATE OFFICE BUILDING

<https://www.energy.senate.gov/public/index.cfm/2018/3/full-committee-hearing-to-examine-cyber-security-in-our-nations-critical-energy-infrastructure-030118>

Robert M. Lee<sup>1</sup>

#### I. Background

Chairwoman Murkowski, Ranking Member Cantwell and members of the committee, thank you for providing me the opportunity to testify before you today. As a kid from a small town in Alabama with my parents who are both retired Air Force Senior Master Sergeants, it is a distinct honor to appear before you. My name is Robert Lee and I am the CEO and co-founder of Dragos, Inc. an industrial cybersecurity focused firm that takes an intelligence-driven approach to our technology and offerings and is staffed by some of the best in the community. Many of my teammates have served in the National Security Agency, military, and at the plant-floor level of the industrial environments we will be speaking about today.

I want to briefly explain my background which informs the testimony I bring before you today. I started my career at the United States Air Force Academy, was commissioned as a Cyber Warfare Operations Officer, and was then tasked out for most of my career to the National Security Agency (NSA).

While at the NSA I was tasked with building a mission to identify new nation-state groups and actors we had not previously known about. I built and led a first-of-its-kind mission focused on identifying the nation-states attempting to break into these environments. It was built on the hypothesis that we would find new threats; and we did. These were new nation-state teams performing new tradecraft during their operations. It was there I came to understand that there is a significant collection bias in the U.S. Intelligence Community and larger information security community. The community focuses and reports

---

<sup>1</sup> CEO and Co-Founder of Dragos, Inc. @RobertMLee



on the threats from where our collection exists and is blind to most of what goes on where we do not collect, such as industrial control environments.

My experiences have led me to assess that our industrial community has two strategic challenges: we do not understand the industrial threat landscape and we do not have enough trained professionals focusing on industrial control cybersecurity. For these and many other reasons I left the military and joined the private sector to tackle these issues. I built the community's first industrial control system incident response and investigations specific course at the SANS Institute and later a dedicated threat intelligence course there as well.<sup>2,3</sup> At SANS I have trained over 2,000 cybersecurity defenders across five continents at the world's smallest and largest companies. I learned from their points of view and their challenges.

I founded Dragos, Inc. with two of my co-workers from the NSA industrial threat discovery mission. It is at Dragos that we built the world's only intelligence-driven software technology for industrial networks to detect and respond to threats. It is also there we have the private sector community's only intelligence team fully dedicated to industrial control threats.

There were three major industrial cyber attacks over the last three years not counting the large number of adversary operations targeting critical infrastructure but not reaching the level of attacks. The Ukraine power grid cyber attack of 2015 was the first time in history a cyber attack halted grid operations, for that I was one of the lead investigators.<sup>4</sup> The Ukraine attack of 2016 where my firm helped identify and analyze CRASHOVERRIDE, the malicious software which was the first ever malware purpose built for disrupting electric grids.<sup>5</sup> And the attack in the Middle East in 2017 where my firm identified and analyzed TRISIS, the malicious software which was the first to ever specifically target human life and caused a petrochemical plant to shut down.<sup>6</sup>

## II. The Three Points Today

Given my experience in the military and intelligence community, training the world's defenders, and leading the world's best against the world's worst, I would like to make three points today that are most relevant for this committee.

- The first, is that the industrial threat landscape is largely unknown. This demands that we seek to change this through an intelligence-driven approach that will then be used to inform our innovations, best practices, standards, and regulations.
- The second is that regulation has served a purpose in the private sector such as electric grid operators, but it is appropriate and needed to pause new regulation to allow the community to develop best practices and out-innovate our adversaries.
- The third is a recommendation for the new Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to focus on new and continued relationships between the DOE and the private sector while respecting that most of the knowledge of the threats and the innovation to counter them is occurring in the private sector. This drives a requirement for communities to work together without interfering in each's respective mission.

---

<sup>2</sup> [www.sans.org/ics515](http://www.sans.org/ics515)

<sup>3</sup> [www.sans.org/for578](http://www.sans.org/for578)

<sup>4</sup> [https://ics.sans.org/media/E-ISAC\\_SANS\\_Ukraine\\_DUC\\_5.pdf](https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf)

<sup>5</sup> <https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>

<sup>6</sup> <https://dragos.com/blog/trisis/TRISIS-01.pdf>



### III. Point I: The Industrial Threat Landscape is Largely Unknown

The industrial threat landscape is largely unknown. For years, the Department of Homeland Security's Industrial Control System Computer Emergency Response Team (ICS-CERT) has collected and centralized what they could to report on incidents in the private sector. Each year, media headlines highlighted the number of incidents in sectors like the electric power community. However, each year the most important metric was reported but went unnoticed. That metric stated that every single year, the number one attack vector for adversaries breaking in to industrial network was: unknown.<sup>7</sup>

The methods and collection the information security community has used to identify adversaries and their intrusions into corporate and business networks have not historically been available or present in the industrial networks. It is most certainly not present in the smaller co-ops and municipalities where adversaries are able to train and prepare undetected and undeterred. Industrial networks are different than the corporate and business networks of each company and require a different focus and approach.<sup>8</sup> Much of the collection by the U.S. Intelligence Community and the private sector has been in observing adversaries breaking into networks and patterning out and identifying their tradecraft and capabilities. This focus on intrusion analysis has led the private sector to be able to produce intelligence reports that rival and, in many cases, far exceed similar reporting in classified government settings. Simply stated, the best place to collect data relevant to cyber threats is in the networks of the targeted companies.

The information security technologies made for enterprise and corporate networks are often not appropriate for industrial networks and thus much of the community has believed that industrial threats are not common because of a limitation in this collection. Despite these limitations, some companies have done great work to identify some of the industrial threats especially when corporate networks are also being targeted. However, in the history of the information security community having purpose-built software, expertise for industrial security incident response, and threat intelligence focused on these environments is very new. In fact, it is only a few years old. As my team and others like it grow we will be faced with existing threats displaying new capabilities and brand-new threats we did not previously know existed. In other words, we will find more because we are looking now but it is also true that the focus of adversaries on industrial control environments is also growing significantly.<sup>9</sup>

Today my firm, Dragos, released three reports documenting our insights and lessons learned from 2017 across threats, vulnerabilities, and lessons learned in threat hunting and incident response.<sup>10</sup> We highlighted the CRASHOVERRIDE and TRISIS malicious software previously referenced but also noted a few very important key findings regarding the threats. First, common malware not purpose built for industrial networks is still incredibly impactful and disruptive in industrial control environments. Many of us heard of the large impacts of WannaCry and NotPetva malware on industrial environments such as the shipping and manufacturing industry that cost billions of dollars.

The report however also highlights and provides a base, census-like metric, that there are, on a very conservative estimate, at least 6,000 unique infections in industrial environments each year from common, non-targeted, malware leading to loss of revenue and in rare cases potentially unsafe conditions. However, common malware infections that spread indiscriminately are not what concerns me or most of the community. What concerns many of us most is the threat activity groups, or teams, who target

<sup>7</sup> [https://ics-cert.us-cert.gov/sites/default/files/Annual\\_Reports/Year\\_in\\_Review\\_FY2015\\_Final\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf)

<sup>8</sup> <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>

<sup>9</sup> [www.dragos.com/yearinreview/2017](http://www.dragos.com/yearinreview/2017)

<sup>10</sup> *Ibid.*



industrial control networks. These types of campaigns against our infrastructures were rarely seen or discussed. In the Dragos annual report, the second key finding identifies that there are five such threat activity groups active this past year alone who are specifically targeting industrial control networks at infrastructure companies. There are significantly more groups that are targeting the corporate environments of infrastructure companies, but the increase in industrial specific targeting is a worrying trend. These five teams launched numerous operations that ranged from espionage to what appears to be the first stages of access required to disrupt operations.

As scary as that sounds, I want to take a moment to add an important note: the threat is far worse than people realize but not as bad as they want to imagine. My team often strives for nuance in our analysis and reporting on threats and we have observed a disservice to the community over the past decade. Even the most casual phishing email sent to a nuclear power station's corporate networks results in media headlines and inquiries about how adversaries are going to take down our infrastructure and kill people. The scenarios presented are often nonsense and full of hype and unintended misinformation. In North America we have some of the most defensible infrastructure on the planet thanks largely to our diversity and the community of people involved. Organizations ranging from the Edison Electric Institute (EEI) to NERC's Electricity Information Sharing and Analysis Center (E-ISAC) to the asset owners and operators who are doing the real defense are simply amazing and have ensured the reliability and safety of electric energy. As an example, our electric power grid and its various asset owner and operators have security infrastructure and culture of which the rest of the world is envious. The idea that a phishing email or even access into industrial networks would equate to mass chaos, disruption, and death is nonsensical and for poorly researched books and media headlines, not reality.

We as a community have only begun our journey though and there are industrial sites including those in North America whose internal teams have never even investigated the networks. I am aware of small electric co-ops, water utilities, gas pipeline facilities, oil refineries, wind farms, and manufacturing networks where not even the basics of security have been attempted although they are vital for modern civilization. The disparity across our infrastructure communities in terms of their investments and culture is a concern. As we identify the threat landscape more fully we must ensure that our technologies, best practices, standards, and regulations are informed by the industrial threat and are not simply copy and pasted insights from information technology and corporate networks as has often been the case in the past.

Equally important, we must be careful of technologies and approaches which sound too good to be true. These approaches are often referred to in the industry as buzzwords. They gain immense traction and attention when used in conversations, but security professionals widely understand their limitations and the abuse of those approaches. Blockchain, machine-speed automated response, and artificial intelligence are three such examples that are thrown around frequently as a panacea for our problems when they are simply not. Blockchain is just a ledger that does not *secure* anything, delays in response are due to vital investigations to have confidence in the actions we take not due to the need to push *machine-speed* changes, and unfortunately, we already have too much *artificial* intelligence in the security industry.

We must be measured and nuanced in how we approach the risk from cyber threats and the approach we take must be an intelligence-driven one that understands our threat landscape as well as the limitations we have in collection and analysis that hamper our understanding. Our approach must also respect that the best defense we can put forth against well-funded human adversaries is well trained and empowered human defenders operating in defensible environments with the right technology and insight and not simply the most interesting sounding.



#### IV. Point 2: The Role of Regulation in the Electric Power Grid

The multiple grids that make up the North American bulk electric system are different than they were fifteen years ago. Massive changes, for the better, have been made especially in the areas of implemented security controls. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are standards for Bulk Electric System asset owners and operators mandated by the Federal Energy Regulatory Commission (FERC). NERC CIP standards are often highly discussed topics, but it is undeniable that the efforts of the community to comply with these standards have made the North American Bulk Electric System the most resilient and well defended in the world. However, regulations and standards are the trailing end of best practices and only serve as a base level of security. They are not, nor would any regulation be, adequate in the face of determined adversaries. Malware and vulnerabilities are not the threat, the threat is the human adversary and we cannot regulate them away.

In fact, many regulations and standards focus on cyber hygiene and information sharing type efforts such as vulnerability management and patching. The Dragos report released today included an exhaustive look at all the industrial control system software and hardware vulnerabilities released in 2017. It identified that 64% of the vulnerability patches do not eliminate any risk because the components they were patching were already insecure to start with.<sup>11</sup> For 2018 we are tracking a new metric looking at the accuracy of the advisories themselves regardless of whether they reduce risk. So far in 2018 roughly 75% of the advisories released publicly had significant inaccuracies. These inaccuracies include a misunderstanding of the product, vulnerability, or the impact and risk it posed to the industrial process.

What that means is the community spends resources to address a problem that provides no benefit in addressing 64% of the time and often the industrial community is unsure if the vulnerability advisory was accurate at all. Patching is meaningful to reduce the attack surface but in industrial networks it is obviously far less meaningful than people realize. In looking at the Ukraine 2015 cyber attack, the investigation found that there were no exploits or software vulnerabilities used by the adversary in the industrial networks to disrupt the grid. In this case, they simply gained access, learned the systems and how to use them against themselves, and then used intended functionality to hijack away the system from their operators. An additional important metric in the Dragos report is that 72% of industrial control system vulnerabilities in 2017 provided no alternative mitigation guidance outside of patching, suggesting no method to reduce risk until after an update cycle. What this effectively means is the overwhelming focus for the industry is on patching away problems while it is, a majority of the time, ineffective against human threats. This is not to say that patching should not occur, but we should instead understand it does not reduce the risk nearly as much as the community would otherwise like to believe and we must take an active defense approach which means monitoring for, responding to, and learning from the threats in our environments. Regulations are not well suited for that challenge.

I have seen first-hand a regulation, check-box, mentality develop at companies subject to strong regulations. In my engagements with customers and in training the defenders of the electric system it is a common complaint I hear as well. Many resources go to satisfying regulations and trying to keep up with what regulations are coming next that a stall in innovation and security can occur. We have electric utilities today that have expressed the desire to do more in their industrial networks including deploying our technology to identify threats but are afraid to do so not knowing what regulation may come next and if their current investments will be upended by those new approaches. There are electric utilities that are

---

<sup>11</sup> [www.dragos.com/yearinreview/2017](http://www.dragos.com/yearinreview/2017)



the most well protected companies in the world, there many more that are in the middle just trying to keep up with the regulations, and there are a rare few who are actually worse off as their precious resources had to be spent addressing regulation instead of the security efforts they were already doing. NERC CIP regulations have been an overall good initiative and have helped the electric community to improve its security, but we must now do something different for a period time.

I recommend for a period of three to four years that no new regulations be imposed under NERC CIP. This would allow companies to catch up with the current regulations that come out every couple of years in an unending push for more regulation. It will also allow the electric asset owner and operator community to spend a period of time innovating and thinking of new best practices informed by experience. At the end of this period DOE, FERC, NERC, and the regulated community can then identify best practices and determine if new regulations are appropriate. It is also in this time that a deep study and analysis of the threats is appropriate to ensure that our regulations are guided by lessons-learned from dealing with the threats and not general community best-practices that may not make sense for our electric community.

If this recommendation is not palatable then I would propose an alternative where the regulations are focused instead on program building, such as regulating that a company implement a threat intelligence program, instead of performance-based auditing. This would satisfy the potential desire to move regulations forward while allowing the electric community to develop their own ways forward inside of those programmatic bounds.

#### V. Point 3: Recommendations for DOE's CESER

DOE's Office of Electricity Delivery and Energy Reliability (OE) leads the DOE's efforts to ensure a resilient, reliable, and flexible electricity system. OE accomplishes this mission through research, partnerships, facilitation, modeling and analytics, and emergency preparedness. These meaningful contributions to the electric community far exceed what regulation alone would ever accomplish. My experiences with DOE's staff and their labs' staff have left me impressed and those I know I am proud to call peers, colleagues, and friends. The DOE's CESER office was the next logical step for DOE's efforts in cybersecurity and energy security. The creation of the office is still a debated topic though. However, that decision has been made and it is important now not to cast doubt on the office's future effectiveness but instead its role and what service it can perform for the community.

As the owner of a private sector company and as a member of the electric sector community I am always hesitant of well-intentioned government programs, grants, and efforts that ultimately are not in tune with what is already going on in the community. Such efforts can result in competition that stifles innovation, it can result in market noise, and it can result in the larger community not dividing and conquering all the various issues we have while working in tune with one another. The labs have historically pioneered discoveries in fields such as avionics, nuclear engineering, and grid reliability but the industrial cybersecurity field is a fast-moving area that I would like to see more cooperation that incorporates private sector technologies as opposed to spending years potentially replicating what already exists.

It is for these reasons that I would recommend three things to DOE's CESER. First, provide multi-year funding and greater operational support to efforts that are prioritized to make foundational changes to the community's risk. As an example, consequence-driven cyber-informed engineering (CCE) should be prioritized and supported. CCE will not address all cyber risks nor will it eliminate the ability for cyber threats to be effective. However, CCE will lead to systems and equipment in industrial control environments that are designed and built with an understanding of the cyber threats and risks translating



to more defensible environments.<sup>12,13</sup> Encouraging improved product designs where efforts such as patching can be effective, and some smaller set of risks are eliminated altogether would be extremely meaningful to the community.

Second, serve as the key team focused on de-duplicating efforts in the DOE and their labs by being keenly aware of what is already taking place in the private sector. There is never malice or intentional overlap but the speed of the private sector in comparison to appropriations and grants as well as the sheer volume of innovation taking place can cause unintentional overlaps and competitive issues to emerge. DOE's CESER could, with the appropriate authorities, significantly reduce these issues.

Third, with a stated mission of focusing on addressing emerging threats realize and appreciate that the best insights and intelligence on threats in the community are inside the networks of the targeted companies. The private sector companies, like Dragos, that are already in those environments and glean threat intelligence can offer unique insights. Partnering with similar companies and such organizations as NERC's E-ISAC will provide the insights CESER needs without trying to recreate any efforts. Additionally, there are challenges for private sector companies to share their information with the government. Even beyond any trust issues much of the information that the government wants, and needs, is more akin to finalized intelligence assessments and not access to raw data. The private sector understandably wants to protect its raw and sensitive data but insights into the threat landscape, trends, and other types of intelligence assessments are often happily shared. There is a distinct role here for private sector security companies and the ISAC framework to act as a trusted layer between the organizations that are being targeted by adversaries and the government's authorities balanced with intelligence requirements. This can be achieved while providing security for these companies instead of just information and intelligence sharing.

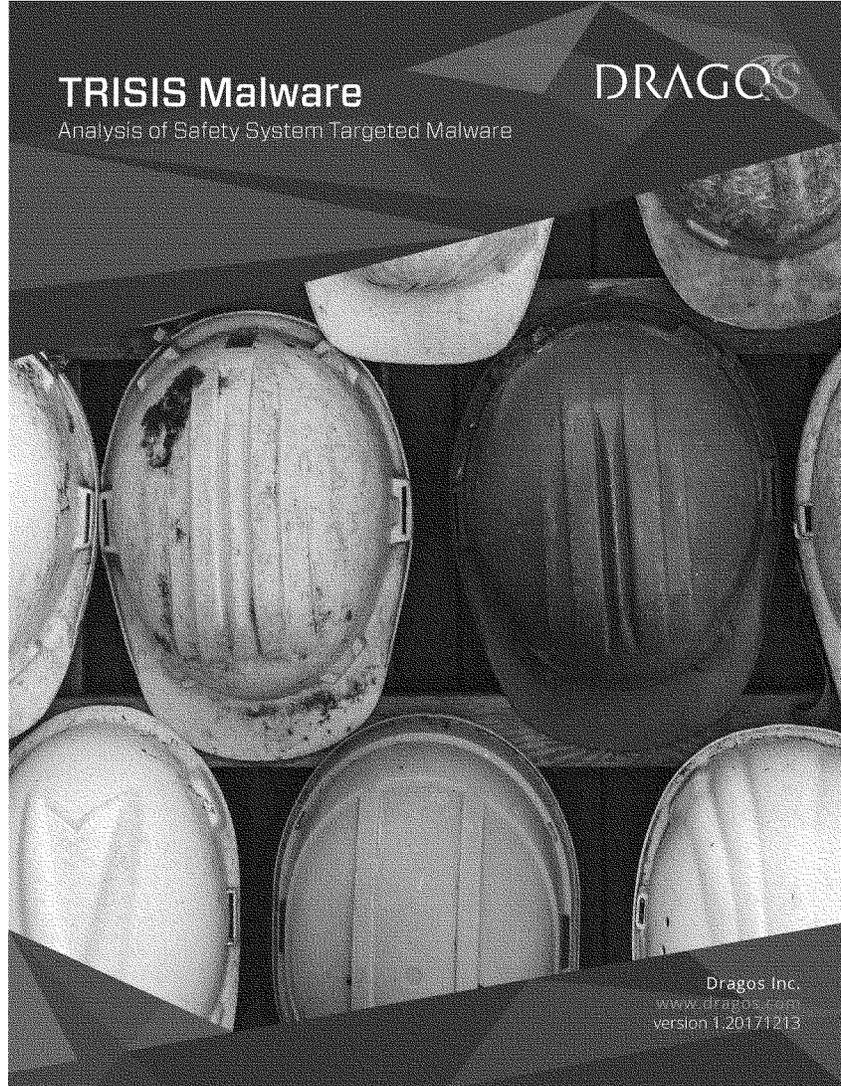
It will be beneficial for CESER to work with organizations already doing the mission such as Dragos and the E-ISAC. Our insights into the threat landscape and emerging threats together is novel and currently underexplored in the larger community today. The value the private sector in concert with efforts such as DOE's CESER can provide meaningful defense to our critical infrastructures as well as those smaller infrastructures critical to our local communities.

I sincerely thank the Committee for providing me the opportunity to testify today and welcome any questions or additional information to help support the safety of our families, communities, and each other.

---

<sup>12</sup> <https://www.ferc.gov/CalendarFiles/20170717080648-Assante,%20SANS%20Institute.pdf>

<sup>13</sup> <https://www.osti.gov/biblio/1341416>



# TRISIS Malware

Analysis of Safety System Targeted Malware

DRAGOS

Dragos Inc.  
[www.dragos.com](http://www.dragos.com)  
version 1.20171213

TLP: WHITE information may be distributed without restriction

### Executive Summary

In mid-November 2017, the Dragos, Inc. team discovered ICS-tailored malware deployed against at least one victim in the Middle East. The team identifies this malware as TRISIS because it targets Schneider Electric's Triconex safety instrumented system (SIS) enabling the replacement of logic in final control elements. TRISIS is highly targeted and likely does not pose an immediate threat to other Schneider Electric customers, let alone other SIS products. Importantly, the malware leverages no inherent vulnerability in Schneider Electric products. However, this capability, methodology, and tradecraft in this very specific event may now be replicated by other adversaries and thus represents an addition to industrial asset owner and operators' threat models.

### Why Are We Publishing This?

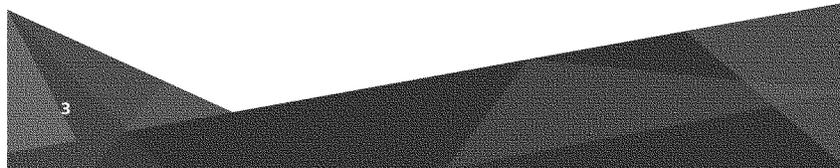
The Dragos team notified our ICS WorldView customers immediately after validating the malicious nature of the software. Following that notification, the team sent a notification to the U.S. Department of Homeland Security, Department of Energy, Electric Sector Information Sharing Analysis Center (E-ISAC), and partners. We broadcasted to our customers and partners that we would not be releasing a public report until the information became public through other channels. It is Dragos' approach around industrial threats to never be the first to identify new threats publicly; infrastructure security is a highly sensitive matter and the more time the infrastructure community has to address new challenges without increased public attention is ideal. Dragos' focus is on keeping customers informed and ideally keeping sensitive information out of the public where the narrative can be quickly lost and sensationalized. However, once information about threats or new capabilities are made public, it is Dragos' approach to follow-up with public reports that capture the nuance to avoid hype while reinforcing lessons learned and advice to the industry.



TLP: WHITE information may be distributed without restriction

### Key Take-Aways

- The malware targets Schneider Electric's Triconex safety instrumented system (SIS) thus the name choice of TRISIS for the malware.
- TRISIS has been deployed against at least one victim.
- The victim identified so far is in the Middle East, and currently, there is no intelligence to support that there are victims outside of the Middle East.
- The Triconex line of safety systems are leveraged in numerous industries - however, each SIS is unique and to understand process implications would require specific knowledge of the process. This means that this is not a highly scalable attack that could be easily deployed across numerous victims without significant additional work.
- The Triconex SIS Controller was configured with the physical keyswitch in 'program mode' during operation. If the controller is placed in Run mode (program changes not permitted), arbitrary changes in logic are not possible substantially reducing the likelihood of manipulation.
- Although the attack is not highly scalable, the tradecraft displayed is now available as a blueprint to other adversaries looking to target SIS and represents an escalation in the type of attacks seen to date as it is specifically designed to target the safety function of the process.
- Compromising the security of an SIS does not necessarily compromise the safety of the system. Safety engineering is a highly specific skill set and adheres to numerous standards and approaches to ensure that a process has a specific safety level. As long as the SIS performs its safety function the compromising of its security does not represent a danger as long as it fails safe.
- It is not currently known what exactly the safety implications of TRISIS would be. Logic changes on the final control element implies that there could be risk to the safety as set points could be changed for when the safety system would or would not take control of the process in an unsafe condition



## SIS Background

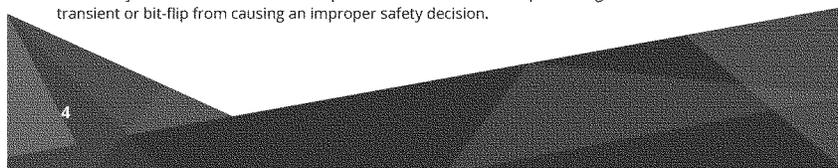
Safety systems are those control systems, often identified as Safety Instrumented Systems (SIS), maintaining safe conditions if other failures occur. It is not currently known what the specific safety implications of TRISIS would be in a production environment. However, alterations to logic on the final control element imply that there could be a risk to operational safety. Set points on the remainder of the process control system could be changed to conditions that would result in the process shifting to an unsafe condition. While TRISIS appears to be focused, ICS owners and operators should view this event as an expansion of ICS asset targeting to previously-untargeted SIS equipment. Although many aspects of TRISIS are unique for the environment and technology targeted, the general methodology provides an example for ICS defenders to utilize when future, subsequent SIS-targeted operations emerge.

Safety controllers are designed to provide robust safety for critical processes. Typically, safety controllers are deployed to provide life-saving stopping logic. These may include mechanisms to stop rotating machinery when a dangerous condition is detected, or stop inflow or heating of gasses when a dangerous temperature, pressure, or other potentially life-threatening condition exists. Safety controllers operate independently of normal process control logic systems and are focused on detecting and preventing dangerous physical events. Safety controllers are most often connected to actuators which will make it impossible for normal process control systems to continue operating. This is by design since the normal process control system's continued operation would feed into the life-threatening situation that has been detected.

Safety controllers are generally a type of programmable logic controller (PLC). They allow engineers to configure logic, typically in IEC-61131 logic. While on their face they are similar to PLCs, safety controllers have a higher standard of design, construction, and deployment. They are designed to be more accurate and less prone to failure. Both the hardware and the software for these controllers must be designed and built to the Safety Integrity Level (SIL) blanket of standards (IEC-61508). This includes the use of error correcting memories and redundant components and design that favors failing an operation safety over continuing operations. Each SIS is deployed for specific process requirements after a process hazard analysis (PHA) identifies the needs for a specific industrial environment. In this way, the systems are unique in their implementation even when the vendor technology remains the same.

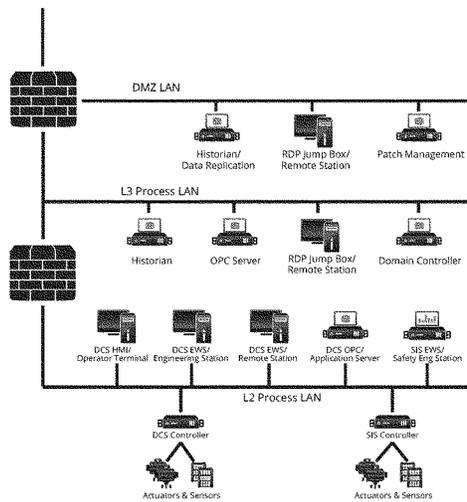
Safety controller components have more flexibility than a typical PLC. A safety controller's output cards will usually have a firmware, and a configuration, which allows the output card to fail into a safe state should the main processors fail entirely. This may even include failing outputs to a known-safe state in the event that the safety controller loses power.

Many safety controllers offer redundancy, in the form of redundant processor modules. In the case of the Triconex system, the controller utilizes three separate processor modules. The modules all run the same logic, and each module is given a vote on the output of its logic function blocks on each cycle. If one of the modules offers a different set of outputs from the other two, that module is considered faulted and is automatically removed from service. This prevents a module that is experiencing an issue such as an internal transient or bit-flip from causing an improper safety decision.

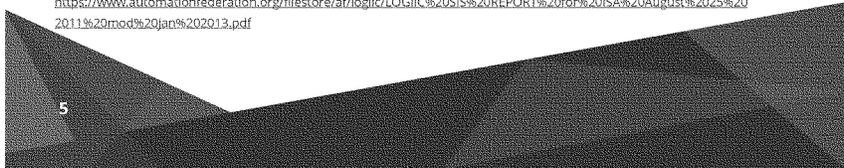


TLP: WHITE information may be distributed without restriction. Safety controller architecture has been debated in the industry. Many end users opt to use the same control LAN for both systems. LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) has identified<sup>1</sup> three distinct integration strategies of SIS with control systems networks. In the case of attacks such as TRISIS, these architectures can be reduced to two, as the security implications of two identified architectures remain the same. End users decide the level of risk that they are willing to accept with their safety system, and use this to determine how tightly they couple their safety system with their DCS (Distributed Control System). A tightly-coupled architecture, shown in figure 1, can provide cost savings, since data from an SIS controller may be incorporated into general operator HMI systems. In addition, network wiring and support is shared between the systems. Sensors data may also be shared, in both directions, between the normal process controllers and the SIS controllers. However, a downside to such an architecture is that an attacker who gains access to the Control LAN systems may attack the SIS directly.

Figure 1: Typical (Insecure) SIS integration

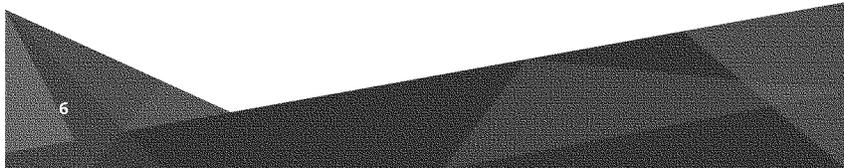
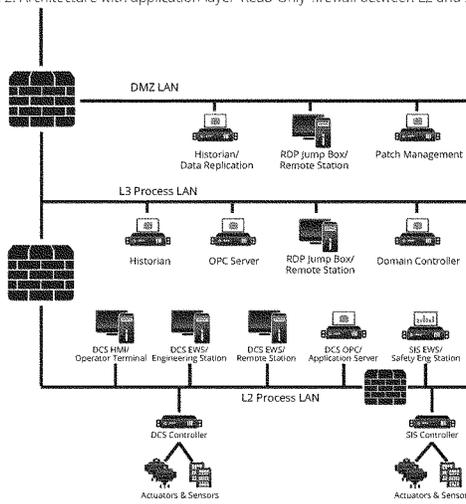


<sup>1</sup> Cyber Security Implications of SIS Integration with Control Networks  
<https://www.automationfederation.org/filestore/af/Logiic/LOGIIC%20SIS%20REPORT%20for%20ISA%20August%2025%202011%20mod%20Jan%202013.pdf>



**TLP: WHITE** information may be distributed without restriction. This architecture can be especially dangerous when combined with engineering remote access. A common practice at many sites is to allow access to the process control network to engineers via the Remote Desktop Protocol. The engineer will most frequently use their corporate workstation to access an RDP jump box inside of the process control DMZ. From there, the engineering may RDP to either the L3 or L2 process LAN. Compromise of this process, either through an infected corporate workstation or theft of the engineer's credentials, can give an attacker access to the L2 engineering systems. In the case of a tightly integrated DCS and SIS, the attacker then has access to all services of the SIS, including the programming service. The attacker may also be able to gain access to the SIS Engineering Station and gain a better understanding of how the SIS is programmed.

Figure 2: Architecture with application-layer 'Read-Only' firewall between L2 and SIS LAN



TLP: WHITE information may be distributed without restriction

Alternate architectures have been suggested. Many security-conscious asset owners will instrument their SIS Controller with a 'read-only' application-layer firewall as shown in figure 2. These firewalls typically support protocols such as Modbus/TCP or OPC and are specifically designed to prevent the assertion of safety outputs from the process LAN. These firewalls will also prevent access to the proprietary configuration services of the SIS, closing that avenue of attack. Placing both the SIS Engineering Workstation (EWS) and SIS Controllers on the secure side of this firewall will prevent easy access to the SIS programming protocols. In this architecture, an attacker who gains access to the L2 LAN will not be able to impact the safety system, unless the attacker also identifies a weakness in the firewall protecting the SIS from the rest of the L2 Process LAN. A downside of this architecture is that an engineer will need to physically access the SIS workstation to make changes to the safety programming. However, SIS programming changes should be much less frequent than normal DCS updates.

Other methods use data diodes or completely separate safety networks which provide data to the DCS via a DC Controller add-on card. These mechanisms further increase security, although in the case of a completely separate safety network, prevent end users from using potentially valuable safety sensor data for ordinary process control.

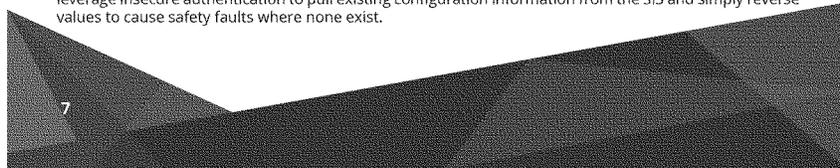
A potential attack on SIS can have multiple implications. Two that immediately come to mind and represent most-likely targets include the following scenarios:

#### Attack Scenario #1: Plant Shutdown

The most likely and operationally easy impact scenario from SIS manipulation or attack is a plant shutdown - and not necessarily due to follow-on physical damage as the result of SIS alteration. There are two general methods of achieving an operational 'mission kill' without physically impacting any element of the target environment:

1. Create operational uncertainty. By altering an SIS where some noticeable effect is produced, even if only recognizing a configuration change or tripping a safety fault where no corresponding physical condition is observed, doubt is introduced into operations as to safety system accuracy and reliability. While the problem is investigated and troubleshooting takes place, operations will likely be significantly reduced if not outright stopped.
2. Trip safety 'fail-safes' to halt operations. Changing underlying logic to enter safety-preserving conditions during normal operations can trip SIS-managed equipment to enter 'fail-safe' modes when such conditions are not actually present. This will lead to a likely halt or stop to the affected process, and likely bring about a much longer shutdown as this scenario rapidly transitions to the item outlined in no. 1 above due to extensive troubleshooting.

Some level of general and plant-specific knowledge is required in order to execute this attack, but the level of knowledge is not as extensive as more fine-toothed, subtle changes to SIS configuration. Simply introducing any noticeable change in the system - which may, through unintended follow-on effects, result in a much more serious issue - results at least in case #1. A slightly more refined approach focusing on specific logic and devices managed can be used to create case #2. Alternatively, an adversary can attempt to leverage insecure authentication to pull existing configuration information from the SIS and simply reverse values to cause safety faults where none exist.



TLP: WHITE information may be distributed without restriction

#### Attack Scenario #2: Unsafe Physical State

Likely the most obvious and assumed attack scenario is creating an unsafe physical condition within the target environment resulting in physical damage to the environment. While this may be the most obvious conceptual attack, the requirements for actually executing make this scenario significantly more difficult – and thus less likely in reality – than scenario #1.

Ensuring an SIS alteration results in physical damage or destruction requires knowledge of the underlying physical processes and controls managed by the targeted SIS. More specifically, knowledge of specific process points where removing a logical fail-safe at the SIS will result in an uncontrolled, damaging physical state – with no complementary physical safety fail-safe in place to prevent damage. The amount of knowledge required specific to the SIS and process installation targeted is significant, and likely not possible to obtain through purely network espionage means. If even possible, the amount of time, effort, and resources required to: obtain necessary environment information; develop and design software tailored to the target environment; and finally, to maintain access and avoid detection throughout these steps all require a lengthy, highly skilled intrusion.

While the above is certainly not impossible – in many ways, it is analogous to the efforts required to launch CRASHOVERRIDE – the combined requirements make this a less-likely scenario attainable only by highly-skilled, well-resourced adversaries with lengthy timelines. Typical operations safety layering, where SIS forms only part (albeit a large one) in overall safety management, should work to mitigate the worst-case damage a destruction scenario in most instances.



TLP: WHITE information may be distributed without restriction

### SIS Defense Status

In theory, SIS equipment is isolated from other operations within the ICS environment, and network connectivity is either extremely limited or non-existent. In practice, operational and convenience concerns often result in more connectivity with other ICS devices than ideal, or that ICS operators may even be aware of. An operator may choose to connect a safety controller to their wider plant network in order to retrieve data from the controller to facilitate business intelligence and process control information gathering. This carries the risk that the safety controller may be affected by malicious network activity, or accessible to an intruder that has penetrated the ICS network.

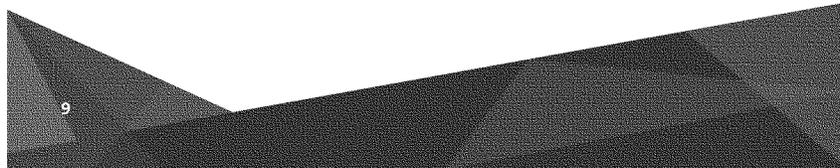
Safety controllers generally have the same security profile as a standard PLC. Controller projects offer password protection; however, projects typically contain two backdoor accounts by default that the user has no control over. While suboptimal from a security perspective, such accounts are vital to ensure administrator-level access and control over the device in an emergency situation. A reverse engineer with moderate skill may uncover these accounts and use them to gain unauthorized access to the project and to the safety controller.

While common to many SIS devices, the newer versions of Schneider Electric's Triconex units are not susceptible to this attack. The older controller (which was deployed at the victim site) is protected by following the deployment recommendations, listed below, to prevent arbitrary changes in SIS functionality via a physical control. Newer model controllers removed the backdoor accounts entirely and added X.509 mutual authentication to the controllers.

Examining SIS devices generally, backdoor accounts cannot typically be disabled due to the operational need for the reasons outlined above. SIS network isolation is critical in preventing abuse of this feature in vulnerable devices it is appropriate to monitor connections to such systems more so than blocking activity without an understanding of the impact.

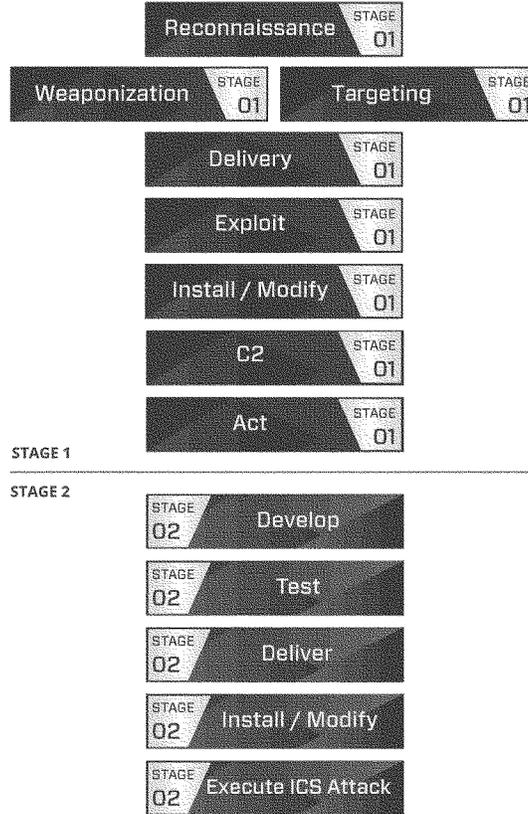
### TRISIS Capabilities

TRISIS is a Stage 2 ICS Attack capability, as defined by the ICS Cyber Kill Chain as shown in figure 3. Given its design and assessed use, TRISIS has no role or applicability to IT environments and is a focused ICS effects tool. As a result, TRISIS' use and deployment requires that an adversary has already achieved success in Stage 1 of the ICS Cyber Kill Chain and either compromised the business IT network or has identified an alternative means of accessing the ICS network. Once in position, the adversary can deploy TRISIS on its target: an SIS device.



TLP: WHITE information may be distributed without restriction

Figure 3: ICS Cyber Kill-Chain



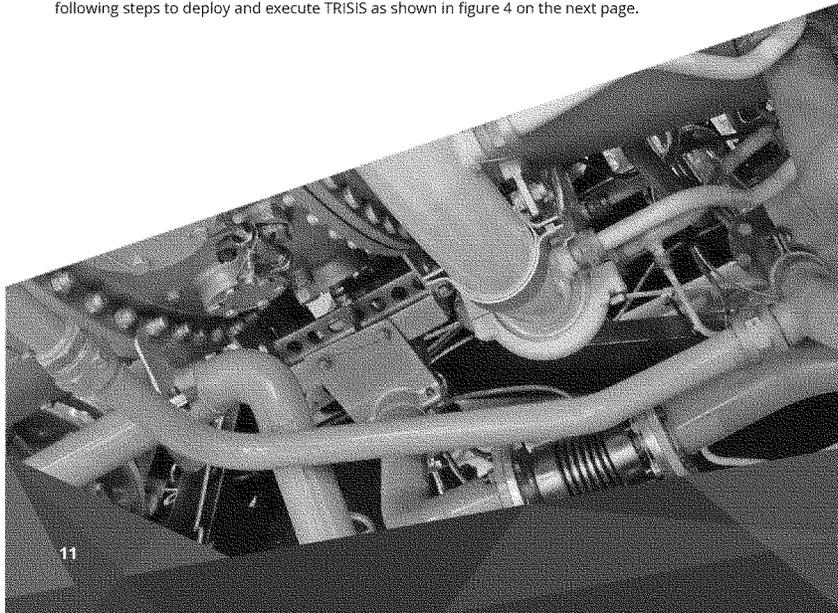
TLP: WHITE information may be distributed without restriction

TRISIS is a compiled Python script using the publicly-available 'py2exe' compiler. This allows TRISIS to execute in an environment without Python installed natively, which would be the case in most ICS environments and especially in SIS equipment. The script aims to change the underlying logic on a target SIS – in this case, a Schneider Electric Triconex device. Subsequent code analysis indicated the script is designed to target Triconex 3008 processor modules specifically. The executable takes its target as a command-line argument passed to it on execution. The implications of this are specifically in targeting at run-time, unless called through an additional script, and based on a review of the code, limiting TRISIS to impacting a single target per execution.

The core logic alteration functionality works through a combination of four binaries that are uploaded to the target SIS:

- Two embedded binary payloads within the compiled Python script.
- Two additional, external binaries that are specifically referenced by name within the script but located in separate files.

Dragos analysis indicates that the embedded items are used to prepare and load the external modules, which contain the replacement logic. As part of a general attack flow, an adversary would need to take the following steps to deploy and execute TRISIS as shown in figure 4 on the next page.



**Completion of Stage 1 of the ICS Cyber Kill Chain:**

Identify and gain access to a system able to communicate with target SIS.

**Stage 2 Develop:**

Identify target SIS type and develop TRISIS with replacement logic and loader

**Stage 2 Test:**

Ensure TRISIS works as intended, likely off network in the adversary environment

**Stage 2 Deliver:**

Transfer TRISIS to the SIS which contains the 'loader' module for the new logic and support binaries that provide the new logic

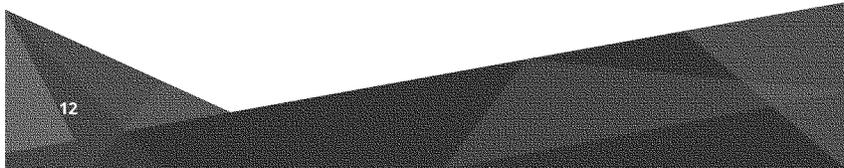
**Stage 2 Install/Modify:**

Upon running the TRISIS executable, disguised as Triconex software for analyzing SIS logs, the malicious software utilizes the embedded binary files to identify the appropriate location in memory on the controller for logic replacement and uploads the 'initializing code' (4-byte sequence)

**Stage 2 Execute ICS Attack:**

TRISIS verifies the success of the previous step and then uploads new ladder logic to SIS

Figure 4: TRISIS Attack Flow



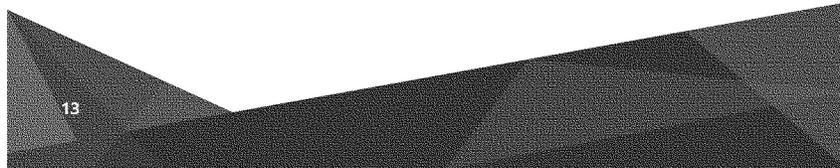
TLP: WHITE information may be distributed without restriction

Based on the description above, TRISIS itself represents a facilitating capability or framework for the actual ladder logic change that has the potential, as outlined in the scenarios above, to alter the environment. As such, TRISIS itself could be repurposed to deliver alternative payloads to either deliver different logic files (the external binaries uploaded by TRISIS to the target SIS) or to utilize differently embedded binaries to target different SIS types entirely. While both are quite plausible, the work involved would be significant and represents the largest amount of effort and required resources for TRISIS efficacy: ensuring that the embedded binaries identify the correct portion of SIS memory for replacement ladder logic upload, and then developing appropriate ladder logic for the target system. Neither of these is trivial, and make scaling or spreading this attack to other environments – and potentially the same Triconex devices but in different installations – extremely difficult.

Dragos was not provided with the external binaries used in the TRISIS attack, and we are therefore unable to determine what precise impact would result on the victim SIS. Nonetheless, any modification to SIS in an operational environment represents a significant risk and potential for damage or even loss of life. The precise attack path is also unknown at this time, but based upon available information and functionality of TRISIS, the target SIS must be network accessible from a device the adversary was able to compromise and establish reasonably persistent command and control over. As a result, TRISIS activity – from initial installation through periodic control followed by ultimate payload delivery – represents multiple steps across Stages 1 and 2 of the ICS Cyber Kill Chain.

While TRISIS as a Python program allows for some level of flexibility in that different modules could be referenced or included to provide different effects, as an attack vector such alterations are difficult to execute in practice for the reasons outlined above. As such, TRISIS is a very focused, target-specific malware that would not be capable of delivering equivalent effects in another environment without significant modification.

An additional point to emphasize is that no real vulnerability or exploit is utilized by TRISIS. Rather, TRISIS functionality depends upon understanding how Triconex SIS devices function and specifics about the process environment. With a full understanding of these items, the adversary then must design and deploy ladder logic to create the desired impact on the target SIS.



TLP: WHITE information may be distributed without restriction

### Implications

TRISIS represents, in several ways, 'game-changing' impact for the defense of ICS networks. While previously identified in theoretical attack scenarios, targeting SIS equipment specifically represents a dangerous evolution within ICS computer network attacks. Potential impacts include equipment damage, system downtime, and potentially loss of life. Given these implications, it is important to ensure nuance in how the industry responds and communicates about this attack.

First, adversaries are becoming bolder, and an attack on an SIS is a considerable step forward in causing harm. This requires the industry to continue its focus on reliability and safety by pursuing appropriate and measured steps towards securing industrial processes. Information technology security best practices are not necessarily appropriate to such situations and an ICS, and a mission-focused approach must be taken into consideration of secondary effects.

Second, the attack of an SIS cannot be taken lightly but should not be met with hype and fear. Eventually, information about this attack will leak to the media and public community. At that point, those in the industrial security community can have a nuanced conversation noting that this attack is not a highly scalable attack that has immediate repercussions to the community. Or simply stated, the public nor government should invoke fear. The industrial asset owner, operator, and vendor community have had a significant dedication to safety and reliability, and now it is obvious that the community is taking steps forward in security. Dragos cautions the community not to use this attack to further other causes as the impact of hype can be far-reaching and crippling. TRISIS is a learning moment to push for more security but in a proper and measured way.

Third, this attack does have implications for all industrial asset owners and operators that leverage SIS. The fact that Schneider Electric's Triconex was targeted should have no bearing on how defenders respond to this case. This was a clear attack on the community. There can be no victim blaming or product shaming that is reasonable nor will it make the community better. The implication is that adversaries are targeting SIS and defenders must live in this reality presented adapting as appropriate to ensure safety and reliability of the operations our society depend upon.

### Defending Against TRISIS

SIS system implementation should begin with relevant vendor recommendations. The recommendations surrounding methods on network isolation are especially critical to preserving SIS autonomy. In the case of TRISIS, Schneider Electric has provided the following recommendations for Triconex Controllers

- Safety systems should always be deployed on isolated networks.
- Physical controls should be in place so that no unauthorized person would have access to the safety controllers, peripheral safety equipment, or the safety network.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All Tristation terminals (Triconex programming software) should be kept in locked cabinets and should never be connected to any network other than the safety network.
- All methods of mobile data exchange with the isolated safety network such as CDs, USB drives, etc. should be scanned before use in the Tristation terminals or any node connected to this network.
- Laptops that have connected to any other network besides the safety network should never be allowed to connect to the safety network without proper sanitation. Proper sanitation includes checking for changes to the system not simply running anti-virus software against it (in the case of TRISIS no major anti-virus vendor detected it at the time of its use).
- Operator stations should be configured to display an alarm whenever the Tricon key switch is in the "Program Mode."

It is important to understand that TRISIS represents only the second stage of the ICS Cyber Kill Chain. This report does not infer or suggest what stage 1 of the attack may be and instead focuses on what has been confirmed through capability analysis. This puts defenders in the position of not stopping activities prior to impact but during or after the SIS impact. Keep in mind there is a wide range of defenses to detect and stop the attacker prior to exposing human safety and equipment during stage 1 and earlier stage 2 phases.



TLP: WHITE information may be distributed without restriction

#### Stage 2 ICS Attack: Delivery

TRISIS requires being executed from a host that can directly communicate with the SIS controller(s). In figure 1 cited above any host on L2: Process LAN can serve this purpose. This allows more options for the attacker and greater scope of what needs to be defended. Delivery of TRISIS to any one of these hosts may be accomplished through network transfer or USB/media transfer.

- Strong architecture can deter, delay or detect adversarial actions as they deliver TRISIS from another network to a host that can communicate to the SIS environment. This is traditional network concepts of segmentation through firewalls, dual factor authentication of interactive access, etc.
- Once architectural foundations are in place, both active and passive defenses are needed. Automated log collection, passive network collection provides the basis of information needed for forensic analysis after an event while strong tailoring of firewalls may limit/prevent delivery or minimally serve as a triggering event for defenses to investigate and respond.

#### Stage 2 ICS Attack: Install/Modification

Once TRISIS resides on a host that has direct access, it is now in a dormant state until either the attacker or unwitting user executes the binary. Once the TRISIS package is on the host, there are several options for the defenders to stop or detect it proactively.

- If the network architecture were already revised to limit what hosts can communicate to the SIS, then the number of hosts that can successfully run TRISIS against SIS has already been reduced. Again, this limits the attacker's options while allowing more focused security controls. Strong mechanisms to limit removable media can be considered- both technical (USB whitelisting or outright disabling of USB ports) or administrative (enforcing scanning of a USB drive prior to usage in production equipment) are valuable. Strong filesystem permissions or execution whitelisting technology become much easier to implement for engineering workstations or hosts that have access to communicate with SIS.
- Reliance on traditional signature-based detection (antivirus) is not sufficient. At the time of discovery, TRISIS was undetected by all antivirus engines. Instead, a more proactive approach is required. For instance, Worldview customers were provided Yara signatures to identify TRISIS. Those signatures also detect any binary compiled with py2exe as any such tool within an ICS or SIS environment is an outlier and immediately suspect.
- Additional proactive baselining can also occur. Hosts such as engineering workstations are often not well managed. They generally are not part of Active Directory and have the option of running a wide range of agents. However, baselining of known files, applications, services, USB insertions, and user accounts can find deviations that could detect TRISIS files on the system. This can offer assurances of the limited number of hosts that can communicate to the SIS.

TLP: WHITE information may be distributed without restriction

#### Stage 2 ICS Attack: Execute

The execution of the TRISIS attack can be broken down into two components: the launch of the process on the host and the network communications from the compromised host to the SIS controller(s).

Architecturally limiting the TRISIS executable to run on the host via execution and/or hampering its ability to communicate to the controllers via windows host firewall would stop any impact.

Additionally, proactive detection – such as identifying when a host is communicating with an SIS controller can serve as an alarm. Even with strong architectures, misconfigurations occur that may allow a host that shouldn't have access to an SIS to communicate to it. Such alarms, even if they fail to stop an attack, are vital to understanding and isolating the cause of the attack.

SIS environments can be some of the most defensible systems. They are largely simplistic and static- usually the most static of any ICS environment. However, good architecture, passive defenses, and active defenses are key to understand when an attack is in progress and how to repel when the attackers use novel techniques. There is no such thing as an undetectable or unpreventable cyber attack, and as defenders, it should be a priority to secure and monitor the safety systems responsible for protecting human life, the environment, and the physical processes.

---

Dragos applies expert human intelligence and behavioral analytics to redefine industrial control system (ICS) cybersecurity. Its industry-first, ICS/OT cybersecurity ecosystem provides control systems operators with unprecedented situational awareness over their environments, with comprehensive threat intelligence, detection, and response capabilities. Dragos' solutions include the Dragos Platform, providing ICS/OT-specific threat detection and response; Dragos Threat Operations Center, providing ICS compromise assessment, threat hunting, and incident response services; and Dragos WorldView, providing global, ICS-specific threat intelligence. Headquartered in metropolitan Washington DC, Dragos' team of ICS cybersecurity experts are practitioners who've lived the problems the industry faces hailing from across the U.S. Intelligence Community to private sector industrial companies.

TLP: WHITE information may be distributed without restriction

## FAQ

### Who Did It?

Achieving a level of confidence on attribution is not as difficult as often positioned. However, achieving a high confidence of attribution can be incredibly difficult without access to a significant set of data or a long period of historical analysis across numerous intrusions into victim environments. Infrastructure attacks are often geopolitically sensitive topics that can carry real considerations between states. In addition, there is little to no value in true attribution (state, agency, or operator identity) to defense teams. In many cases, attribution can actually negatively affect defense teams. Due to the lack of value to defenders and the ramifications of incorrect attribution Dragos does not comment publicly on attribution.

### Is TRISIS a Big Deal?

TRISIS is the fifth ever publicly known ICS-tailored malware following STUXNET, HAVEX, BLACKENERGY2, and CRASHOVERRIDE. It is the first ever publicly known ICS-tailored malware to target safety instrumented systems. For these reasons, it is of significant importance to the ICS community, and it should be analyzed fully to capture lessons learned. The malware is not capable of scalable and long-term disruptions or destruction nor should there be any hype about the ability to leverage this malware all around the community. Attacks on an industrial process that are as specific in nature as TRISIS are considerably difficult to repurpose against other sites although the tradecraft does reveal a blueprint to adversaries to replicate the effort. However, because SIS are specifically designed and deployed to ensure the safety of the process, environment, and human life an assault on one of these systems is bold and unsettling. While fear and hype are not appropriate in this situation, this is absolutely an escalation in the types of attacks we see against ICS and should not be taken lightly.

### Could This Attack Lead to Loss of Life?

Yes. BUT, not easily nor likely directly. Just because a safety system's security is compromised does not mean it's safety function is. A system can still fail-safe, and it has performed its function. However, TRISIS has the capability to change the logic on the final control element and thus could reasonably be leveraged to change set points that would be required for keeping the process in a safe condition. TRISIS would likely not directly lead to an unsafe condition but through its modifying of a system could deny the intended safety functionality when it is needed. Dragos has no intelligence to support any such event occurred in the victim environment to compromise safety when it was needed.

### What are the Indicators of Compromise?

Dragos supplied Yara rules to our ICS WorldView customers to help defenders scope their environments for this or similar malware. However, indicators of compromise (IOCs) are not appropriate in most cases for industrial threats and capabilities. Technical data is often not similar in adversary capabilities between victims. Defenders should instead focus on defense recommendations and the adversary tradecraft and techniques.

TLP: WHITE information may be distributed without restriction

#### **I Do Not Use Triconex Should I Care About TRISIS?**

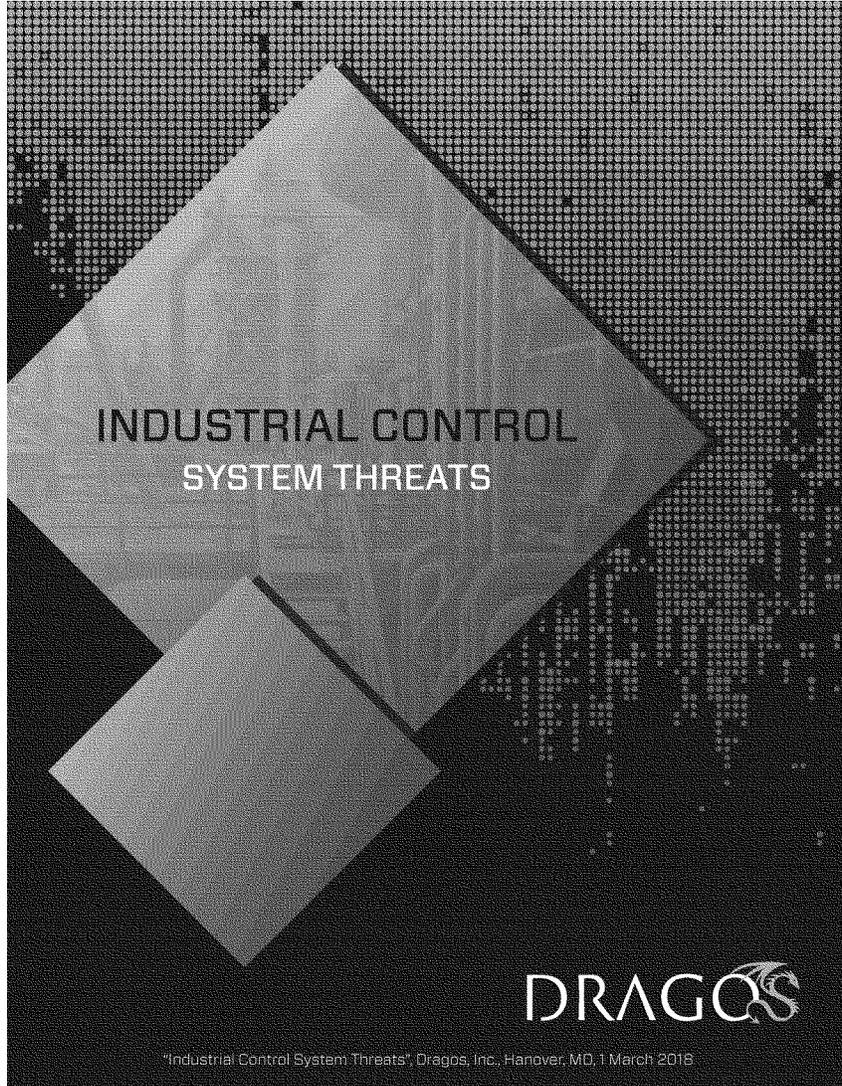
Vendors targeted in specific malware implementations such as Schneider Electric with TRISIS are victims. The malware was not designed because Triconex was a good choice for this attack; the malware would have been designed because the intended victim was using Triconex. If the victim was leveraging a different type of SIS, it is reasonable to conclude the malware would have targeted a different vendor. Therefore, defenders should instead focus on monitoring their environments and being aware of how they have SIS configured if it's deployed according to best practices, and the ability to respond if there was an issue detected with the SIS. The Triconex connection is specific to this malware, but the lessons learned apply to anyone using safety systems.

#### **What Questions Should Executives Ask?**

Executives should ask, and thus their security teams should anticipate these questions, questions such as: Do we have an SIS and if so where and what type(s)? If we needed to collect data from the environment or validate the system has not been modified could we? If the SIS is disrupted is there a cybersecurity component to the processes in place to determine root cause analysis and if an attack has occurred? Do we have an incident response plan that factors in the loss of the SIS even if it does not immediately lead to an unsafe situation? Is our SIS properly segmented off of the network and if not what monitoring do we have in place to ensure it is not impacted?

#### **I Want to Speak on or Write About Safety Instrumented System Security What Should I Know?**

Please ensure you talk to a certified safety engineer. The security of SIS is important, but safety engineering is a very specific skillset. What seems feasible and nuanced from security professionals may not fully represent the reality of the situation. I.e., please avoid sensationalist writing on the subject by including both security and an engineering input. There have been presentations and topics at information security conferences on safety systems before that impress generalist audiences but are known to the community to be inaccurate or simplistic; fantastic research but not holistic in how it is often implemented or discussed. What that translates into is the "what is possible in a given scenario" should have an expert on the threat and an expert on the SIS speaking.



INDUSTRIAL CONTROL  
SYSTEM THREATS

DRAGOS

"Industrial Control System Threats", Dragos, Inc., Hanover, MD, 1 March 2016

**TABLE OF CONTENTS**

**2017: A YEAR IN THREATS . . . . . 01**

**INDUSTRIAL CONTROL SYSTEM THREATS . . . . . 02**  
 2017 ICS THREAT REVIEW

**2017 ICS THREATS . . . . . 03**  
 A SUMMARY

    NEW ICS-FOCUSED MALWARE . . . . . 04  
     TRADITIONAL IT MALWARE CRIPPLING  
     OPERATIONAL NETWORKS . . . . . 04  
     ADVERSARIES STAYING BUSY:  
     ICS-FOCUSED ACTIVITY . . . . . 04

**RECOMMENDATIONS . . . . . 05**

**2017 ICS THREATS IN DETAIL . . . . . 06**

    CRASHOVERRIDE . . . . . 07  
     TRISIS . . . . . 08  
     DISRUPTIVE IT MALWARE . . . . . 09

**ACTIVITY GROUPS . . . . . 11**

    ELECTRUM . . . . . 12  
     COVELLITE . . . . . 13  
     DYMALLOY . . . . . 14  
     CHRYSENE . . . . . 16  
     MAGNALLIUM . . . . . 17



DRAGOS

## A YEAR IN THREATS

2017

2017 represents a defining year in ICS security: two major and unique ICS-disruptive attackers were revealed; five distinct activity groups targeting ICS networks were identified; and several large-scale IT infection events with ICS implications occurred. While this represents a significant increase in 'known' ICS activity, Dragos assesses we are only scratching the surface of ICS-focused threats. 2017 may therefore represent a break-through moment, as opposed to a high-water mark - with more activity to be expected in 2018 and beyond.

While our visibility and efforts at hunting are increasing, we recognize that the adversaries continue to grow in number and sophistication. By identifying and focusing on adversary techniques - especially those which will be required in any intrusion event - ICS defenders can achieve an advantageous position with respect to identifying and monitoring future attacks. This report seeks to inform ICS defenders and asset owners on not just known attacks, but to provide an overview for how an adversary must and will operate in this environment moving forward. By adopting a threat-centric defensive approach, defenders can mitigate not just the adversaries currently known, but future malicious actors as well.

Joe Slowik  
Adversary Hunter | Dragos, Inc.



## I INDUSTRIAL CONTROL SYSTEM THREATS

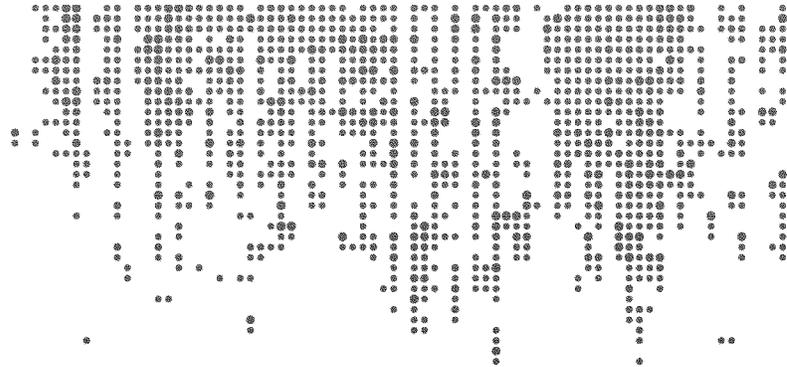
### 2017 ICS THREAT REVIEW

2017 was a watershed year in industrial control systems (ICS) security largely due to the discovery of new capabilities and a significant increase in ICS threat activity groups. Cybersecurity risks to the safe and reliable operation of industrial control systems have never been greater. While numerous, incidental infections occur in industrial networks on a regular basis, ICS-specific or ICS-tailored malware is rarer.

Prior to 2017 only three families of ICS-specific malware were known: STUXNET, BLACKENERGY 2, and HAVEX. In 2017 the world learned of two new ICS-specific malware samples: TRISIS and CRASHOVERRIDE. Both of these samples led to industry firsts. CRASHOVERRIDE was the first malware to ever specifically target and disrupt electric grid operations and led to operational outages in Kiev, Ukraine in 2016 (although it was not definitively discovered until 2017). TRISIS is the first malware to ever specifically target and disrupt safety instrumented systems (SIS), and is the first malware to ever specifically target, or accept as a potential consequence, the loss of human life. The impact of these events cannot be understated.

The number of adversaries targeting control systems and their investment in ICS-specific capabilities is only growing. There are now five current, active groups targeting ICS systems – far more than our current biases with respect to the skill, dedication, and resources required for ICS operations would have us believe possible. These events and continued activity will only drive a hidden arms race for other state and non-state actors to mature equivalent weapons to affect industrial infrastructure and ensure parity against possible adversaries.

We regrettably expect ICS operational losses and likely safety events to continue into 2018 and the foreseeable future.



## 2017 ICS THREATS

### A SUMMARY

2017 featured multiple, concerning developments within the ICS security space. On a general level, wormable ransomware such as WannaCry and NotPetya provided notice to ICS owners and operators that industrial networks are far more connected to the IT environment than many realized. While significant and – for some organizations – costly, 2017 also featured some targeted events led by activity groups focused exclusively on the ICS environment.

Previously, defenders perceived ICS threat actors as rare with significant technical limitations or hurdles to overcome. But 2017 demonstrated – either because ICS is an increasingly enticing target, or because researchers and defenders are merely ‘looking harder’ – that these groups are more common than previously thought. Toward that end, Dragos identified five active, ICS-focused groups that displayed various levels of activity throughout 2017. While only one has demonstrated an apparent capability to impact ICS networks through ICS-specific malware directly, all have engaged in at least reconnaissance and intelligence gathering surrounding the ICS environment.

Overall, the scope and extent of malicious activity either directly targeting or gathering information on ICS networks increased significantly throughout 2017.

As a result of these events, Dragos has been able to analyze and develop strategies for defending and mitigating various types of attack against ICS assets.

## NEW ICS-FOCUSED MALWARE

2017 witnessed a dramatic expansion in ICS security activity and awareness. During the year, Dragos identified and analyzed CRASHOVERRIDE, responsible for the Ukraine power outage event that occurred in December of 2016, and then discovered and analyzed TRISIS, the first ICS malware designed to target industrial safety systems in October. Considering that defenders knew of only three ICS-focused malware samples before 2017 – STUXNET (pre-2010), BLACKENERGY2 (2012), and HAVEX (2013), the emergence and discovery of two more this year indicates that adversaries are focusing more effort and resources on ICS targeting, and those capabilities are expanding.

## TRADITIONAL IT MALWARE CRIPPLING OPERATIONAL NETWORKS

Early 2017 saw the release of the EternalBlue vulnerability (MS17-010) and the subsequent WannaCry ransomware worm. The infection of operational networks with this ransomware and operational disruption illustrated the symbiotic relationship between the two networks. While engineers and operations staff have long held the separation between “business” and “operational” environments as the ICS model, the border is increasingly permeable and therefore operational ICS networks are facing traditional business threats.

Closely following the WannaCry ransomware adversaries launched NotPetya. What was unique is that this was a wiper masquerading as ransomware appearing to initially target Ukraine business and financial sectors. In addition to weaponizing the EternalBlue exploit, NotPetya leveraged credential capture and replay to provide multiple means of propagation, resulting in rapid spreading to organizations well-removed from Ukrainian business sectors. Perhaps the most sobering example is Maersk, which is estimated to have lost up to \$300 million USD while also having to rebuild and replace most of its IT and operations network.<sup>1</sup>

To combat malware infection events such as the above examples, Dragos pursues ‘commodity’, non-ICS-focused malware through the MIMICS project: Malware In Modern ICS Environments. By aggressively hunting for standard IT threats that can pose a specific danger to ICS environments, Dragos works to provide early warning and defensive guidance on potentially overlooked threats.

## ADVERSARIES STAYING BUSY: ICS-FOCUSED ACTIVITY

Dragos currently tracks five activity groups targeting ICS environments: either with an ICS-specific capability, such as CRASHOVERRIDE or with an intention to gather information and intelligence on ICS-related networks and organizations. These groups have remained relatively constant regarding overall activity throughout the year, and Dragos is confident that additional unknown events have occurred.

<sup>1</sup> <https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481875>

## RECOMMENDATIONS

▶ An ICS intelligence-driven approach to threat intelligence is not universal. Indicators of compromise are not intelligence and will not save any organization. Organizations must understand and consume ICS-specific threat intelligence to monitor for adversary behaviors and tradecraft instead of simply detecting changes, anomalies, or after-the-fact indicators of compromise.<sup>2</sup>

### ▶ DETECTION-IN-DEPTH

Just as defense-in-depth is a necessary component of modern cybersecurity, so must detection-in-depth monitoring of behaviors across all industrial control levels but also. Enhanced monitoring must especially include any permeable "barriers" such as the IT-OT network gap. ICS networks are increasingly connected not only to the IT network but also directly to vendor networks and external communication sources leaving monitoring of the IT environments alone entirely inefficient.

### ▶ ASSUME BREACH

Disruptive ICS-specific malware is real, traditional IT threats now regularly cross the "IT-OT" divide, and ICS knowledgeable activity groups are targeting industrial infrastructure directly instead of just the IT networks of industrial companies. Gone are the days of protection via a segmented network – detection is the first component of an assume-breach model – you can only respond to what you can see.

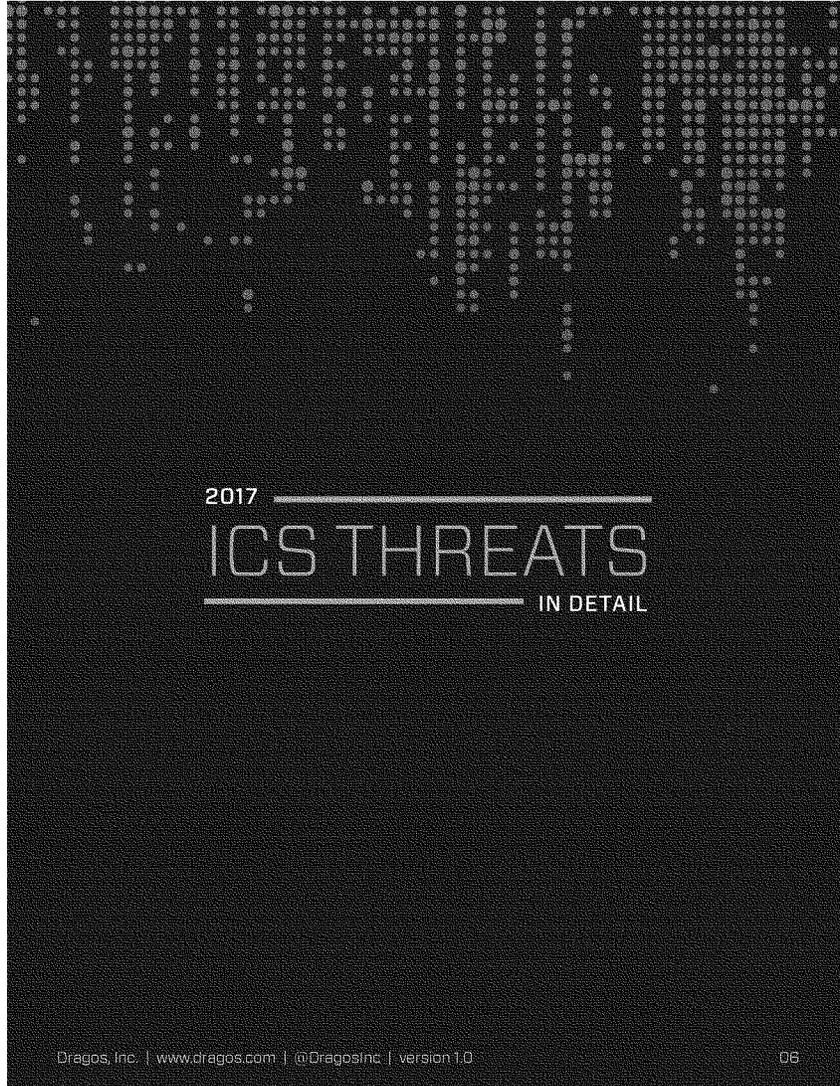
### ▶ ICS-SPECIFIC INVESTIGATIONS

In the event of a breach or disruption there must be ICS-specific investigation capabilities and ICS-specific incident response plans. This is the only effective way of identifying root cause analysis and reducing mean time to recovery in the operations environments when facing industrial specific threats.

### ▶ RESILIENCE AGAINST CYBER ATTACK

Resiliency analysis and engineering surrounding industrial processes must include cyber-attacks. For example, safety systems must be designed and operated with the understanding that they may now be purposefully attacked and undermined.

<sup>2</sup> To understand ICS threat intelligence read the Dragos whitepaper "Industrial Control Threat Intelligence" <https://dragos.com/media/Industrial-Control-Threat-Intelligence-Whitepaper.pdf>



## CRASHOVERRIDE

Although taking place in late December 2016, the ICS security community did not fully understand the extent and significance of the 2016 Ukrainian power outage until later in 2017. After identifying samples, Dragos determined that specifically-tailored malware caused the 2016 event by manipulating the breakers at the target substation in Ukraine.

At the time, this represented only the second instance where malware was utilized to directly impact an ICS device or process with little human intervention – the other example being the Stuxnet worm. In this case, the adversary developed a modular attack framework that combined a reasonably protocol-compliant manipulation program to create an ICS impact (opening breakers to generate a power outage), with malicious wiper functionality to impede and delay system recovery.

Further investigation identified a distinct activity group behind the CRASHOVERRIDE event, as both a developer and attacker: ELECTRUM. As detailed below, ELECTRUM is assessed to be a highly sophisticated, well-resourced activity group that remains active.

Defenders lack any knowledge of CRASHOVERRIDE itself or similar capabilities used after the December 2016 event. While CRASHOVERRIDE, as deployed in the Ukraine attack, is not capable of impacting environments dissimilar to the equipment and protocol setup at the target utility, the framework and method of operations deployed provide an example for other adversaries to follow. Examples of new 'tradecraft' to emerge from CRASHOVERRIDE include: leveraging ICS protocols to create a malicious impact; creating modular malware frameworks designed to work with multiple protocols; and incorporating automatically-deployed wiper functionality chained to an ICS impact.

Thus, even if CRASHOVERRIDE itself cannot be used again outside of very narrow circumstances, the tactics, techniques, and procedures (TTPs) employed by it can be adapted to new environments. By identifying these TTPs and building defenses around them, organizations can prepare themselves for the next CRASHOVERRIDE-like attack, rather than focusing exclusively on the specific events from December 2016 leaving the enterprise open and undefended against even minor variations in the attack.

## TRISIS

TRISIS is the third-recorded ICS attack executed via malware, the previous two being Stuxnet and CRASHOVERRIDE (see above). TRISIS is a specifically-targeted program designed to upload new ladder logic to Schneider Electric Triconex safety systems. The malware utilizes a specially-crafted search and upload routine to enable overwriting ladder logic within memory based on a deep understanding of the Triconex product.

Unique compared to past ICS events, TRISIS targeted safety instrumented systems (SIS), those devices used to ensure system remain in and fail to a 'safe' state within the physical environment. By targeting SIS, an adversary can achieve multiple, potentially dangerous impacts, ranging from extensive physical system downtime to false safety alarms, physical damage, and destruction. Additionally, by targeting a SIS the adversary must either intend or willfully accept the loss of human life from the operation.

Although extremely concerning both as an attack and as an extension of ICS operations to cover SIS devices, TRISIS represents a highly-targeted threat. Specifically, TRISIS is designed to target a specific variant of Triconex systems. Additionally, an adversary would need to achieve extensive access to and penetration of a target ICS network to be in a position to deliver a TRISIS-like attack.

While TRISIS is profoundly concerning and represents a significant new risk for defenders to manage, TRISIS-like attacks require substantial investments in both capability development and network access before adversary success.

While ICS defenders and asset owners should note the above regarding TRISIS' immediate impact, in the longer-term TRISIS is likely to have a concerning effect on the ICS security space. Specifically, while TRISIS itself is not portable to any environment outside of the specific product targeted in the attack, the TRISIS tradecraft has created a 'blueprint' for adversaries to follow concerning SIS attacks. This is not bound to any specific vendor and vendors such as ABB maturely and rightfully stated that similar styled attacks could equally impact their products. Furthermore, the very extension of ICS network attack to SIS devices sets a worrying precedent as these critical systems now become an item for adversary targeting.



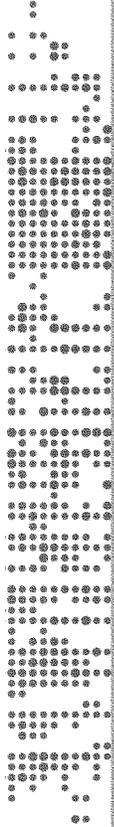
## DISRUPTIVE IT MALWARE

IT malware infecting and causing issues in operational networks is not a new phenomenon. Tracking the metrics related to these infections has always been difficult due to collection issues from these environments. This led to very low metrics, such as the ICS-CERT's consistent ~200 incidents each year, to very high metrics including some vendors claiming upwards of 500,000 infections a year. For this reason, Dragos created the Malware in Modern ICS (MIMICS) project in late 2016 and running through early 2017.<sup>3</sup> The research performed a census-styled metrics count of infections in ICS networks and identified around 3,000 unique industrial infections during the research period. This led to the estimate of around 6,000 unique infections in industrial environments every year including various types of viruses, trojans, and worms. While any of these infections could cause issues in operational environments none represented the type of disruption that would come from the latest generation of ransomware worms.

WannaCry appeared in May 2017 following the weaponization of the MS17-010 vulnerability in the Microsoft Server Message Block (SMB) protocol (EternalBlue<sup>4</sup>), released as part of the 'Shadow Brokers' continual leak of alleged National Security Agency hacking tools. WannaCry itself was a form of ransomware designed to self-propagate via the MS17-010 vulnerability, resulting in not only a quick spread globally but also the systematic infection of networks due to the malware's 'wormable' nature.

<sup>3</sup> To understand ICS threat intelligence read the Dragos whitepaper "Industrial Control Threat Intelligence" <https://dragos.com/media/Industrial-Control-Threat-Intelligence-Whitepaper.pdf>

<sup>4</sup> <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>



While ransomware is typically not a concern for ICS defenders, WannaCry challenged the traditional view due to its self-propagating method exploiting a common ICS communication mechanism (SMB).

Various data transfer functions, such as moving data from the ICS network (e.g., historians) to the business network for business intelligence purposes, rely upon SMB for functionality. Combined with poor patch management and enabling older, vulnerable forms of SMB instead of the newer SMB version 3 variant, hosts within the ICS network were not only reachable through pre-existing connections to the IT network but vulnerable as well.

The result of the above circumstances was WannaCry spreading into and impacting ICS environments, including automotive manufacturers and shipping companies. The impact to operations from system loss due to encryption certainly varies, but in ICS environments the damage potential is significant regarding lost production and capability.

Furthermore, WannaCry was not the only ransomware type to implement worm-like functionality, with additional malware NotPetya and BadRabbit emerging over the course of 2017. Of these, NotPetya was especially concerning for several reasons: first, it included multiple means of propagation through credential capture and re-use aside from relying solely on the MS17-010 vulnerability; second, the malware was effectively a 'wiper' as encrypted filesystems could not be recovered. Although initially targeting Ukrainian enterprises, NotPetya soon spread to many organizations resulting in significant system impacts and, in several documented cases, production losses in ICS environments.

Although not targeted at ICS environments, the impact of WannaCry and related malware demonstrates the capability for IT-focused malware to migrate into ICS environments. While patching may not be a viable solution for ICS defenders in cases such as MS17-010, strengthening and hardening defenses at porous boundaries could help.

---

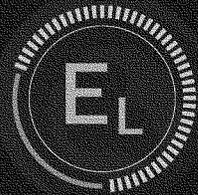
## ACTIVITY GROUPS

---

Dragos tracks and organizes related threat activity as 'activity groups': essentially, combinations of behavior or techniques, infrastructure, and victimology.<sup>8</sup> This process avoids the potentially messy and hard-to-prove traditional attribution route – aligning activity to specific actors or nation-states – while also providing concrete benefits to defenders by organizing observed attackers into collections of identified actions.

Within the scope of ICS network defense, Dragos currently tracks five activity groups that have either demonstrated the capability to attack ICS networks directly or have displayed an interest in reconnaissance and gaining initial access into ICS-specific entities.

<sup>8</sup> The concept of activity groups comes from The Diamond Model of Intrusion Analysis: <http://www.diamondmodel.org/>



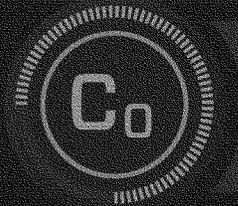
## ELECTRUM

**E**LECTRUM is responsible for the 2016 Ukrainian power outage event, created through CRASHOVERRIDE. In addition to this signature, high-profile event, Dragos has linked ELECTRUM with another group, the SANDWORM Advanced Persistent Threat (APT) (iSight), responsible for the 2015 Ukrainian outage. ELECTRUM previously served as the 'development group' facilitating some SANDWORM activity - including possibly the 2015 Ukrainian power outage - but moved into a development and operational role in the CRASHOVERRIDE event.

While ELECTRUM does not have any other high-profile events to its name as of this writing, Dragos has continued to track on-going, low-level activity associated with the group. Most notably, 2017 did not witness another Ukrainian power grid event, unlike the previous two years. Based on available information, ELECTRUM remains active, but evidence indicates the group may have 'moved on' from its previous focus exclusively on Ukraine.

While past ELECTRUM activity has focused exclusively on Ukraine, information from low-level ongoing events and the group's link to SANDWORM Dragos assesses that ELECTRUM could be 're-tasked' to other areas depending on the focus of their sponsor.

Given ELECTRUM's past activity and ability to successfully operate within the ICS environment, Dragos considers them to be one of the most significant and capable threat actors within the ICS space.



## COVELLITE

**C**OVELLITE First emerged in September 2017, when Dragos identified a small, but highly targeted, phishing campaign against a US electric grid company. The phishing document and subsequent malware – embedded within a malicious Microsoft Word document – both featured numerous techniques to evade analysis and detection. Although the attack identified is particular to the one targeted entity, Dragos soon uncovered attacks with varying degrees of similarity spanning Europe, North America, and East Asia.

Common to all of these observed COVELLITE-related instances was the use of similar malware functionality, including the use of HTTPS for command and control (C2), and the use of compromised infrastructure as C2 nodes.

As Dragos continued tracking this group, we identified similarities in both infrastructure and malware with the LAZARUS GROUP APT<sup>6</sup> (Novetta), also referred to as ZINC (Microsoft), and HIDDEN COBRA (DHS). This activity group has variously been associated with destructive attacks against Sony Pictures<sup>7</sup> and to bitcoin theft incidents in 2017.<sup>8</sup> While Dragos does not comment on or perform traditional nation-state attribution, the combination of technical ability plus the willingness to launch destructive attacks displayed by the linked group LAZARUS make COVELLITE an actor of significant interest.

Dragos has yet to identify another grid-specific targeting event since September 2017 although similar malware and related activity continue. Finally, noted capabilities thus far would only suffice for initial network access and reconnaissance of a target network – COVELLITE has not used or shown evidence of an ICS-specific capability.

<sup>6</sup> <https://www.novetta.com/tag/the-lazarus-group/>

<sup>7</sup> <http://www.novetta.com/2016/02/operation-blockbuster-unraveling-the-long-thread-of-the-sony-attack/>

<sup>8</sup> <https://www.recordedfuture.com/north-korea-cryptocurrency-campaign/>



## DYMALLOY

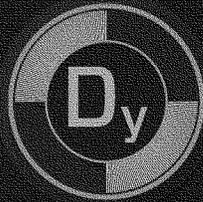
Dragos began tracking the activity group we refer to as DYMALLOY in response to Symantec's 'Dragonfly 2.0' report. Importantly, Dragos found a significant reason to doubt an association to the legacy Dragonfly ICS actor with the newly-identified activity.

Dragonfly was originally active from 2011 to 2014 and utilized a combination of phishing, strategic website compromise, and creating malicious variants of legitimate software to infiltrate ICS targets. Once access was gained, Dragonfly's HAVEX<sup>6</sup> malware leveraged OPC communications to perform survey and reconnaissance activities within the affected networks.

Although no known destructive attacks emerged from these events, Dragonfly proved itself to be a capable, knowledgeable entity able to penetrate and operate within ICS networks.

**D**YMALLOY is only superficially similar to Dragonfly, in that the group utilized phishing and strategic website compromises for initial access. However, even at this stage, DYMALLOY employed credential harvesting techniques by triggering a remote authentication attempt to attacker-controlled infrastructure, significantly different from the exploits deployed by Dragonfly. All subsequent activity shows dramatic changes in TTPs between the groups, such as differences between the content and targeting of the phishing messages, and the outbound SMB connections.

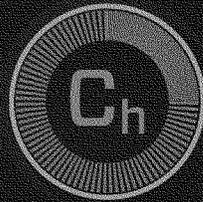
<sup>6</sup> The Impact of Dragonfly Malware on Industrial Control Systems - SANS Institute Whitepaper



Although DYMALLOY does not appear to be linked with Dragonfly, or at least not directly, the group remains a threat to ICS owners.

Starting in late 2015 and proceeding through early 2017, DYMALLOY was able to successfully compromise multiple ICS targets in Turkey, Europe, and North America. Dragos has also learned that, while the group does not appear to have a capability equivalent to Dragonfly's HAVEX malware, the group was able to penetrate the ICS network of several organizations, gain access to HMI devices, and exfiltrate screenshots. While less technically sophisticated than HAVEX, such activity shows clear ICS intent and knowledge of what information could be valuable to an attacker – either to steal information on process functionality in the target environment or to gather information for subsequent operations.

Since Symantec's public reporting, followed by additional US-CERT notifications several weeks later, Dragos has not identified any additional DYMALLOY activity. While analysts found some traces of DYMALLOY-related malware in mid-2017, no artifacts or evidence suggesting DYMALLOY operations appear since early 2017. Given the publicity, Dragos assesses with medium confidence that DYMALLOY has reduced operations or significantly modified them in response to security researcher and media attention.



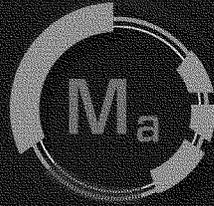
## CHRYSENE

**C**HRYSENE is an evolution of on-going activity which initially focused on targets in the Persian or Arabian Gulf. CHRYSENE emerged as an off-shoot to espionage operations – as well as potential preparation actions before destructive attacks such as SHAMOON<sup>10</sup> – that focused mostly on the Gulf area generally, and Saudi Arabia specifically. CHRYSENE differs from past activity in that it utilizes a unique variation of a malware framework employed by other groups such as Greenbug (Symantec) and OilRig (Palo Alto Networks), with a very particular C2 technique reliant upon IPv6 DNS and the use of 64-bit malware.

Where CHRYSENE mostly differentiates itself is in targeting; all observed CHRYSENE activity focuses on Western Europe, North America, Iraq, and Israel. CHRYSENE targets oil and gas and electric generation industries primarily within these regions. This activity first emerged in mid-2017 and had continued at a steady state since.

While CHRYSENE's malware features notable enhancements over related threat groups using similar tools, Dragos has not yet observed an ICS-specific capability employed by this activity group. Instead, all activity thus far appears to focus on IT penetration and espionage, with all targets being ICS-related organizations. Although CHRYSENE conducts no known ICS disruption, the continued activity and expansion in targeting make this group a concern that Dragos continues to track.

<sup>10</sup> <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>

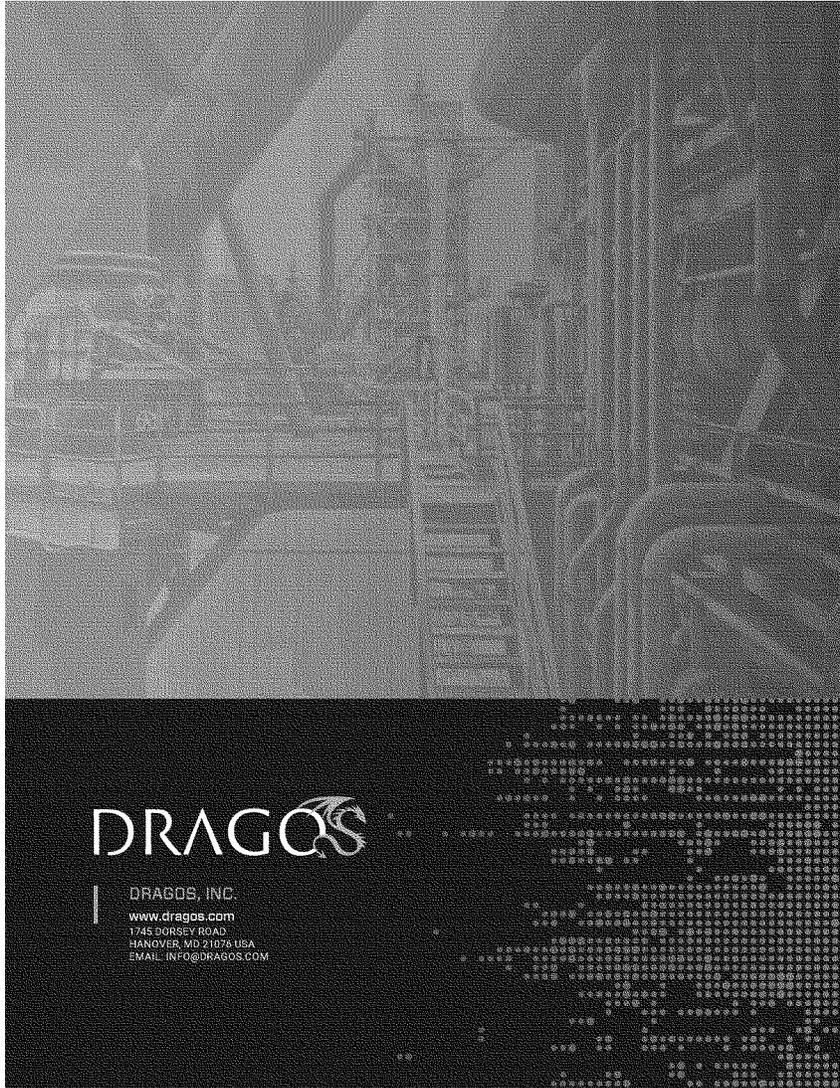


## MAGNALLIUM

**D**RAGOS began tracking MAGNALLIUM in response to public reporting by another security company on a group identified as 'APT33' (FireEye). The press initially treated MAGNALLIUM as a significant threat to ICS and critical infrastructure. A subsequent investigation by Dragos indicated that all of this group's activity focused on Saudi Arabia, specifically government-run or -owned enterprises in petrochemicals and the aerospace industry.

While the group targets organizations which contain ICS, the lack of an ICS-specific capability combined with the group's very narrow targeting profile make this less of a concern.

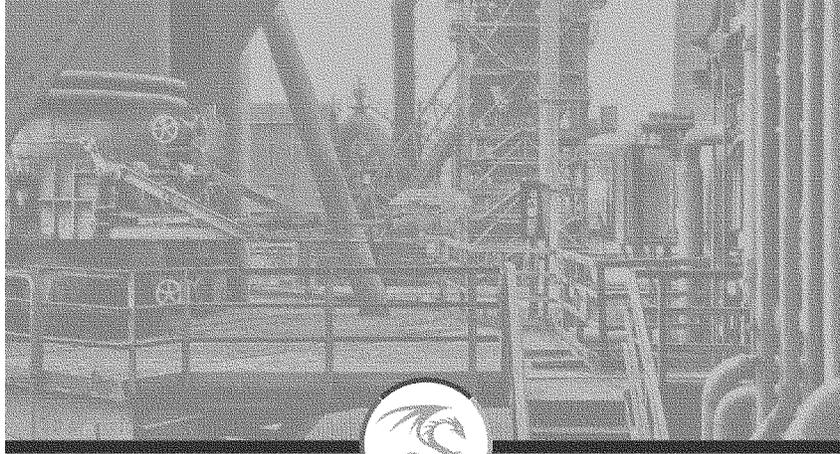
We continue to monitor MAGNALLIUM to determine if targeting changes, or if this group's actions splinter resulting in new, 'out of area' operations, as observed with CHRYSENE.



# DRAGOS

DRAGOS, INC.  
www.dragos.com  
1745 BORSSEY ROAD  
HANOVER, MD 21076 USA  
EMAIL: INFO@DRAGOS.COM





INDUSTRIAL CONTROL  
**VULNERABILITIES**  
2017 IN REVIEW

DRAGOS

"Industrial Control Vulnerabilities: 2017 in Review", Dragos, Inc., Hanover, MD, 1 March 2018

## CONTENTS

2017: A YEAR IN VULNERABILITIES .....	4
KEY FINDINGS .....	5
RECOMMENDATION .....	6
BETTER ICS VULNERABILITY .....	6
RESEARCH WITH STRONGER COMMUNITY .....	6
END USER PATCH APPLICATIONS .....	6
OPERATIONS IMPACT .....	7
ICS VULNERABILITY IMPACT CATEGORIES	
2017 ADVISORIES: OPERATIONAL IMPACT .....	8
PERIMETER IMPACTING VULNERABILITIES .....	9
2017 ADVISORIES: LIKELIHOOD OF ADVISORY IMPACTING	
NETWORK BORDER .....	9
PERIMETER IMPACT .....	9
2017 ADVISORIES: COMPONENT TYPE .....	10
VULNERABILITIES IN FREE/ACCESSIBLE ICS .....	11
2017 ADVISORIES: FREE/DEMO VERSION AVAILABLE .....	11
VULNERABILITY DISCLOSURES OVER TIME .....	12
VULNERABILITIES BY MONTH: OVER 2017 .....	12
ALTERNATE MITIGATIONS .....	13
2017 ADVISORIES: ALTERNATE MITIGATION PROVIDED .....	13



DRAGOS

---

A YEAR IN VULNERABILITIES

---

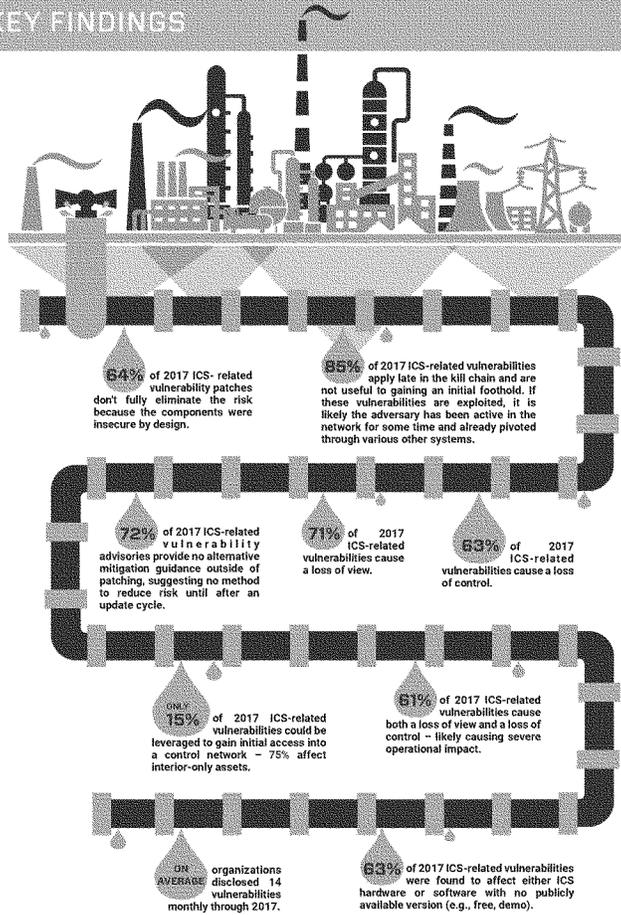
2017

In 2017, Dragos tracked 163 vulnerability advisories with an industrial control system (ICS) impact. Of these, the majority were vulnerabilities in insecure-by-design products which are typically deep within an ICS network.

Dragos found that public reports failed to adequately define the industrial impact of vulnerabilities. Coupled with the fact that most public vulnerability disclosures provide no alternative guidance beyond, "patch," or "use secure networks," Dragos sees huge room for improvement in public disclosure reports – improvement that it strives to make in its own reporting.

Reid Wightman  
Senior Vulnerability Analyst | Dragos, Inc.

KEY FINDINGS



## RECOMMENDATION

### BETTER ICS VULNERABILITY

ICS vulnerability assessments as published are frightfully inadequate to providing asset owners and operators with meaningful guidance.

“Deploy firewalls and use only trusted networks” is not a meaningful suggestion yet is the only alternative guidance provided by most advisories aside from “patch.”

#### RECOMMENDATION

Vulnerability advisories must provide reasonable effective alternative options. Offer several alternatives which may not be applicable to all users but help some. This advice should include specific ports and services to restrict or monitor to reduce risk and impact from an attack, or specific system hardening recommendations to better defend systems from local exploitation.

ICS vulnerability impact analysis is woefully uninformed leading to poor risk assessment by asset owner/operators. For example, a “denial of service” against field devices doesn’t determine if such an attack results in a communications disruption or impact physical function which are radically different risks.

#### RECOMMENDATION

Traditional IT impact assessments are insufficient for ICS/OT environmental risk analysis. Advisories should adopt ICS-specific metrics to better inform users of operational risks.

### RESEARCH WITH STRONGER COMMUNITY

Researchers tend to over-focus on hardware and field devices, and focus little on the network perimeter and entry points to ICS networks. Research thus ignores helping to detect and prevent the critical early stages of an attack.

Industrial-focused advisories ignore common firewalls and VPNs used for both separating ICS networks from the corporate network, and for providing remote access. These firewalls tend to be enterprise IT firewalls, and not ICS-specific, however they are an important protection component of ICS networks.

#### RECOMMENDATION

Advisories should provide broader coverage and include common enterprise devices and applications commonly used in ICS network separation.

Nearly 66% of advisories cover human-machine interface (HMI), engineering workstations (EWS), and Field Device components; historians, OPC servers, and analytics services all provide cross-domain access between Corporate and ICS networks. Mitigating vulnerabilities in these components does little to reduce overall risk, because the components themselves are insecure by design.

#### RECOMMENDATION

The research community should increase scrutiny on cross-domain devices and applications where research outcomes will lead to a stronger first layer of defense.

### END USER PATCH APPLICATIONS

The beginning of 2018 has shown some massive flops in patch production. Major vendors have released patch-sets that triggered failures in end user systems.

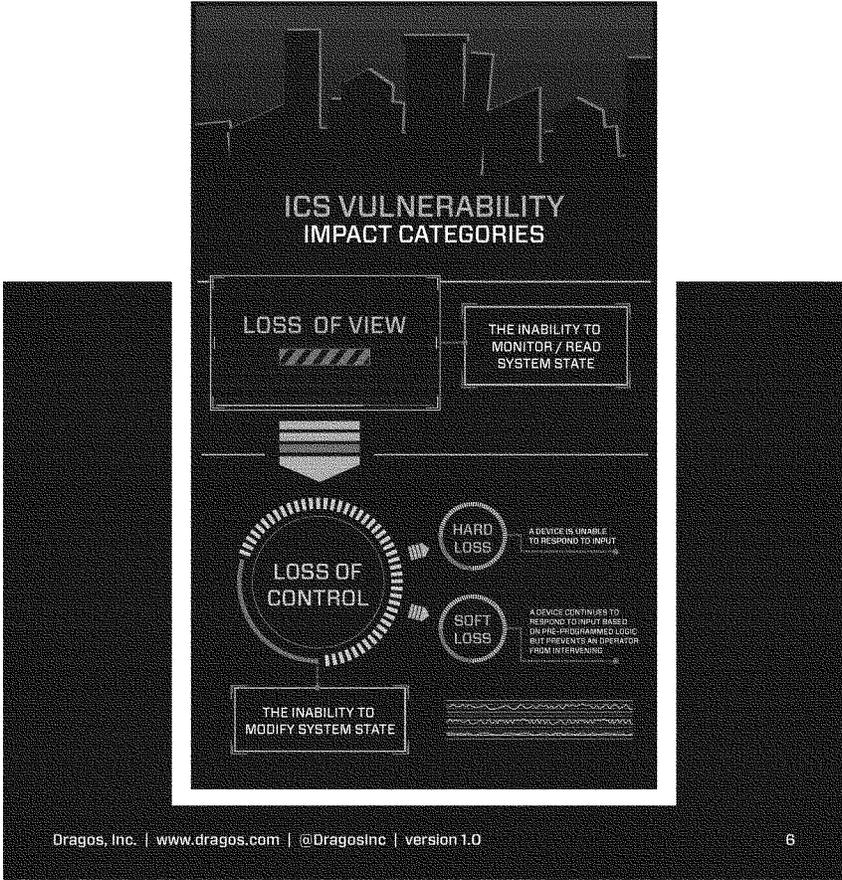
Patches are rarely applied quickly in ICS environments due to concern that the patch may cause an operations outage. Recent patch failures are reinforcing this argument.

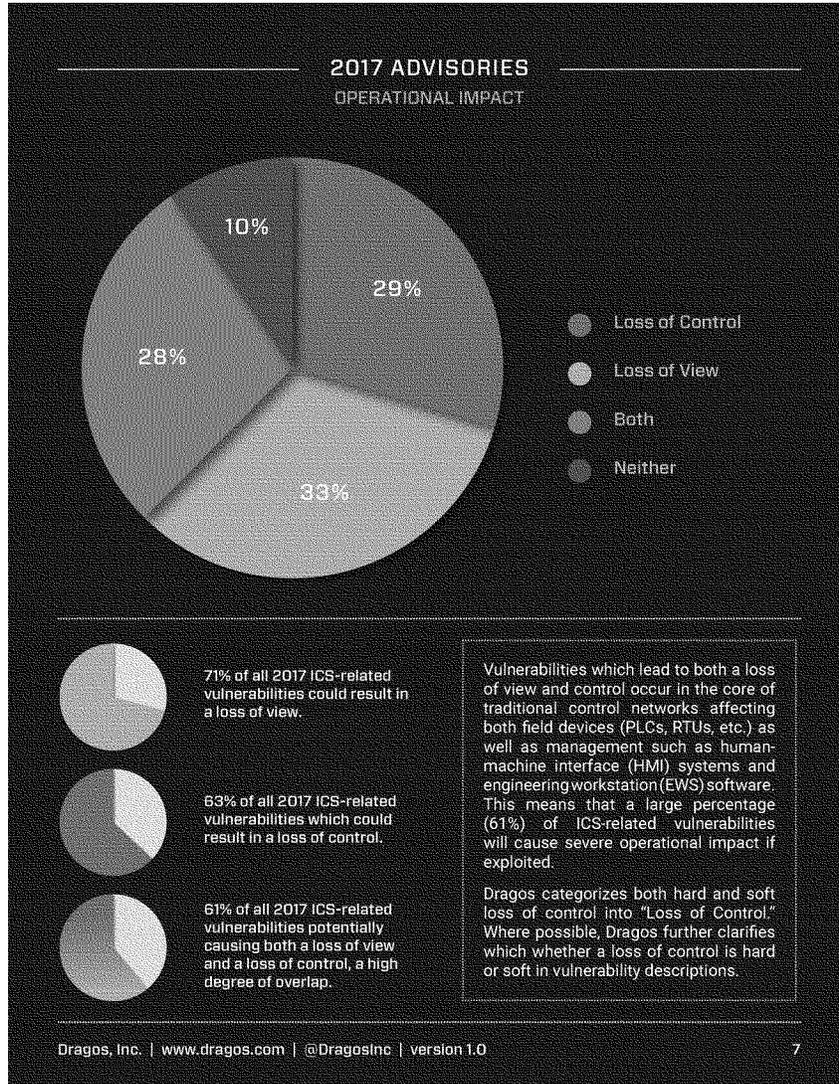
#### RECOMMENDATION

The first step to starting a patch management program must be developing a ‘test’ or ‘development’ control systems network which contains samples of the actual plant’s critical systems. This allows for proper testing of patches, and minimizes the risk of outage of any critical plant systems.

## OPERATIONS IMPACT

Dragos assesses each vulnerability's operational impact on industrial control processes. Specifically, threats against industrial processes result in three impact categories: Loss of View, Loss of Control, or both.



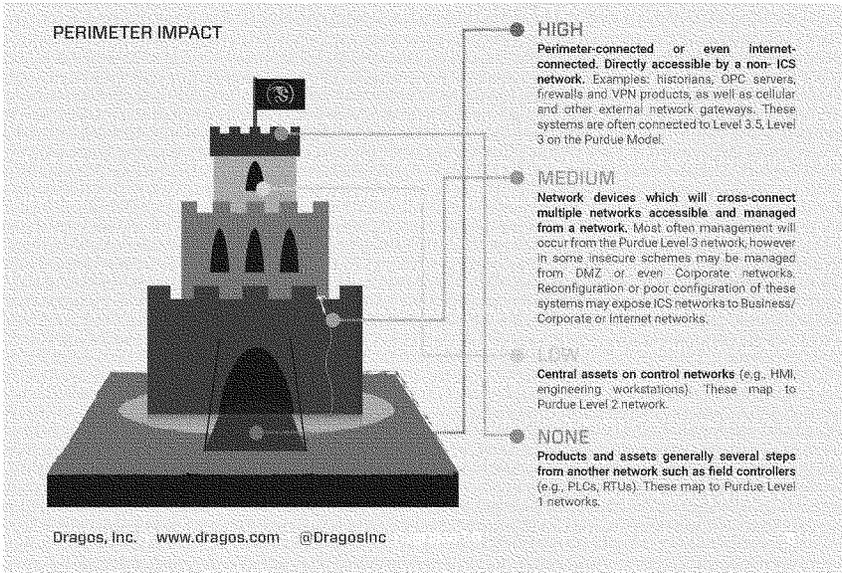
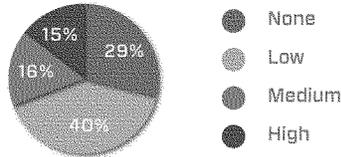


## PERIMETER IMPACTING VULNERABILITIES

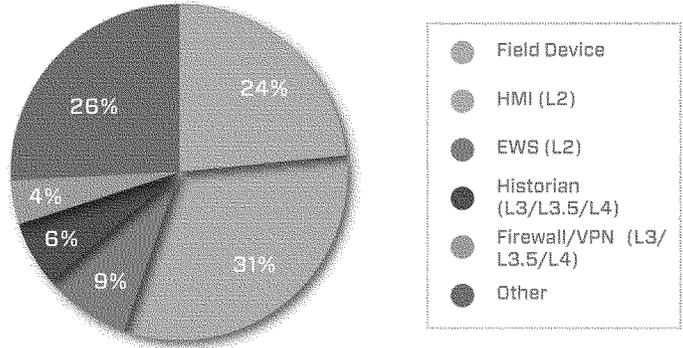
Most industrial control networks exist as separate entities separated from the Internet by the business or corporate network. Even within an industrial control network, devices are layered – with some close or even in the business network while others are deep and more inaccessible. Dragos assesses each vulnerability based on the exposed product’s usual proximity to the ICS network perimeter: high (close), medium, low, and none (far).

### 2017 ADVISORIES

LIKELIHOOD OF ADVISORY IMPACTING NETWORK BORDER



2017 ADVISORIES  
COMPONENT TYPE



The vast majority of vulnerabilities (85%) expose systems unlikely to be used to pivot into an ICS network (proximity: none through medium).



Only 15% of 2017 ICS-related vulnerabilities would be used to gain initial access to a control network (proximity: high).



64% of the 2017 ICS-related vulnerabilities impact interior control systems components (HMI, EWS, or controllers).



26% of all vulnerabilities were reported in field devices (PLCs, RTUs, and other networked controllers which directly read and operate the physical process).

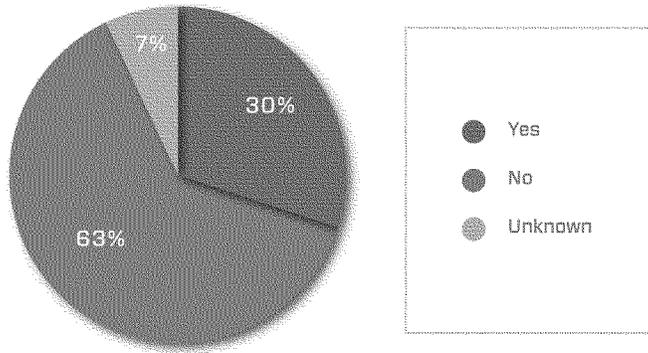
Most of the control system vulnerability patching focus should be placed on the 30% of vulnerabilities which impact exterior-facing systems. Since so many assets and interior control elements are nowhere near a network border, applying patches in the 85% of interior and none-to-medium proximity cases would likely have little to no reduction in risk for impact against attack. However, we caution that this analysis only applies to ICS-related vulnerabilities not underlying traditional operating system patching whose vulnerabilities can lead to worm-like threats and ransomware inside of a control network.

While patching vulnerable field and Purdue layer devices will be rare in practice, and provides little direct benefit due to the insecure-by-design nature of the devices, the sheer percentage of vulnerabilities identified in these devices indicates a decent likelihood of attack should an attacker find its way onto the ICS network. While applying patches to field devices can generally only be performed during a plant outage, providing segmentation such that only valid HMI, EWS, or OPC systems can access the field devices directly, provides a terrific mitigation strategy for defending the interior of the network, should the perimeter be breached. Since accessing the physical process requires sending commands to these controllers, taking a defensive posture can force an attacker to access the HMI or EWS as a step in achieve a process disruption goal. In this way, an end user closes off potential attack vectors to important field devices.

This also highlights the importance of network monitoring at this low level of the network. Since a large amount of security research is performed on these low-level components, it presents a potential source of attack detection via analytics on control protocols – not only in detecting the use of true vulnerabilities in products, but also in the detection of abnormal behavior from the insecure-by-design protocols for manipulating the process.

## VULNERABILITIES IN FREE/ACCESSIBLE ICS

### 2017 ADVISORIES FREE/DEMO VERSION AVAILABLE



63% of all 2017 ICS-related vulnerabilities were found to affect either ICS hardware or software with no publicly available version (free, demo, etc.)

#### COMMON MYTH

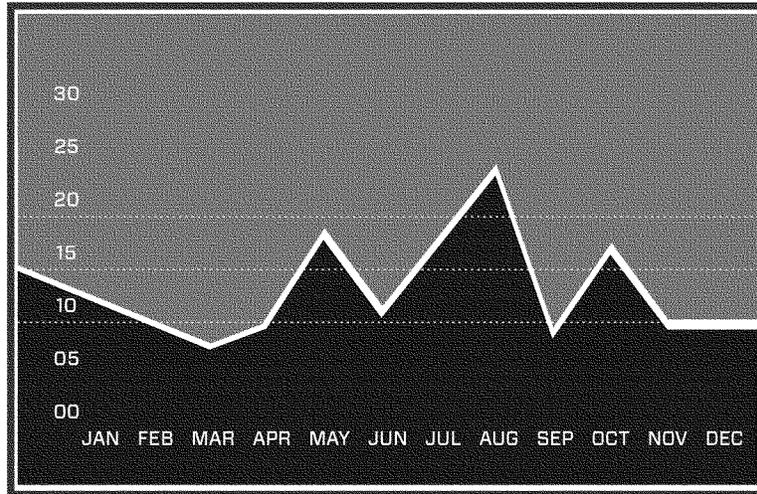
Most ICS vulnerabilities are uncovered in 'Free' and 'Demo' software that is seldom-used in actual control systems.

#### DETERMINATION: FALSE

This means that the majority of 2017 ICS-related vulnerabilities are sourced from hardware or software which had to be procured at cost.

## VULNERABILITY DISCLOSURES OVER TIME

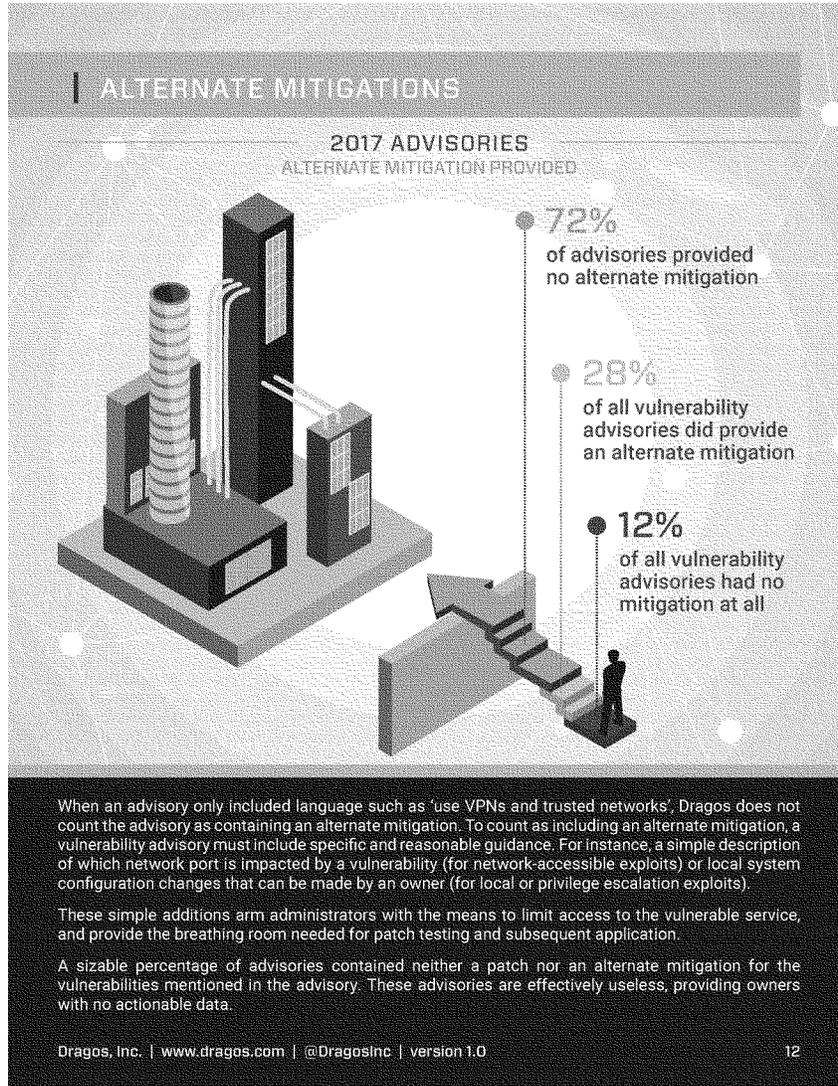
### VULNERABILITIES BY MONTH OVER 2017

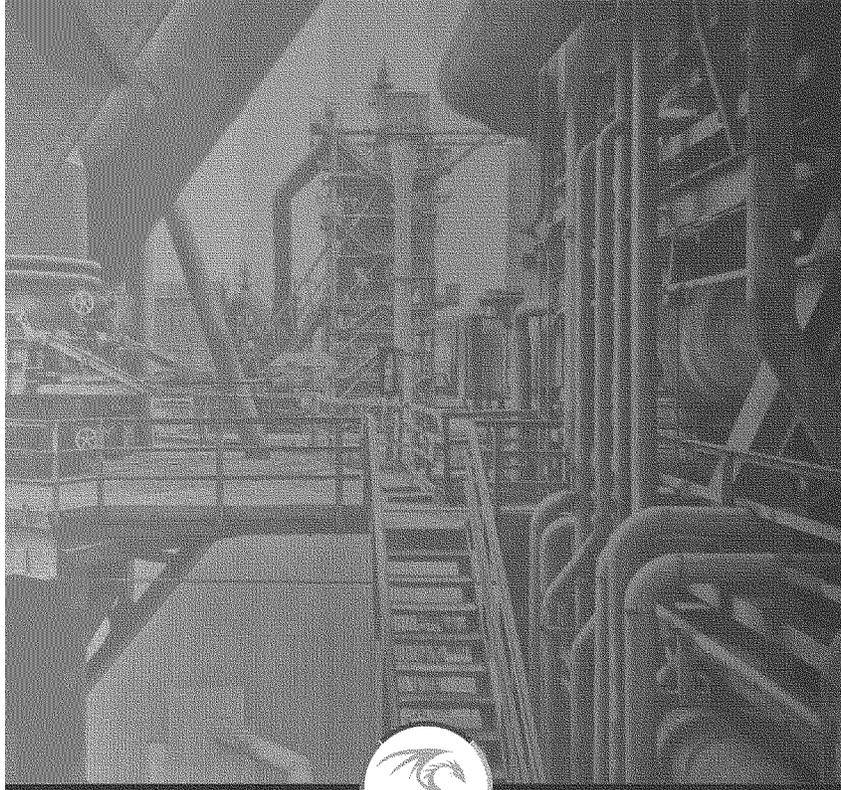


On average, organizations disclosed 14 vulnerabilities monthly through 2017.

Accounting for known conferences and other variables, the disclosure rate remained reasonably flat through 2017.

An increase in ICS-related vulnerability disclosures in July and August most likely coincides with 'conference season' – the BlackHat and DefCon security conferences. This also coincides with the disclosure of MS17-010 impacting Microsoft Windows. Spikes in the Fall season of 2017 coincide with the KRACK vulnerability, when many ICS vendors updated wireless systems.





DRAGOS

Dragos, Inc. | [www.Dragos.com](http://www.Dragos.com) | version 01

1745 Dorsey Road | Hanover, MD 21076 USA | email: [info@dragos.com](mailto:info@dragos.com)

The CHAIRMAN. Thank you, Mr. Lee.

Thank you all. We appreciate your testimony this morning. We will begin with a round of questions.

Senator Cassidy has to go preside in another Committee, so I am going to defer my questions, and you may proceed.

Senator CASSIDY. Thank you, Madam Chair.

Mr. Walker, there is a book, *Black Swan*, by Nicholas Taleb, and one of his premises is that the more complex organizations become, the more vulnerable they become to a black swan event, that which is two standard deviations beyond the norm but just totally brings things down—think the financial crisis of 2007.

Part of your testimony spoke of the interrelatedness of all of our systems. I never pronounce it correctly, MISO or meso, but that network which takes electrons all throughout the middle part of our country. Do we have such increasingly complex energy systems that we are prone to that black swan event, you see where I am going with this?

Mr. WALKER. Yes sir, and thank you for the question, Senator.

I believe that, as I did mention in my testimony, the interdependencies that are resulting through the retirement of many fuel-shored coal and nuclear plants that are being replaced with natural gas plants, has placed a significant interdependency of the electric generation system upon the infrastructure that supplies and supports the gas infrastructure throughout the United States.

And to that end, I have been working with the labs to actually do a single point of failure analysis of the gas infrastructure system in order to understand the overall impact on the generation components that are impacted on the electricity system.

Senator CASSIDY. I hear what you are saying, but the basis of my question is should we fear this interdependency?

Mr. WALKER. I believe we need to understand the interdependency which is why the first goal of my department is the building of a North American, fully integrated model that highlights the interdependencies and is able to do an  $n-1-1-1$  analysis to demonstrate what the interdependencies are and therefore define the complexities to determine what the mathematical, the two-standard deviation impact is away from a secure network.

Senator CASSIDY. I am not sure you are answering my question because it does seem as if within that you acknowledge that we should fear, but you are just trying to prepare us as much as possible to insulate that highly complex system from that two-standard deviation event.

Mr. WALKER. I guess I don't fear it. I need to understand it.

Senator CASSIDY. Got it.

Mr. WALKER. And my—

Senator CASSIDY. Okay.

If I don't get this quite right, ma'am, but Dr. Endicott-Popovsky, I occasionally stutter, so I apologize.

You said everybody is our neighbor, but Mr. Lee said that really we are reasonably, I don't want to misquote or overstate but, secure within the energy sector. But if everybody is our neighbor and we have an Internet of Things and somebody's little modulator on their thermostat back home, can that sneak all the way in and disrupt our grid? And what if that thermostat is in Spain or Mexico

or China, can it similarly do it because from what you said they are our neighbor?

Dr. ENDICOTT-POPOVSKY. When I spoke about everybody is your neighbor in the online world and in cyberspace, I'm speaking in a high level, metaphorically. And theoretically what you're talking about is possible.

Certainly what the gentleman from Dragos was talking about with the adversaries that we face, there are individuals out there that are spending overtime and double time to figure out just those kinds of scenarios. And we should make no mistake, we have allowed, in my opinion, our valuables to sit on a table in the kitchen with our back door open without thinking about what that invites.

And so——

Senator CASSIDY. Now, that is a little bit contra to what you said, Mr. Lee, in which you said, don't sit on laurels, but we are not as quite as incredibly, you know, our valuables are not necessarily on the table, at least when it comes to the energy grid.

Would you accept that or——

Mr. LEE. So, I would not disagree that we are interconnected in a way that opens up new risk, but I think my, sort of, point was the fact that every single thing that occurs gets messed with headlines that everybody is going to die. And I think that does a disservice to the amount of work that the energy community has put into our infrastructure——

Senator CASSIDY. Then that brings me to Dr. Sanders' comment in which you suggest that we are not having this. Implied in your conclusion was that we are not having this academia, industry, government working group to find solutions, are we not?

Dr. SANDERS. So, we are having that. There are, actually funded by the Office of Electricity (OE), there are efforts going on that are combining together academics, industry people and government. Some of the nice programs that have been run by OE, so-called industry projects——

Senator CASSIDY. I am almost out of time so I gather that we are, you just, perhaps, have more of it.

Dr. SANDERS. We are doing it. We need more of it——

Senator CASSIDY. Last thing.

Ma'am, you have raised working group and I had, somehow, in the back of my mind in Washington State that you all had a bill. I don't know if it was implemented, that you would allow computer programming to be used as a substitute for a foreign language requirement in your primary and secondary school. Do I remember that? And if so, was it implemented? And if so, what are the results?

Dr. ENDICOTT-POPOVSKY. I will get back to you with that answer. I recall that that was proposed, but I will get back with you, sir, with that answer.

[The answer to Senator Cassidy's question appears on page 152 at the end of the hearing.]

Senator CASSIDY. Sounds great. It just sounds great to me because no one who ever studied French in school ever learned French, on the other hand, in fact, I am not sure they know where France is.

[Laughter.]

But if they learned how to use even Excel or Python, wouldn't we be better off?

Dr. ENDICOTT-POPOVSKY. I agree that we need to be looking from an educational perspective down into the K-12 arena, absolutely.

Senator CASSIDY. Okay.

Madam Chair, I thank you for deferring.

The CHAIRMAN. Thank you, Senator Cassidy.

Senator MANCHIN.

Senator MANCHIN. Thank you, Madam Chair.

I would just like to say also that Latin was not much experienced later either.

[Laughter.]

I am thinking I had two years in high school and still can't speak a word of it.

Thank you, Madam Chairman and Ranking Member Cantwell, for having this important hearing. I would also like to thank each one of you, the witnesses, for appearing here today.

It is nice to see Congressman Matheson, and we appreciate your appearance here. I believe it is your first in this capacity. During your time in Congress you were known for your bipartisanship which we miss very much. That is one of the many reasons I have no doubt that the Rural Electric Cooperative Association is in very good hands, sir.

We have held several cyber hearings this year, including the Subcommittee on Energy on which I serve as the Ranking Member, alongside Chairman Gardner, as we discussed previously, new digital technologies have increased energy efficiency and allowed for enhanced customer experience. However, increasing our reliance on these platforms also leaves us more vulnerable to cyberattacks. It is not a question of if, but a question of when.

With that in mind, my home State of West Virginia, as all of you know, I think, continues to be a net exporter of energy. That means that our neighbors really depend on us for reliable electricity which coal and natural gas produces on a regular basis. I cannot stress the importance of reliable transmission of energy is our way of life, and I am concerned about our security every day.

I applaud the ongoing work by the Department of Energy and Department of Homeland Security, Mr. Walker, but I also want to make sure we can eliminate our energy sector's vulnerabilities.

As a member of the Senate Intel Committee, I consider these cyber hearings vitally important and I am very, very appreciative that we are having this hearing.

Congressman Matheson, I would ask, what has been the single most helpful strategy or approach for your members to prepare for and mitigate the risk of cyberattack? What do you think that you all have been able to do to assist the Department of Energy and any of our other agencies?

Mr. MATHESON. The answer starts with the word partnership and we've had excellent relationships in terms of working with the Department of Energy and developing, as I mentioned in my opening comments, the program we call RC3, which is a program that we put together to train our co-ops. It's really a toolbox of different options that they can use to do a self-assessment of their cir-

cumstance at their co-op, identify potential vulnerabilities and risks, share best practices with each other.

And it's, sort of, a self-improvement process as well, continuous improvement dynamic because this threat is evolving every day, as we've all discussed, and it's something that we recognize that wherever we are today, we've got to get better by tomorrow. And that's been a significant play for us through these smaller utilities, you know?

Senator MANCHIN. Yes.

Mr. MATHESON. We need a program that recognizes the small, medium-sized utilities and the fact that the Department of Energy recognized as well and help fund this effort.

And I might mention, this effort was not just done with the Rural Electric Co-ops, it was also done with the municipal utilities as well. I think that's been an important program, and that's a specific answer I give to your question.

Senator MANCHIN. Let me say this, I have been told by my utility producers, whether they be electricity by coal-fired for baseload or whether it be our natural gas in all the pipelines, that we are building and pumping stations. I am concerned about the vulnerability. I have been able to go up myself, with maybe just a little gate or a little fence around it.

Mr. MATHESON. Yeah.

Senator MANCHIN. The pumping or our transmission, I would guess. I would ask each one of you, and I will start with Mr. Lee. What keeps you up at night and what are you worried about, because I see vulnerabilities it would not be hard to attack by any of us?

If our pumping stations go down most of the East Coast is in trouble. If our transmission lines go down and our big transfer stations, which are not all that foolproof.

So, if you could tell me, Mr. Lee, what are you concerned about and what do you think we need to do for the next step?

Mr. LEE. Thank you, Senator, for your question.

I'm extremely concerned about the disparity between our industries. So I often like to applaud the electric industry, specifically, but that does not equate to every other industry.

I think the threats are far more, sort of, aggressive than people realize, but not as bad as they want to imagine. And in there is that nuance we have to capture.

I've been in manufacturing facilities, small to medium-sized co-ops, gas locations that are vital to critical communities where not even the basics of security have been done. So, there is this back and forth we have to address.

So I'm concerned about that, and I'm also concerned about some of the smaller events and our ability to respond to them. I'm very confident the U.S. Government has a response if a major cyberattack were to occur.

Senator MANCHIN. Okay.

Mr. LEE. But what about a 30-minute power outage in DC?

Senator MANCHIN. Yes.

Mr. LEE. That's something that brings me, sort of keeps me up at night at how we respond.

Senator MANCHIN. Mr. Walker, if I could go to you real quickly on this. I know we are concerned about the cyberattack and what cyber can do and shut down with a person from far away. I am concerned also about the hardened attack that can occur.

Mr. WALKER. Sure.

Senator MANCHIN. What you all have been doing there and making sure utilities are strengthening their position to protect?

Mr. WALKER. Thank you for the question, Senator.

Specifically, what keeps me up at night in relation to this is the actual physical security component and, to that end, our Department has worked with our security department that does the evaluations of our NNSA sites. We are extrapolating upon the work that has been done extensively by the national labs and our security sites to bring it into and we're using our PMAs which are federally-owned, as the test bed for the proving ground to utilize the physical security strategies, if you will, developed mostly by the Sandia labs to employ them on both the gas, electric and oil infrastructure throughout the United States.

Senator MANCHIN. Thank you.

My time has expired. I wish I could hear from all of you, but if you get a chance, just chime in when you can.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Manchin.

Senator Gardner.

Senator GARDNER. Thank you, Madam Chair, and thanks to the witnesses for being here today.

It is a critical issue, obviously. As we speak, the Colorado Department of Transportation is actually dealing with a cyberattack now. It has gone through several days' worth of a SamSam ransomware attack that has shut down the Colorado Department of Transportation computers within the Colorado Department of Transportation for days.

So this isn't just something that we should worry about for tomorrow. This is something that we should have been worried about a long time ago and were worried about a long time ago and need to worry even more about how we address this today so that we can prevent these kinds of things from spreading even further into hospitals and to roads and to other places.

Thank you for being a part of that solution and bringing these ideas forward, because you were worried about this a long time ago. You are worried about it today and a part of the solution going forward and I thank you for that.

Congressman Matheson, if you don't mind, I enjoyed serving with you in the House. You and I are affectionately referred to as House broken, being in the House and having that experience.

[Laughter.]

But we have talked a lot with our folks back home in Colorado, the co-ops and others, about the challenges they face in cyber.

Would an expedited security clearance process address your need for enhanced background checks and would having more cleared personnel improve the flow of specific additional information? For example, we had a hearing, I believe it was last Congress, where somebody said that they were told by a security audit that they had a piece of equipment that would not pass federal standards,

but they were then told that they could not tell them what that piece of equipment was because they did not have the right clearance.

Mr. MATHESON. Right.

No, you've raised a really important issue and that is the internal threat, the human threat. And what we propose, and it's not just the co-ops of the electric industry in general that feels this way, is we would like access where we could have FBI background check clearance to really check on key employees. Although, the industry is willing to pay for that and we don't even want the information, the personal information, the FBI can keep that, but we would like to have that capacity to have key employees go through that security check process.

I think that would be important risk mitigation for the utility industry and to having better confidence in the people that have access to sensitive information.

Senator GARDNER. Thank you for that.

For those members that do have clearances, do they have difficulty trying to find or accessing classified briefing space? Is that a problem as well or—

Mr. MATHESON. Yeah, there is a question about timing in particular, more than ultimately gain access. And I think that we're always looking to improve, but there's no question that if we could find efforts for timely information to get to us in a way that we can act on it in a reasonable way when we have a threat. That always should be the goal.

And yes, we need to improve—

Senator GARDNER. You can't just pick up the phone, on a regular unsecured line, and talk to the general manager of Highline Electric or something like that.

Mr. MATHESON. You got it.

And we're trying to figure out, you know, this is a two-way street to how this information goes.

Yes, we want access to information from government sources in a timely way where we get that confidential information. We also need to get that information to the government. We want some protections about how that sensitive information is going to be used when it goes in that direction as well.

Senator GARDNER. Great.

Mr. Walker, I have a couple minutes here so I want to get to you as well.

In your testimony, you talk about defense critical energy infrastructure which was defined in the FAST Act. Can you explain what DOE is doing to address Defense Critical Energy Infrastructure (DCEI)?

Mr. WALKER. Thank you for the question, Senator.

The—I want to note that I think it was an astute observation by the Congress to include the DCEI in the FAST Act. Upon taking office in DOE, one of the first things I did was focus in on that point that was raised by the FAST Act.

To that end, I did a significant amount of research—my team and working with members from the Department of Defense, DHS, the Army Corps, RPMAs, particularly WAPA, as well as other members in the key stakeholder groups—we developed a strategy,

an operational strategy, that will enhance our ability to ensure that when those defense critical infrastructure are necessary to be utilized, that they'll be available, notwithstanding what the impact is to the rest of the grid throughout the United States. And we continue to work on that diligently with our federal partners and our industry partners to focus on that.

And if I may, I'd like to comment on the previous question—  
Senator GARDNER. Great.

Mr. WALKER. —to Congressman Matheson.

Earlier this week, DOE, I chair and DHS chairs the Energy Government Coordinating Council and with regard to clearances, one of the things that was a key takeaway from that meeting is the clearance process and getting an expedited process is important, but I think what's more notable and what I focus the organization on, in conjunction with DHS, was we need to provide timely and actionable information to the energy partners that we have in both the ESCC and the ONG.

And it's really about that action, very black and white. You either need to act on this or you don't need to act on that and we need to figure out how to declassify information enough to be able to provide that guidance so that we won't get caught into this clearance issue.

So that's one of the key takeaways that we're working on diligently as well, Senator.

Senator GARDNER. Great. Thank you, Mr. Walker.

Thanks to all of you, and I yield my time.

The CHAIRMAN. Terrific timing, thank you, Senator.

Next, we will turn to Senator Hirono.

Senator HIRONO. Mr. Lee, did I hear you correctly when you responded to an earlier question that we are prepared to respond adequately if there is a major cyberattack? And did you mean a major cyberattack on our energy infrastructure?

Mr. LEE. Yes, ma'am.

So with that discussion, I think that the U.S. Government is more well-positioned on a major cyberattack than it would be on a smaller cyberattack was my—

Senator HIRONO. No, but are you talking about with particular reference to the energy infrastructure that we are prepared to respond so that we can keep our energy infrastructure going?

Mr. LEE. No, Senator.

So, the response is on the private sector. I think the belief structure that U.S. military or others are going to go on civilian networks is misplaced. I'm referring to the geopolitical and, sort of, diplomatic response that we would be able to have.

Senator HIRONO. Well, it is just that I just came from an Armed Services Committee hearing with General Nakasone, who is a nominee to lead NSA and Cyber Command, and he did—now there is general acknowledgement that we have not responded to various, particular state-sponsored cyberattacks on OPM, for example, in other ways.

That is why I wanted to get clarification from you as to exactly what you meant when you said that you thought we were prepared to respond. According to General Nakasone, we are not quite there.

I wanted to further ask you, Mr. Lee. As our control systems become more complex, and you were asked this, and perhaps we have become more vulnerable to attacks. So on the other hand, perhaps, technical advances could potentially make state-of-the-art security technology, we can incorporate state-of-the-art security technology such as advanced encryption algorithms and other measures to protect our systems.

So, in your opinion, is progress being made to ensure that industrial control systems are 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?

Mr. LEE. Thank you, Senator, for your question.

I think it's definitely a race that we're also introducing new risk while they become more verbose in their capabilities. Some systems that were never designed to do certain things now have those capabilities built into them and they shouldn't. At the same time, though, we are making a lot of progress in the sector.

So, I think it is, sort of, in this position where we're increasing risk. We're increasing security, but we have to do more of the security to offset that risk.

Senator HIRONO. I think you also testified that our infrastructure, and I assume that's our energy infrastructure, is quite resilient at this point so that, particularly on the electric side, they have done a lot to protect themselves—

Mr. LEE. Yes, and I think there is still balance there that we didn't have a lot more we need to do, but I think that we should not be so careful, or we should be careful and sort of, just say that they haven't done anything which is inaccurate.

Senator HIRONO. Yes, I understand.

Mr. Walker, you describe the DOE's work with industry in developing the voluntary Cyber Risk Information Sharing Program, or CRISP, as a way of monitoring and managing the security and resiliency of the electric grid.

I would imagine a utility may not be inclined to voluntarily report a cyber incident that may have exposed a weakness in their cybersecurity posture. If they are not required to share that kind of information, how forthcoming do you believe utilities have been in sharing sensitive information relating to cyber risks that they are confronting on a daily basis? And in your view, is there a way to induce and encourage greater participation in programs such as CRISP?

Mr. WALKER. Thank you for the question, Senator.

I believe that the partnership that we have between the electricity sector, Coordinating Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council is extremely strong and it continues to get stronger, particularly as we work through the Government Coordinating Council to integrate that information with DHS.

So I believe the industry is completely forthcoming, just like we are completely forthcoming with that bidirectional flow of information, both classified and unclassified.

You know, this is an ongoing evolution and a partnership that we all understand that we need to work together. The integration

of both the oil and natural gas as well as the electric industry into an overall system of energy that's highly dependent upon each other has driven us to work together over the years and we continue to progress that.

In fact, today we're meeting at DHS for the C-PAC to further work between government and our energy partners.

Senator HIRONO. So the voluntariness of this program is not preventing the utilities from fully participating and cooperating in—

Mr. WALKER. Not at all.

The limiting factor has been the cost of the implementation which is why we've been working very hard. We're going to continue to work hard with NRECA and the APPA to further embed this.

You'll note in my testimony, I said about 75 percent of the utility customers throughout the United States are covered by that. Our goal is, obviously, 100 percent. And we need to work harder, and we are working, to develop cheaper solutions, more cost-effective innovation in our labs for the sensing technology that's necessary to effectuate the CRISP program.

Senator HIRONO. Thank you.

So continuing research in this area is really important and to provide those resources.

Mr. WALKER. Absolutely and we are doing that.

Senator HIRONO. Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator Hirono.

Assistant Secretary Walker, let me ask you this.

With the restructuring and the division now between the Office of Electricity Delivery and now this separate Office of Cybersecurity with its own Assistant Secretary, there would be some that would argue that so much of this is just intertwined, the issues of electricity delivery and energy reliability are not distinct, they are very much intertwined. Then you have the reality that we are talking here about how we can design cybersecurity into every aspect of system operations so that an entirely separate office might be actually counterproductive.

Now I am not saying that I am one of those skeptics, but I do think it is important, as the Committee that is looking at that, that you share with us the rationale for this separate office and the response to those who might say it is a little bit counterproductive to have it separate.

Mr. WALKER. Thank you, Senator Murkowski.

I think that's an excellent question and being part of the decision-making for doing this, I'd like to answer this.

Number one, in taking this position and looking across all of the different departments that I'm responsible for and understanding what was set forth in the FAST Act and really the focus of cybersecurity and given the fact that the FAST Act designated DOE as the sector-specific agency. That is a significant undertaking, and I've done the analysis myself as to what work is necessary.

As I mentioned with Senator Gardner, the DCI component, just that strategy alone and identifying and working through the defense critical energy infrastructure, is a significant undertaking both in breadth and depth.

Now the way I would specifically delineate how the two are intertwined in one concept but very distinct in the others is the whole idea of the CESER program is to be actionable, near-term and highly responsive today. So things like DCI strategies are things that are actionable today and need to be done. However, I would note that the remaining portion of OE that I will be leading focuses on the longer-term solutions so just because we solve and have an operational strategy to make the system work for DCI today, having a longer-term strategy that looks at different R&D capabilities, different design strategies, is really what the focus of the OE Department is going to be.

And I note, Senator Murkowski, I'm taking the opportunity to change the name of my department because both you and I struggle with it every time we're here.

The other part of the OE component which is very, very significant and a massive undertaking is the development of the North American model, an energy sensitive model that is able to do enhanced analysis, to do contingency analysis to understand what the next worst case is when a significant infrastructure, whether it be gas or electric or petroleum, goes offline to be able to do real load following analyses with a high integration of interdependency analysis. That work will drive and fundamentally change the way that we make investments in our infrastructure throughout the entire United States and it will change the way markets are driven and it will change the way that we look at reliability, make investments in operation and maintenance. So that will be work that will be done in that OE Department and that's a significant undertaking that we've laid out the strategy for as well.

The CHAIRMAN. You have your work cut out for you.

I am going to defer my time and go to Senator King and then we will go to Senator Daines.

Senator KING. Thank you.

Mr. Walker, welcome back to the Committee. You were here not long ago, and we are glad to have you back.

Mr. WALKER. Thank you, sir.

Senator KING. Napoleon said, "War is history." Freud said, "Anatomy is destiny." King says, "Structure is policy."

I welcome the new office because I think you are creating a structure that will facilitate good policy in this area because without some area of responsibility in the department that focused, specifically, on the problem of cybersecurity and resiliency, I am afraid the response and the planning and the programs will be diffused and unfocused. So I hope that you will move quickly to facilitate the formation of this office and to get it, to stand it up so that it can meet its urgent purpose.

Mr. WALKER. Yes, sir, that's the goal.

It's important for us which is why the Secretary announced it and, you know, one of the things I learned early in my career is you design organizations around process and how you want to drive the policy. And that was part of the distinguishing factor in establishing this Department, specifically for cybersecurity. And you'll note the second part, which is energy security which incorporates that closely, you know, type, physical component which is abso-

lutely necessary for us to focus on, particularly as the interdependency exacerbates our risk.

Senator KING. Now the problem here—and this is not your problem, this is an all-of-government problem and I just came from a hearing in the Armed Services Committee with the nominee to head Cyber Command—is that this country lacks a coherent strategy of deterrence in the cyber realm. You can argue, we are either at war now or a war is imminent in terms of cyberattacks on this country, small and large. And yet, we have no deterrent policy. Our adversaries feel there is no cost to their attacking us in a variety of ways, large and small.

So, again, this is not your responsibility, but I hope that in the councils of government as you are discussing these matters, we cannot simply rely on defensive measures. We cannot keep patching software.

Ultimately, people who are making a calculation as to whether to attack us have to believe there will be a response, whether in the cyber field or sanctions or some other area, but this is something that I am urging everyone. I don't have the Secretary of Energy or the Secretary of Defense or the President sitting here, so you are it. I hope you will take this message back, because without a deterrent strategy we are simply sitting ducks and there will be, not maybe, there will be an attack unless we can deter our adversaries. I hope you will take that message back.

Mr. WALKER. Yes, sir, I will.

Senator KING. Thank you.

Mr. Lee, you did some analysis on the Ukraine attack, is that correct?

Mr. LEE. Yes, Senator.

Senator KING. Rolling out of the response to that, Senator Risch and I have introduced a bill that is here that essentially is a back to the future bill because one of the learnings, I understand, from the Ukraine attack was that they had some places where there were analog switches and there was human intervention that enabled them to recover more swiftly.

Our concern is that if we are totally digital that there, as you, I think, testified a few minutes ago, there may be unintentional provisions in there that allow us to not be resilient and we have asked the national labs to look at some of these ideas. Is that something that you think makes sense?

Mr. LEE. Thank you for your question, Senator.

And yes, I do. I was actually able to provide some comments to the House companion for that. I thought it was very well positioned. I thank you for your leadership on it. There are a lot of—

Senator KING. I did not know you were going to say that, but I am delighted.

Mr. LEE. Yes, sir. So, teed up.

[Laughter.]

But there is a lot of functionality we're putting in that doesn't make sense. This is not to say we need to go back, sort of, to the Stone Age. We cannot stop innovation and we should not. I mean, a lot of optimizations make sense for the businesses that run, but there are certain locations and certain functions of protection equipment and safety equipment that doesn't need to be able to

run minesweeper and solitaire on it. They can do a more basic function which, in a sense, makes it a much more difficult information and tax base for the adversary.

So I do think it makes a lot of sense in the right application.

Senator KING. Well, I hope we can. I hope, Madam Chair, that is a bill we can move.

Again, talk to the national labs, instruct the national labs to work on this concept of where in the system, not the entire system and not taking it back, but where in the system could we place some of these elements that would be more rudimentary, if you will, but would protect us from a catastrophic cascading of software.

Mr. Walker, I hope that you can, and I am out of time, but I hope that you will get back to us with thoughts as you are standing up this office.

And one of the critical points here is the relationship between the government and the private sector. We don't run the electric grid. We can only help work with the utilities to do so.

And to the extent that there are impediments to full coordination and cooperation, in other words, things like utilities concerns about liability or costs or how do we do this in a way that is not the heavy hand of government, but is a cooperative relationship.

What I am asking you is, if you observe and develop, and I would ask this question also to the electric cooperative and to the utility industry, generally, if there are impediments here, please let us know what they are so that we can try to address them, because this is a crucial issue and it has to be close coordination without smothering is, I guess, the way I would put it.

Mr. WALKER. Sure.

And thank you for the point and I surely, if I run into an impediment, I have not seen one yet, we have a fantastic relationship with EEI, APPA and NRECA and then working through the ONG Coordinating Council and the Electricity Subsector Coordinating Council.

You know, we work through these issues. And the great part about these forums is we've all got the same and similar mission. We approach it from different angles, perhaps, but we've got the mission is to make sure that the energy infrastructure is available when needed. And fortunately, we have great partnerships with those members.

Senator KING. I am out of time, but with the Chair's indulgence, I hope one of your elements of your work will be red teaming so that you can demonstrate to utilities where they have problems.

Mr. WALKER. Yes, we are.

We're taking a very progressive, proactive approach on many of these issues.

Senator KING. Thank you.

Thank you, Madam Chair.

The CHAIRMAN. Thank you, Senator King.

Senator DAINES.

Senator DAINES. Thank you, Chair Murkowski, for this hearing. I know that cybersecurity and the protection of the electrical grid has been an important issue for this Committee, and I hope we

continue to press on it and do find some good solutions to secure our grid. As you all know there are many threats to the grid.

I first want to thank all the witnesses today for working hard to continue to keep the lights on. Mr. Matheson, it's good to have you here today, back on the Hill.

Mr. MATHESON. Thank you.

Senator DAINES. We served together in the House and I have said the rural co-ops when they, the electric co-ops, when they come to my office once a year, I am not sure there is a better organization that represents a true cross section of our state and is closest to I call it, kind of, the real Montana, as our rural electric co-ops. I mean that sincerely.

Mr. MATHESON. And that sure sounds good to me.

Senator DAINES. Yes, but it is true, you know, when in doubt speak the truth, my mom and dad always told me.

Mr. MATHESON. Thank you.

Senator DAINES. I do believe our rural co-ops are on the front line in the defense of our grid, especially in rural states like Montana.

Mr. MATHESON. Yeah.

Senator DAINES. But for the most part the co-ops you represent do not have a lot of excess cash to spend on research or new expensive technologies. And further, there isn't one single solution as we know, in fact, I have quoted Senator King when you said, "There's no such thing as a silver bullet, maybe silver buckshot." I think that is one of the best takeaways I have had in a long time.

Senator KING. Thank you, sir.

[Laughter.]

Senator DAINES. Thank you.

Because co-ops are as diverse as any other business and they span great distances, particularly in rural states like Montana.

Mr. Matheson, do you have examples of some of the efforts that co-ops are doing to address these challenges and how our co-ops in Montana are working to protect local grids?

Mr. MATHESON. Well, thank you, Senator, and you are correct that there is a diverse set of circumstances of the over 900 electric co-ops in America. They're in very different situations. Some are large. Some are small. Some have great dispersed geographic areas. Some are more confined. So it's definitely, there's not a one-size-fits-all. We preach that often within the co-op community.

When it comes to the cyber threat there is one way I would delineate between two categories of co-ops. There are about 120 co-ops in this country that really are connected really in the bulk electric system and that is an area where the need to comply with the NERC reliability standards and cybersecurity standards comes into play. And it's where the real threat to the grid exists, if you will. And those electric co-ops are subject to the NERC audits. They are subject to that regulation. They perform well in that regard and that's where we like to use operational threats, that's where the co-ops have, that set of co-ops, that set of co-ops have dealt with that type of circumstance.

The other co-ops are the smaller distribution co-ops. They're not necessarily directly with the bulk electric system and a lot of the cyber threats that they see are more on the information side, you

know, on the personal information, they're trying to hack in to get a social security number whatever that might be.

And so, in that situation, again, we have large, small but what we try to do is create a peer-to-peer relationship where co-ops can compare, they can consolidate and share assets in terms of taking on these threats because you said some of them don't have a lot of extra money laying around.

And that's really what cooperatives are about. It's in their name. They cooperate with each other. That's how our sectors really try to take on this issue, even across the diverse set of circumstances we have, we have a really coordinated effort to make sure that we're sharing best practices with each other to take on the cyber threat.

Senator DAINES. Regarding the cyber threat, I recently introduced the Cyber SAFETY Act which would, I think, incentivize—

Mr. MATHESON. Yeah.

Senator DAINES. —the private sector and generally we are better off served with carrots versus sticks—

Mr. MATHESON. Yeah.

Senator DAINES. —to incentivize the private sector to innovate and commercialize the next generation of cybersecurity technologies. Could you discuss how that bill might help rural co-ops?

Mr. MATHESON. The rural co-ops and, I might add, the rest of the electric utility sector, support this bill. It's an important bill for a number of reasons.

One is it removes an impediment that was in the original Safety Act from sharing information where before we could share, events had to be described as, declared as acts of terrorism by Homeland Security. And this legislation that you have introduced removes that requirement and it will facilitate greater information sharing between the utility sector and the relevant federal agencies.

The effort to produce more innovation in this area is something we strongly support, and I think it's a step that would go in the right direction.

Senator DAINES. Thanks, Mr. Matheson.

The CHAIRMAN. Thank you, Senator Daines.

Senator Smith.

Senator SMITH. Thank you very much, Madam Chair, for this hearing and thank you, Ranking Member Cantwell. I am just also very much appreciating your testimony today.

Senator Daines, you and I share an interest in rural electric cooperatives, so I appreciate your questions on that as well. Thank you, thanks very much.

I wanted to just touch quickly on a couple of things. By now we have all seen the conclusion of the United States intelligence community that the Russian government has engaged in cyberattacks intended to sway the outcome of our election. We also know that Russia has previously targeted energy systems, twice taking down portions of the Ukrainian grid in '15 and '16. And this is in addition to cyber events taking place in the American energy sector such as the Russian malware that was found on the computer of the Vermont utility. Senator Kaine touched on this with our need for a deterrent strategy for cyberattacks.

But Mr. Lee, I was struck by a point in your testimony that I would like you to elaborate on a little bit where you said, "We do not understand the industrial threat landscape and we do not have enough trained professionals focusing on industrial control cybersecurity." Could you just touch on that briefly and also suggest what, if anything, the Federal Government can do to address this shortage of cyber professionals in the energy sector?

Mr. LEE. Thank you, Senator, for your question.

It comes down to an aspect of collection. So, going back to the co-op discussion. I know of a number of co-ops that have told me, well, we don't have cyber threats in our industrial networks. And I'll ask, well, have you ever collected or looked inside those networks? And the answer will be, well, no. Then how would you know that they're not there because I've absolutely seen nation-state level threats going into those environments. And oftentimes, utilities and others will say, well, I'm not a good threat, but that's the one thing you don't get a vote on. I mean, I've seen adversaries training in those environments, if nothing else.

I think it's important to address that our lack of understanding of that threat landscape translates to also how we are trying to defend against these attacks. A lot of our best practices and standards and regulations are built off of what would be applied to enterprise security networks at JP Morgan and may not be appropriate for an electric utility. So I think there is that balance and we have to understand that collection gap.

One of the things that I think is most important is that workforce development. And this is coming from a technology vendor, I will tell you, the most important aspect is the human. We use technology to, sort of, be a Band-Aid until we get that.

On the human aspect by having better trained professional industrial security, they will be able to make the right decisions for their infrastructure.

We talk about information sharing, but the problem with information sharing is always the ability to action it which is at the utility or infrastructure site.

These professionals that we're training are very critical, not only in K through 12, but also in the professional training that we have out in the industry.

Senator SMITH. So the big issue is, we ought to be focusing on workforce development and that capacity. Okay, thank you very much.

I have just a little bit more time and I would like to address a question to the panel more broadly which is, we are seeing this incredible transformation in the way energy is generated and distributed and delivered in the United States with much more distributed energy resources and smart grid technologies coming online. I am really interested in how this is impacting grid security overall. Is it making it worse? Is it making it better? Could you just or could anybody on the panel feel free to chime in about what challenges or benefits does a more decentralized grid have when it comes to cybersecurity?

Mr. WALKER. I'll weigh in first.

Senator SMITH. Thank you.

Mr. WALKER. I think there's two components to the question.

The first is, the diversity of the portfolio on the generation component, for instance, has and can have the tendency, if it's modeled properly, we understand where it's being placed and if it's strategically being placed, have the benefit of adding security from the standpoint that there's just more diversity and therefore, more iterations to be able to go through.

However, I would offset that by the fact that by adding certain levels of diversity, depending on what they are and the case I'll point to is the heavy reliance due to economic factors on natural gas has now placed natural gas in a place where it's providing a significant amount of generation.

As I noted in my testimony, what that does is it more than doubles the amount of critical infrastructure that has to be protected simply because there's an entire pipeline now that once was, it was a contributing factor, but it wasn't a significantly contributing factor, to the generation of electricity throughout the United States.

Senator SMITH. Dr. Sanders, did you want to chime in here?

Dr. SANDERS. I'll just add very quickly that I think that Mr. Walker spoke well about the diversity in the energy and generation portfolio.

But you brought up, Senator Smith, a very, very important point. Much of the growth of the smart grid is on the distribution side and much of the cybersecurity protections and resiliency that's put in place is in the bulk electric power grid. In fact, NERC and FERC rules only apply on the bulk electric power grid side.

So as we see this very different kind of smart grid, it's the architecture, it's the complexity of the architecture that we need to understand and the kind of point solutions we've had in the past just aren't going to apply.

Thank you.

Senator SMITH. Thank you very much.

And Madam Chair, oh—

Mr. MATHESON. I know we're over time—

Senator SMITH. Yes, please.

Mr. MATHESON. —but just what I said within some earlier comments about we appreciate the fact that there has been an effort and we've received R&D efforts to look at small and medium-sized utilities. We still think that that's an area that merits continued emphasis and your questions have raised another reason why that's the case.

Senator SMITH. Thank you very much.

Madam Chair, I believe I am past my time. Thank you.

The CHAIRMAN. Thank you, Senator Smith.

Senator Cantwell.

Senator CANTWELL. Thank you, Madam Chair.

As former Director of National Intelligence, General Clapper said, "Cybersecurity is now more significant to our national security than terrorism."

So, last year along with all those numerous cyberattacks and breaches, we see that more and more of our economy and critical infrastructure is being attacked. I see everyone nodding here.

Do we have the right threat assessment yet on our grid? Do we have an accurate threat assessment, Mr. Lee?

Mr. LEE. I do not believe so.

Dr. SANDERS. I do not believe so as well. I think that's a capability that's absolutely critical to develop and the maturity models we have today just are not sufficient.

Senator CANTWELL. Anybody else?

Okay, so what do we need to do to get that? Mr. Lee?

Mr. LEE. When it comes to the threat landscape and understanding the threats that pose, I do think private sector is best positioned.

I always hear discussions about security clearances which I think are incredibly important, especially for the strategic level, but I think people are going to be dismayed when they get a security clearance to go in for this magical intel about the industrial threats and be met with nothing or very little. A lot of the insights are in the private sector companies. My insight at my firm today rivals what I have when I led the NSA mission for it. So, I think to do proper work we have to work together.

It's where I do think DOE's CESER will be important, work with the ISAC is important, trying to understand what's going on at the operational layer of the CRISP program as an example is great, but it's for the enterprise networks. It doesn't touch the operations networks and our ability to do that together will give us that threat landscape.

Senator CANTWELL. Dr. Endicott-Popovsky?

Dr. ENDICOTT-POPOVSKY. Yes, I'd like to suggest that the work that the National Guard is doing in Washington State has relevance to your question.

I point to the recent work that they did with SnoPUD and later with a utility in the middle of the state where the Guard cooperated with the utility itself, with the Governor's permission, to go in and do red teaming which is not easy considering that you're working military to the private sector. But that kind of effort, I think, was beneficial to the utility itself where they understood where they were vulnerable when they actually thought they were not.

It puts people in the mindset of the threat actor and one of the things that could help this Committee, going back to some conversation earlier about the threat actors involved, is to understand the evolution and the motivation of the threat actors. Many people still remember War Games and we had this mental model that it's some kid at a computer that's hacking in randomly and causing trouble. We very quickly saw organized crime figuring out that it was easier to log into a bank than to walk through the front doors with a gun and risk life and limb.

And so, monetary motivations are really easy to grasp, but for nation-state actors, it's more complex to figure out what they're after. And that, I think, has made it challenging for the private sector to really think about what's going on because strategically they don't think militarily. They think markets, they think economies but they've never been a military target. And so, now they find themselves as a military target and your strategic thinking has got to be different and this is where those red teaming exercises with the Guard were so helpful. Kilmer's bill is designed to replicate this in Major Lowenberg's name across the country with all National Guards.

Senator CANTWELL. We are finding our whole political system is a target.

Dr. ENDICOTT-POPOVSKY. Correct.

Senator CANTWELL. And so, I think people think that when we sent this letter a year ago that we were trying to echo, maybe, some larger tone about the Russians. We are just dead serious that this is a problem.

Dr. ENDICOTT-POPOVSKY. And it's not just—

Senator CANTWELL. And we are dead serious that we have to come up with a threat assessment and work through it, as you just said. I like the way you described it because you are saying you have to understand what the threat actors' motivation is and then you will understand the potentials and possibilities for attack and what you want to do with it. I see you all nodding there.

Dr. ENDICOTT-POPOVSKY. And it's not just the Russians. It's the North Koreans. It's the Chinese. The Russians, I think, are particularly good at it, but we certainly have a variety of nation-states that raid against our own infrastructure.

And I go back to World War II movies. What did we, as the Allies, take out with the German attacks from our bombers? We went for infrastructure. And now our infrastructure can be breached at a distance. What would you do if you were a nation-state actor? And so, getting your mind in the role of the adversary, I think, is very helpful.

Senator CANTWELL. Yes, Dr. Sanders?

Dr. SANDERS. I think you asked a really excellent question.

I agree with Mr. Lee that we need more data collection. I agree with my academic colleague on the right that red teams can be useful. But I want to emphasize that red teams only can find problems. They cannot give forward-looking assessments.

When we find a problem with a red team we, hopefully, fix that problem. We do not know what our state is going forward.

So exactly what you're asking for is a credible way to assess the situation, to understand the bad guys, to understand the threat actors, but also to understand the users of the system because the users of the system through incorrect use or accidental use will also open up vulnerabilities.

So it's really three things we need to understand: we need to understand the attackers, we need to understand the users of the system and we critically need to understand the architecture of the system because if the system is not perfectly secure then we need to understand how that architecture can create cascading failures or prevent cascading failures. So these three things.

Senator CANTWELL. Mr. Walker, is this something that the Office can achieve? A threat assessment?

Mr. WALKER. Yes, ma'am.

We work with the intelligence communities which DOE is part of and the effort in understanding the different components with regard to CRISP.

One of the things we've already done, and we're in the early stage of development, is the development of a program, an R&D program, called CYOTE which is Cybersecurity for the Operational Technology Environment. So it goes to the OT environment that Mr. Lee was speaking about before.

Much of the work in the past has been spent on the IT side of this. We are now focused on the OT side of this and that will provide us the situational awareness that we need to understand the threat assessment, particularly on the OT side which is where the vulnerability for the energy sector resides the most.

Senator CANTWELL. Do you think this squarely resides at DOE?

Mr. WALKER. I think that it needs to be a partnership between private industry that owns the majority of infrastructure throughout the United States as well as other agency partners that have, particularly on the intelligence side as well as DHS where they have much of the information necessary for us to have a 360-degree view of the vulnerability.

But we could work, obviously, through our EGCC and the ONG SCC to get the oil, natural gas, private sector, as well as the electricity subsector together and working with the energy government side, the coordinating council which I co-chair with DHS, to take this initiative on, move forward and come back with a complete understanding of what we've got, as well as a number of solutions.

Senator CANTWELL. Well, I think, as the witnesses have all said, we need to be serious about this. We need to get the threat assessment done.

Mr. WALKER. Yes, ma'am.

Senator CANTWELL. We need to get an understanding of what our workforce need is from that threat assessment.

What other additional focuses besides just hardening of our infrastructure? What else do we need to be undertaking to make sure that we can continue to grow in the ways that we want to grow in an information age so that we can give our constituents certainty?

I so appreciate it, Madam Chair. Thank you for the extended time.

The CHAIRMAN. Very important questions.

It really goes to the broader issue. If we don't know what our threat is, it is pretty tough to be able to address it and the recognition that knowing what we know now is wonderful, but how are we able to anticipate and project and basically stay one step ahead of those that are looking to be destructive?

I just note that there is a report out this morning from the House Science Committee that describes Russia's extensive efforts to influence U.S. energy markets through divisive and inflammatory posts on social media platforms, not unlike what was going on at the time of the election. I, obviously, have not read this. This just came out this morning but, again, it just speaks to what we are dealing with and the, kind of, the multiheaded issue that it is. How you pin down or can target what that next threat is is anybody's guess here.

I wanted to ask just a few follow-on questions from some of the things that have been raised by members this morning.

This is directed to you, Congressman Matheson. Last Congress when we moved the FAST Act through we gave the Energy Secretary these emergency authorities and we strengthened the information sharing—

Mr. MATHESON. Right.

The CHAIRMAN. —with FOIA exemptions for our critical infrastructure information. Have these FOIA exemptions been helpful?

And then to Senator King's question. He mentioned the issue of liability and the information sharing and how it can be further improved if you have some assurances—

Mr. MATHESON. Sure.

The CHAIRMAN. —that the sensitive information is going to be properly protected and free of liability concerns.

On the liability side of things, is this an area where we need to legislate with that? Are you comfortable with what we've put in place with the FAST Act and the provisions that we have now with regards to the information sharing?

Mr. MATHESON. First on the FAST Act and we were, we, of course, supported the FAST Act as it moved through Congress.

Your question of how it's played out now in terms of the FOIA exemptions, since this Act, since it's been implemented, has been in its infancy. It's a little bit of an open question still.

The CHAIRMAN. Because we don't really know.

Mr. MATHESON. I have no concerns. I'm just saying I can't tell you this is how it's worked in a really substantive way because it's just too new to get that kind of answer.

The CHAIRMAN. Okay.

Mr. MATHESON. But we did support the FAST Act as it was moving through Congress, and we appreciate that it's a law. If we have any issues with it, I'm sure we'll be communicating that back.

On the liability, yeah, look, I think this is an issue where there's always going to be an interestedness looking for opportunities to make sure that information that we pass on to our government partners has some level of protection and the FAST Act clearly addressed some liability concerns that we had and we appreciate that. Am I going to tell you we've got everything off the table now? I'm sure this is going to be an ongoing conversation as we look at going into practice, where we have information transfer and making sure we have appropriate liability protections, that's going to be an ongoing conversation which is going to have to happen.

The CHAIRMAN. Assistant Secretary Walker, on the government disclosure of data, we have the Critical Energy Infrastructure Information, CEII, and this dealing with, basically, the public's right to know certain information and I think we all support levels of transparency. But when it comes to critical infrastructure information, it seems reasonable that we want to be somewhat circumspect here.

Is this an issue where we need to, again, look at FERC and how it is able to release data in the format that it is right now? Is this a policy, given what is going on out there in terms of balancing the need to know with the need to be as secure as possible, is this something that we need to revisit possibly?

Mr. WALKER. At this time, I don't think it is.

I recently had a meeting with our newly confirmed Administrator for EIA with regard to much of the information that is promulgated out through that department on a pretty regular basis. And the reason I had met with her was because of the significant work we're doing with developing this North American interdependency model for the entire energy system. Clearly one of the things that's

been raised as we start talking across the bouncing authorities and the regional coordinators is to protect the flow of information.

That legislation actually enabled DOE to even develop a policy. So we're actually in the process of working through finalization of our policy with regard to the CEII that you noted that was defined in the FAST Act.

So, again, I think the FAST Act provided for a very significant insight into the needed collaboration between Congress and the Executive Branch and all of the partners that really have the purpose of protecting national security.

The CHAIRMAN. Good. Good.

Back to you, Mr. Matheson, and this is as it relates to compliance with mandatory standards. You have said in your testimony that the electric sector today is the only one with mandatory and enforceable standards when it comes to cybersecurity. We have noted that and, in fact, these violations come with some fines, some pretty hefty fines.

Mr. MATHESON. That's correct.

The CHAIRMAN. A million dollars per day per violation is pretty significant.

Mr. MATHESON. Yeah.

The CHAIRMAN. But we also have those who would suggest that our utilities are overly focused on compliance. And so, you have a situation that in an effort to meet the mandatory standards that have been set out and avoid these financial penalties, nobody wants to be paying a million dollars a day per violation, that the electric sector is possibly losing ground because they are focusing on the wrong thing here. They are focusing on checking the box on the compliance, and they miss the goal of cybersecurity protections. Do you think that that is a real concern?

Mr. MATHESON. You know, I would resist that, actually.

The CHAIRMAN. Okay.

Mr. MATHESON. I believe that, you know, this is an industry driven process through NERC to develop these standards. FERC, of course, approves those standards.

Resilience, reliability have always been a concern for the electric industry throughout its history. Cyber is the issue that has evolved over the last several years as part of that now, but no, I don't see any sense where the regulations or the requirements that the NERC process has produced have diverted our attention as an industry from focusing on what's most important.

I'd like to think, instead, it's actually created the focus on what we ought to be looking at. So, yeah, I would disagree with that premise that it has caused some inappropriate attention on compliance at the expense of legitimate cybersecurity efforts.

The CHAIRMAN. Okay, fair enough.

Let me ask you one more question.

Mr. MATHESON. Sure.

The CHAIRMAN. You were asked a question from Senator Daines, specific to Montana and Montana's co-ops, but obviously in my state, pretty small, pretty small entities.

Do you have confidence that our smaller co-ops, our smaller entities, are capable of meeting the cyber challenges? It doesn't make

any difference if you are in Seattle or if you are in Aniak, you still want to be able to rely on your energy grid—

Mr. MATHESON. Absolutely.

The CHAIRMAN. —whether it is a little bit smaller or not. Do you have a level of confidence that our smaller entities are holding up okay?

Mr. MATHESON. Yeah, I do have that confidence. And I'm going to say what everyone else has said in this hearing that this is an evolving threat so we never, even if we're confident today, we still have to work for tomorrow.

I would offer Alaska specific, you know, there are—a lot of our electric co-ops that are isolated. They're microgrids.

The CHAIRMAN. Yes.

Mr. MATHESON. And we have one co-op in Alaska that's right now working on implementing, sort of, a cybersecurity protocol specifically for a microgrid distribution utility.

The CHAIRMAN. We think we are going to pioneer on this and everyone is going to want to come up and see what we are doing.

Mr. MATHESON. I'm all for that.

The CHAIRMAN. Yes.

Mr. MATHESON. Because as we said earlier, every co-op is different and municipal utilities have the same. And so, yeah, I like to think that individually people are recognizing—these are my circumstances, what should I do to take on cybersecurity risk and mitigate in an appropriate way? And I see even smaller co-ops doing just that.

The CHAIRMAN. Good. Good.

One last question and this relates to the workforce. I appreciate what Senator Cantwell raised in her opening statement and the work that you have done, Dr. Endicott-Popovsky, in focusing just on this.

The training is absolutely key and critical. I think we recognize that. I think we know that the training has to go all the way down the chain, those who are making the decision at the top, all the way down to the grid operators at the very, very local level. I wrote down your comment here, Doctor, that you said, "there's no firewall for stupid here." I think we all want to make sure that at the end of the day we have that level of training and skill and expertise all the way down. Are you convinced that we are getting the training all the way down to that local grid operator?

Dr. ENDICOTT-POPOVSKY. I think it's mixed, but I think that is the trend. Every person that participates in some fashion is a potential node in the network that can cause a problem.

I think Mr. Lee had mentioned something about a phishing attack, clicking on a link and causing problems. I mean, this is a very common issue and firewalls don't prevent that. You've got people that need to know not to do that sort of thing. So, you're absolutely right. There does have to be training down through every level.

There are some organizations that are modeling some very effective training. You have to avoid the yada, yada flavor of the month. That happens in many organizations. I take asbestos training. I take this. I take that.

And so, there's some ways to make training vivid and NIST has some guidelines that they've published that are very good at telling

you how to be effective with your training. We use them in our classes.

But somehow you have to get it visceral for people. We could conduct a training here for the Committee, give you a sense of what it's like to be the bad guys. Once you start to think like bad guys, you start to see more things.

I had a student, internationally, one time write me a little note—and I teach things that are safe to teach: operations, business operations—but he wrote me a very telling note, “Why do you people in the West keep emphasizing the technology when the bad guys”—and I'm thinking, how do you know?—“when the bad guys are always looking for the person?”

So, if you put yourself in the role of the adversary, a nation-state, if you have a particularly plum target, something luscious that you can't resist. What lengths would you go to to violate that system? How important is that to you? It's a completely different mindset. We have to be right every time. They only have to be right once. So it's a daunting problem and we have complex systems and lots of participants. I don't think we can expect to get it right every time. I think we have to recognize vulnerabilities and risk. But awareness is the beginning.

The CHAIRMAN. Yes.

Dr. ENDICOTT-POPOVSKY. I'd be happy to provide some materials, if you're interested.

The CHAIRMAN. I think it would be helpful for the Committee.

Dr. ENDICOTT-POPOVSKY. It's a passion of mine.

The CHAIRMAN. I can tell and that is appreciated.

Senator Cantwell, did you have any follow-on?

Senator CANTWELL. I want to thank you.

The CHAIRMAN. I want to thank each of you. I think your testimony has been very, very important. We have had a very important discussion today, and we will look forward to additional input for the record as some have promised.

We will look forward to working with you, Mr. Walker, in this capacity here with a very keen focus on cyber.

I will note the Committee's appreciation for your attendance here, Mr. Lee. Not only have you given us good insight, but I'm told that your wife is expecting and has been expecting to deliver for quite some time—

[Laughter.]

—and that your appearance here today was made possible because hopefully, hopefully, she is going to have this labor—

Mr. LEE. Today.

The CHAIRMAN. —commence—

Mr. LEE. So, she's amazing.

The CHAIRMAN. —soon—

[Laughter.]

—after you are excused from this table. So hopefully if she is watching now, she's got the go ahead—

[Laughter.]

—and she can deliver a beautiful baby safely into the world. We congratulate you on that.

Mr. LEE. Thank you.

The CHAIRMAN. You have always got to end the Committee on a happy note, so thank you all.

Dr. ENDICOTT-POPOVSKY. Madam Chairman, I have a question.

The CHAIRMAN. Doctor?

Dr. ENDICOTT-POPOVSKY. I did get a real-time update on Senator Cassidy's question about the potential change in the language requirements for K-12 in the State of Washington. They are still considering computer language as a substitute for foreign language. The original bill died, but there's still residual interest in that concept, and it's being studied throughout this year. And apparently, we're going to be meeting with the Office of Superintendents here sometime in the near future to discuss this issue. So can you pass that on to him?

The CHAIRMAN. We will share it with him and others as well.

Dr. ENDICOTT-POPOVSKY. Alright, thank you.

The CHAIRMAN. We appreciate that.

Thank you all.

The Committee stands adjourned.

[Whereupon, at 11:53 a.m. the hearing was adjourned.]

**APPENDIX MATERIAL SUBMITTED**

---

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

QUESTIONS FROM CHAIRMAN LISA MURKOWSKI

- Q1. **North American Info. Sharing** – How does DOE work with Canada and Mexico on energy issues related to cybersecurity? Do we have good information sharing efforts among our North American neighbors?
- A1. The Department of Energy (DOE)'s objective for cybersecurity is to minimize the vulnerability of facilities, systems and networks by creating a resilient environment that prevents, deters and detects cyberattacks in the energy sector. International cooperation plays an integral part of this mission. Ensuring the reliability and security of energy systems across North America is essential to the United States' national security and economic well-being.

Electricity, liquid fuels, and natural gas cross U.S. borders with Canada and Mexico at many points and in large quantities each year. In the case of the United States and Canada, there are more than 80 transboundary pipelines and more than 30 electricity transmission lines that transport crude oil, refined products, natural gas, and electricity. Between the United States and Mexico, there are currently 15 cross-border natural gas pipelines, seven petroleum product pipelines, and 11 electric transmission lines.

DOE works with Canada and Mexico bilaterally and trilaterally on issues and information sharing related to cybersecurity, as follows:

Bilaterally, in March 2016, the United States and Canada pledged to enhance efforts to develop a joint strategy for strengthening the security and resilience of the electric grid. Since that time DOE, the U.S. Department of Homeland Security (DHS), Natural Resources Canada (NRCan), and Public Safety Canada have been instrumental in the development of the Joint Strategy and each nation's corresponding Action Plan (released in December 2016) and implementation of their respective Action Plan initiatives. The Joint Strategy and Action Plans rely on existing strong bilateral collaboration between the United States and Canada to address the vulnerabilities of the two countries' respective and shared electric grid infrastructure.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

On January 7, 2017, DOE, the Federal Energy Regulatory Commission (FERC), Mexico's Secretariat of Energy (SENER), Mexico's Energy Regulatory Commission (CRE) and the National Center of Energy Control (CENACE) signed a non-binding foundational document that will support a continued effort by both countries to assure reliability of our electricity grids. On March 8, 2017, the North American Electric Reliability Corporation (NERC) signed a Memorandum of Understanding with CRE and CENACE establishing a framework for a cooperative relationship between Mexico and NERC to enhance reliability of the grids in Mexico and the United States.

With regard to bilateral nuclear security cooperation with Mexico, DOE's National Nuclear Security Administration (NNSA) supports two or three workshops annually on nuclear security topics such as cybersecurity for nuclear facilities, physical protection, and nuclear security culture.

Trilaterally, the Canadian and Mexican governments and electric industry officials are invited to participate in joint Energy Government Coordinating Council (EGCC)/Electricity Subsector Coordinating Council (ESCC) meetings, hosted by DOE's Office of Electricity Delivery and Energy Reliability (OE) three times a year.

The EGCC serves as the principal liaison between DOE and other U.S. Government (USG) partner agencies to discuss and collaborate on energy infrastructure security issues. Canada is a standing member. The ESCC serves as the principal liaison between the USG and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to national-level disasters or threats to critical infrastructure. Canada is a standing member; Mexico is not. Both Canadian and Mexican government and electric industry officials are invited to the meetings.

Canada also is a standing member of the United States' Oil and Natural Gas Sector Coordinating Council (ONG SCC), and is invited to meetings held three times a year. The ONG SCC serves as the principal liaison between the USG and representatives from oil and natural gas companies and major trade associations on matters of oil and natural gas physical and cyber security.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

DOE Emergency Authority Rulemaking

- Q2. DOE recently issued the final rule specifying procedures to implement DOE's new authority to issue emergency orders to industry and NERC for grid security emergencies. The effectiveness of this authority will require close coordination. What is DOE's plan to work with industry and NERC to ensure this coordination?
- A2. Collaboration with owners and operators is critical to ensure emergency orders result in the safe and effective operation of the electric grid. To the extent practicable, DOE will promptly alert all stakeholders impacted by grid security emergencies through existing alert mechanisms, such as the NERC alert system and Electricity Subsector Coordinating Council (ESCC) communication coordination processes. If the situation permits, DOE will then consult directly with industry on the types of orders that can or should be issued.

After the Secretary issues an emergency order, the Department will communicate the order's content to the entities subject to the order. Should the Secretary issue such an order, the order itself would set out the requirements and procedures for impacted entities to seek clarification or reconsideration of the order. Since there may be occurrences where the consultative process is not feasible, the Department is also researching options for how to make implementation of orders more flexible in extreme hardship cases.

Cybersecurity Risk Information Sharing Program

- Q3. Can you discuss the further opportunities that exist for the Cybersecurity Risk Information Sharing Program (CRISP) or other platforms DOE may be working on, to use real time data to improve not only cybersecurity, but also the cyber resiliency that Dr. Sherman spoke to in his testimony?
- A3. The Office of Electricity Delivery and Energy Reliability (OE) is working with the Electricity Information Sharing and Analysis Center (E-ISAC) to grow industry participation in CRISP, upgrade CRISP technologies and devices to enable enhanced two-way information sharing, improve performance, and reduce costs. DOE is enhancing analysis by working to integrate CRISP data into the Intelligence Community Information Technology Environment (ICITE; pronounced "eye sight"). ICITE provides a common platform for the Intelligence Community to easily and securely share analytic

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

tools and technologies, information, and resources. This will help to identify emerging threats and potential mitigations before utility information technology (IT) networks are widely infiltrated.

OE is also working on other platforms as follows:

- Cyber Analytics Tools and Techniques (CATT) will improve the speed, value, and cost of CRISP analysis, reports, and mitigations. It will improve IT threat detection by adding new analytic tools and capabilities to the CRISP platform (working with the Pacific Northwest, Idaho, Oak Ridge, and Argonne National Laboratories). It will also better leverage U.S. intelligence capabilities by enabling direct analysis of CRISP data in secure government storage (ICITE) using unique and sophisticated intelligence tools.
- Cybersecurity for the Operational Technology Environment (CYOTE) is a pilot program focused on the analysis of operational technology (OT) infrastructure information to analyze the cybersecurity risk factors. This complements the existing CRISP program, which only focuses on the security of IT networks. Four utilities are participating in this pilot.
- The Next Generation CRISP initiative will capitalize on the existing CRISP experience and concepts by integrating the latest available technologies and architecture, through innovative partnerships with the energy sector, to provide the enhanced cyber protection. This initiative will address the security needs of both IT and OT infrastructures, beyond the existing CRISP effort which is IT-centric. DOE's vision is to dramatically increase CRISP's footprint across the energy sector infrastructure and to provide a near-real-time capability for energy owners and operators to voluntarily share cyber threat data, analyze the data, and receive machine-to-machine mitigation measures.
- To increase cybersecurity and cyber resiliency, we must accelerate information sharing to enhance situational awareness and better detect and defend against sophisticated cyber

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing:** *Private Sector and Government Challenges and Opportunities*  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

threats within the energy sector infrastructure. The energy sector must have the ability to continue critical energy delivery functions, even during a cyberattack. DOE is working with the energy sector to enhance the sector's day-to-day operational capabilities to share cyber incident information, complying with legal restrictions placed on the sharing or use of cybersecurity incident information and cyber risk indicators and improve organizational and process-level cybersecurity posture.

Increasing cyber-threat information sharing techniques will give the energy sector a better opportunity to detect, deter and prevent an attack. Tools are being developed under the Cybersecurity for Energy Delivery Systems research and development program to address resilience issues so that the utility systems can survive the cyber incidents while continuing to operate the electric system.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing:** *Private Sector and Government Challenges and Opportunities*  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

QUESTION FROM SENATOR RISCH

- Q1. What is the federal government doing to expand security clearances to the private sector down to the analyst level and address the backlog in the security clearance process?
- A1. DOE, as the Sector-Specific Agency for the energy sector, works in conjunction with the Department of Homeland Security (DHS), the agency charged with running the Private Sector Clearance Program, to nominate key individuals, including analysts, for security clearances. As a nominator, DOE has streamlined its internal nomination process to prioritize and submit nomination forms to DHS for approval in an expeditious manner. DHS then works through the Office of Personnel Management (OPM) on background checks and adjudication, which is where the backlog exists. DOE cannot speak to OPM's process or resources and defers to OPM on its approach to reducing the backlog.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

QUESTIONS FROM SENATOR CORTEZ MASTO

- Q1. In your testimony you mention how DOE works with DHS to plan for, respond to, and recover from significant attacks on our power grid. Can you further clarify your respective roles authorities, for example in developing regulations?
- A1. As the Sector-Specific Agency for the energy sector and the lead agency for Emergency Support Function #12 – Energy under the National Response Framework, it is the Department of Energy’s (DOE’s) role to help industry plan for, respond to, and recover from attacks. Department of Homeland Security (DHS), through the National Protection and Programs Directorate and the Federal Emergency Management Agency (FEMA), provides the supporting framework. Under Presidential Policy Directive 41 (PPD-41), DHS, through the National Protection and Programs Directorate’s National Cybersecurity and Communications Integration Center, is the Federal lead agency for asset response activities in response to any cyber incident, and DHS coordinates with DOE in responding to significant cyber incidents affecting the energy sector. The Federal Energy Regulatory Commission and the North American Electric Reliability Corporation develop and enforce reliability standards for the electricity sector. DHS’s Transportation Security Administration (TSA), in coordination with the Department of Transportation’s Pipeline and Hazardous Materials Safety Administration (PHMSA), has the authority to develop regulations for pipeline security.”
- Q2. Hydropower accounts for about 40 percent of the renewable energy produced in Nevada, but while the PPD-21 designates DOE as the SSA with responsibility for the power grid, DHS is responsible for the dams sector. How are DOE and DHS addressing the unique challenges faced by our hydropower facilities?
- A2. As the Sector-Specific Agency for the energy sector, Department of Energy (DOE) collaborates with Department of Homeland Security (DHS) on the security and resilience of various subsectors and critical infrastructure. DOE will continue to offer subject matter expertise to support the energy sector, including hydroelectric facilities. Hydroelectric facilities do not face specifically unique challenges related to cybersecurity threats as addressed in Presidential Policy Directive 21.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

DOE's Hydropower Program is part of the Water Power Technologies Office within the Office of Energy Efficiency and Renewable Energy. As an R&D organization, the Program manages a research portfolio that develops technological advances, provides information and analyses, and creates tools that help reduce costs in the hydropower industry. We agree that hydroelectric dams are a crucial component of our Nation's critical energy infrastructure necessary for grid stability and resiliency. Recognizing the unique multi-purpose nature (e.g., flood control, consumptive water storage) of hydropower, the Program is investigating R&D needs that could support both cybersecurity and dam safety. This type of work could include examining cybersecurity assessment and evaluation tools, best practice analyses for cybersecurity prevention, detection, and mitigation of cybersecurity threats, or national assessments to identify short- and long-term risks of dam malfunction or failure and tools and methodologies for effective dam health inspection.

- Q3. Nevada's Governor Sandoval recently created the Office of Cyber Defense Coordination, which serves as the primary focal point for cyber threats and security for the State of Nevada. With the addition of a Cyber Defense Coordinator, the OCD will serve as the primary conduit with the federal government, as well as the primary entity managing cyber threat issues across the State of Nevada. As a former local government official, how do you think the federal government can best coordinate with State cyber offices like Nevada's to perform cyber threat analysis and reporting of threat information?
- A3. The Federal Government coordinates with State cyber offices by sharing actionable information about cyber threats, which the State cyber offices can share among relevant stakeholders. DOE also works with state associations to host energy assurance events to discuss coordination between government and industry on planning for the potential physical consequences of cyber incidents. For example, the lessons learned from the Liberty Eclipse exercise, hosted in Rhode Island in December of 2016 and featuring

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

nearly 100 participants from 15 states, continue to inform planning and coordination efforts with states, and set the stage for future coordination exercises.<sup>a</sup>

- Q4. Through the DOE Budget Request, the Secretary recently announced his intention to establish an Office of Cybersecurity, Energy Security, and Emergency Response (CESER) “to strengthen the Department’s role as the sector-specific agency for cybersecurity in the energy sector. This office would be created from existing responsibilities from within the Office of Electricity Delivery and Energy Reliability (OE). What exactly will DOE be doing differently through the creation of this new office, different from what OE has already been doing?”
- A4. The creation of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) will build on all that we do today and elevate the Department’s focus on energy infrastructure protection and enable more coordinated preparedness and response to cyber and physical threats and natural disasters. By combining Departmental elements that support response and recovery, DOE will enhance the efficiency and effectiveness of the preparedness cycle for events impacting the energy sector.

The President has requested \$95 million in FY 2019 for CESER with a focus on early-stage activities that improve cybersecurity and resilience to harden and evolve critical energy infrastructure. CESER will continue building partnerships with energy sector utilities, vendors, universities, national laboratories, and cybersecurity service providers to reduce the risk that a cyber incident might disrupt energy delivery. These activities include early-stage R&D at National Laboratories to develop the next generation of control systems, components, and devices with cybersecurity built in, and a greater ability to share time-critical data with industry to detect, prevent, and recover from cyber events.

CESER programs will reduce the risks of and impacts from cyber events and provide a renewed focus on the resilience (the ability to withstand and quickly recover from disruptions and maintain critical function) and security (the ability to protect system assets and critical functions from unauthorized and undesirable actors) of the U.S. energy infrastructure.

---

<sup>a</sup> The after-action report is available at [https://www.energy.gov/sites/prod/files/2017/05/f34/LE%20FINAL%20Exercise%20Summary%201May2017\\_Public%20Doc.pdf](https://www.energy.gov/sites/prod/files/2017/05/f34/LE%20FINAL%20Exercise%20Summary%201May2017_Public%20Doc.pdf).

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing:** *Private Sector and Government Challenges and Opportunities*  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to the Honorable Bruce J. Walker**

Forming one office to support energy stakeholder engagement and the Nation through planning for and responding to incidents while developing supporting capabilities, training, exercises, and evaluating lessons learned will more directly inform research and development efforts in grid resilience and security. Additionally the important subject matter expertise collected supports the critical role energy plays in national security.

U.S. Senate Committee on Energy and Natural Resources  
 March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities  
 to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
 Questions for the Record Submitted to the Honorable Jim Matheson

Questions from Chairman Lisa Murkowski

**Question 1: Compliance with Mandatory Standards – There is genuine concern that the electricity sector should be stepping up its efforts on cybersecurity. As you note in your testimony “the electric sector today is the only one with mandatory and enforceable standards when it comes to cybersecurity.” Violations of these mandatory standards can result in fines of up to \$1 million per day, per violation. At the same time, others assert that utilities are overly focused on compliance – that in an effort to meet the mandatory standards and avoid the financial penalties, the electric sector is losing focus on the goal of cybersecurity protections. How do you respond?**

That is a misconception. Through NERC, the electric sector has mandatory and enforceable standards on operations, planning and security issues, but industry doesn't go only to the letter and then stop. The NERC cybersecurity standards create a baseline for industry to exceed, not a ceiling. In the electric sector you will continue to see the industry strive to improve our cyber security stance in this ever-evolving environment. This is why the sector has gone through multiple revisions to the cyber standards. As the environment evolves so do our standards. It is also important to remember that standards are not the only solution, but rather one tool in a broader toolbox. There are cybersecurity events that cannot be realistically addressed by NERC standards. In these cases, NERC has the authority to issue industry alerts that have mandatory acknowledgment and reporting requirements. NERC alerts can be issued in a matter of hours or days. Additionally, under the FAST Act DOE now has emergency authority in the event of an imminent threat.

**Question 2: Expectations for DOE's New Cyber Office – Throughout your testimony, you provide examples of how DOE's Office of Electricity has assisted co-ops in their cybersecurity efforts. For example, the NRECA has used DOE funding to establish the Rural Cooperative Cybersecurity Capabilities Program (RC3) to provide cyber training, services and tools to member co-ops. Last year, the RC3 Program had six Cybersecurity “Summits,” and you note that NRECA hopes to have another round of cyber summits this year – with continued support from DOE.**

- **What are your expectations for DOE's new cybersecurity office? Are you concerned with the potential impacts to your ongoing efforts with the Office of Electricity?**

We are looking forward to continuing the same engagement we currently have at DOE, like those referenced in this question, when the new office is stood up. The expectation is the new office will help raise the prioritization of these important issues within DOE.

- **What does NRECA need from DOE and this new office?**

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to the Honorable Jim Matheson**

Continued engagement and partnership with consistency during the transition and a key focus on industry R&D needs.

**Question 3: Public Affairs-related activities – You testified that the Electric Subsector Coordinating Council (ESCC) supports “public affairs-related activities and initiatives designed to enhance the reliability and resilience of the electric grid.” Please elaborate. What kinds of public affairs activities has the ESCC undertaken and to what result?**

ESCC efforts around public affairs related activities are to ensure that during regional or larger events there is not only a shared awareness across industry, but an ability to communicate that to the public as appropriate. The ESCC brings together public affairs staff across the sector in what are called “blue sky days” for advance planning and coordination in the event of both notice and non-notice events to ensure that industry and government harmonize public affairs efforts effectively. This coordination proved essential during hurricanes Harvey and Irma last year, allowing ESCC members to exchange information in a timely manner and relay key information to the public.

**Question from Senator Debbie Stabenow**

**Question: As Ranking Member of the Senate Agriculture Committee, I am working closely with Chairman Roberts to advance the Farm Bill this year. As you know, Farm Bill programs provide critical assistance to rural energy systems through USDA Rural Development. This is particularly the case for the Rural Utility Service, which provides capital that electric cooperatives use to build, improve, and harden their energy systems.**

**Do you have any thoughts about how RUS might be able to partner with your member companies to help protect critical electric infrastructure from cyber-attacks?**

RUS can help rural electric cooperatives by continuing to provide affordable capital to support the expansion, improvements, upgrades, and modernization of our members’ electric system.

**Question from Senator Catherine Cortez Masto**

**Question: In your testimony you note that different types of entities, for example large and small, face different challenges. What are some specific challenges faced by rural cooperatives and what can the federal government do to help address these issues?**

One of the biggest challenges all utilities are facing is access to a limited cybersecurity workforce that understands the electricity sector and industrial control systems cybersecurity issues. Rural communities face the double challenge of the high price of relatively rare cybersecurity talent, coupled with the difficulties associated with attracting that limited workforce to a rural area.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to the Honorable Jim Matheson**

Federal programs that invest in cybersecurity training programs for all levels of education, particularly in rural high school and community colleges, can help address the workforce shortage issues. For example the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) programs, and the National Science Foundation's (NSF) cybersecurity education programs are both actively working in this area.

In addition to federal support to address the cybersecurity workforce shortages, continued efforts by the Department of Energy (DOE) to support cybersecurity research and development (R&D) programs that specifically address issues relevant for distribution utilities are needed. NRECA works with a wide range of partners to compete for cybersecurity research grants. Funding for this research is essential to make the technological advancements we need to keep pace with changing threats. We will continue to work with partners to help shape the research agenda so it meets the needs of our members, but the breadth of that research agenda is dependent on funding allocations.

The Cooperative Agreement between NRECA and DOE, similar to the Cooperative Agreement between APPA and DOE, created a unique partnership with the DOE to address the cybersecurity needs of our distribution members. NRECA created our Rural Cooperative Cybersecurity Capabilities (RC3) Program using funding from this Cooperative Agreement. It is clear from the RC3 Program's success thus far that our members are highly motivated to implement solutions when they are tailored to their business model. The RC3 Program is only in its second year and there are many opportunities to continue to expand the impact of the program with additional resources. NRECA and APPA have weekly calls to ensure our efforts under the Cooperative Agreements are collaborative and to share ideas and best practices with each other as we implement our respective programs. We have a common goal – improving the cybersecurity posture of the electricity sector. We hope that DOE and members of the Committee will recognize the value and impact of our work and continue to support our efforts.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

Chairman Murkowski and Ranking Member Cantwell, and distinguished Members of the Committee. Thank you for the opportunity to respond to Questions for the Record following my testimony at the March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*. As the Executive Director of the Center for Information Assurance and Cybersecurity (CIAC) at the University of Washington, founded in 2004 as an NSA/DHS designated Center of Academic Excellence in Cybersecurity Defense Education and Research and an NSA CAE Regional Resource Center named to disseminate best practices in cybersecurity education and to mentor other colleges and universities, our focus is on convening industry, government and military around shared problems such as the alarming lack of cybersecurity talent to handle the cybersecurity attacks and breaches we are experiencing. This problem is amplified for government and private infrastructure who must compete with the private sector who pay higher wages for cybersecurity talent that they can't match.

Motivated by this problem, our education research focuses on methods to increase the supply of cybersecurity graduates while condensing the time-to-expertise. I deeply appreciate your interest in this often overlooked area of cybersecurity and commend you for your collective wisdom in recognizing the dire need for talent. I answer your questions from the years of experience I have spent developing this area of research.

What follows are succinct answers to your questions followed by appendices offering additional reading for further study if an area interests you.

In addition, I would be happy to discuss any of this further. Please don't hesitate to ask. I can be reached at either of my offices—most readily available by cell phone or email:

Barbara Endicott-Popovsky, Ph.D.  
Executive Director, Center for Information Assurance and Cybersecurity  
Center for Information Assurance and Cybersecurity in Education CAE-CDE  
Box 358523  
Husky Hall 10909 NE 185th Street, Room HH 1439  
Bothell, WA 98011-8246  
Cell: 206-240-0345  
Fax: 206-260-0115; Academic Affairs office fax: (425) 352-3611  
[endicott@uw.edu](mailto:endicott@uw.edu)

Center for Information Assurance and Cybersecurity in Research (CAE-R)  
Applied Physics Lab  
Box 355640  
Benjamin Hall 616 NE North Lake Place, Room 525  
Seattle, WA 98101  
Office: 206-685-0548

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

**Questions from Chairman Lisa Murkowski**

**Questions: Training Staff in Control Rooms** – Mr. Lee (DRAGOS) has made the point that we cannot overlook the critical role that effective cybersecurity professionals must play. One of the best ways to be prepared for an attack of any sort is to be prepared and trained for responding to that attack.

- *I can envision two types of training for an attack. The first would involve the Information Technology (IT) specialists that work behind the scenes in keeping computers up and running throughout the grid. The second would involve the actual operators of those computers. Are both receiving the best training that they can get?*
- *Is the cybersecurity training for our grid operators sufficient? What needs to be improved? Is this training reaching down to all grid operators? Or is it only reaching the biggest companies with the greatest resources?*
- *Since the Ukraine attacks are real-world events where control room operators were forced to handle an unexpected situation --- an event where we've heard that operators discovered that somebody else had remotely hijacked their computers, to what extent are the lessons learned about Ukraine being taught in training classes here in America?*

**Chairman Murkowski, these are interesting and pertinent questions. Allow me to provide an integrated answer:**

**BACKGROUND**

NIST (National Institute of Standards) Special Publication 800-50 outlines standards for the development and implementation of security awareness training. [1] Recognizing that the "people factor" is the weakest link, NIST recommends that all users of any information system be made aware of their roles and responsibilities in maintaining security. [1] Further, to be effective, any awareness educational program should be designed for the intended audience, built around a message and desired outcomes and gain attention. [1]

**Annex I** provides an effective example of applying SP 800-50 for Seattle business community leadership in 2005 to alert them to the risks of identity theft through misuse of online search engines. The results drew local and national attention and resulted in State legislative reforms.

**ANSWER**

**QUESTION 1:** Given that data breach is inevitable (See **Annex II: The Probability of 1** [2]) all users, at every level in the organization, should receive security training designed for their roles/responsibilities ranging from the incidental user to the highly trained operator. From the attacker's point of view they are

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

looking for the easiest way in, often that's through social engineering, i.e., 'conning' someone in the organization to let them in.<sup>1</sup>

**ANSWER**

**QUESTION 2:** My experience has been that implementation of effective programs is a function of organizational size, cybersecurity sophistication, resources and availability of good instructors. Although in recent years, I've observed more attention being paid to security training, and many more options exist, my experience has been that training is not as effective or as pervasive in organizations as it could be. Further the dearth of cybersecurity talent includes a lack of instructors.

The work of the FCC's Communications Security Reliability and Interoperability Council (CSRIC)<sup>2</sup> Working Group 7, specifically chartered to provide recommendations to the FCC for improving development of the cybersecurity workforce could be leveraged for the energy sector.<sup>3</sup> The Executive Summary of CSRIC's Final Report can be found in **Annex III** and can be downloaded in full at CSRIC's website.<sup>4</sup> The co-chairs for this effort were:

William (Bill) Boni Sr. VP Digital Security, T-Mobile  
 (425) 383-4879  
[william.boni@t-mobile.com](mailto:william.boni@t-mobile.com)

Drew Morin, Director of Federal Cybersecurity Tech Program, T-Mobile  
 (202) 654-8224  
[drew.morin2@t-mobile.com](mailto:drew.morin2@t-mobile.com)

Drew is 'officed' in Washington, DC, where he can be readily available to acquaint you/DOE with the results of the CSRIC cybersecurity education study that could provide insights for the Energy Sector. I've contacted both who assure their willingness to help in this regard.

May I add that cybersecurity is professionalizing, like medicine, law, library science. We are seeing education standards converging, inclusion of ethics in curriculum, internships/apprenticeships. This was a deficit area identified by the CSRIC report that is being addressed aggressively by NSA, DHS and the ACM (Association for Computing Machinery) organizations.

<sup>1</sup> Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information

<sup>2</sup> The mission of the Communications Security, Reliability and Interoperability Council (CSRIC) is to provide recommendations to the Federal Communications Commission (FCC) to ensure optimal security and reliability of communications systems, including telecommunications, media, and public safety. The CSRIC has identified best practices and developed recommendations to identify, protect, detect, respond to, and recover from cyber events. The CSRIC has formed a number of working groups that have developed useful information on cybersecurity information sharing, secure hardware and software, and consensus cybersecurity controls, among other topics.

<sup>3</sup> In February 2013, Executive Order 13636 assigned NIST to develop a flexible cybersecurity framework for critical infrastructure protection that could be adapted to meet the specific needs of individual sectors. CSRIC collaborated with NIST and leveraged that work to achieve final recommendations.

<sup>4</sup> <https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf>

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

**ANSWER**

**QUESTION 3:** This is an excellent question and suggestion. I am aware that the Ukraine attacks are incorporated in training for the National Guard in the State of Washington. We are developing a certificate in critical infrastructure protection that will be including this content.

**PLEASE NOTE:**

Cybersecurity training content is a moving target as adversaries aggressively improve. Training not only must be continuous (and continuously developed)<sup>5</sup>, throughout an organization, but also should include hands-on. The latter is challenging with the energy sector that would require access to SCADA and industrial control systems. Our adversaries train on this equipment in their universities. For the most part, we don't for many reasons.

**REFERENCES**

- [1] Wilson, M. and Hash, J. (2003). "Building an Information Technology Security Awareness Training Program." U.S. Department of Commerce, NIST Special Publication 800-50.
- [2] Endicott-Popovsky, B. The Probability of 1. *Journal of Cyber Security and Information Systems*. 2015, Vol.3 (1), pp.18-19.

---

<sup>5</sup> ISACs and cybersecurity professional organizations are interesting sources for maintaining currency for practitioners.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

**Question from Senator Debbie Stabenow**

**Question:** I very much appreciated hearing your testimony about the importance of providing skills and training needed for careers in cyber security.

I am a strong supporter of professional development programs, and I have introduced several bills that would help strengthen employer-training partnerships; foster career and technical education in our high schools; and spur on-site job training and career development.

Would you please elaborate on the successes of the University of Washington's cooperative learning program and how important on-site training is to developing our cyber workforce?

**ANSWER**

**Senator Stabenow, I deeply appreciate your interest in our project which was funded by the National Security Agency (NSA) and an industry partner.**

Many universities offer internships, but we have expanded that concept, devising a cybersecurity cooperative learning pilot where students maintain their current academic load in the last year of their degree programs and, in addition, opt into an integrated program of professional instruction and half-time industry employment. The additional professional education includes: 1) an information security and risk management (ISRM) certificate that covers all the necessary knowledge units required of NSA Centers of Academic Excellence in Cyber Defense Education <sup>6</sup> and 2) professional seminar/mentoring conducted in partnership with industry to help students triage their work experience with what they learn in the classroom. The addition of the professional seminar/mentoring and certificate accelerate student work readiness when they formally graduate.

An expanded description of the University of Washington's cooperative learning program pilot is included in **Annex IV**. We will have a final report of the first year's experiences at the end of this academic year, which I can provide when published, that will include analysis of the data we collect. Preliminarily, indications are that the program was successful. Our flagship industry partner, T-Mobile, committed to a second year and increased the numbers of interns, offering jobs to 90% of the first cohort. Feedback from students and management is being incorporated into next year's program and new industry partners are joining the program. We will be disseminating a generalized model and publishing results to encourage others to benefit from our work.

I will be happy to forward to the committee/your office any reports, models, publications as our work completes.

---

<sup>6</sup> The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation. <https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/>

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

**Question from Senator Catherine Cortez Masto**

**Question:** The public and private sectors must compete for a limited pool of highly trained cyber experts, creating a shortage of cybersecurity leadership and expertise. Are we developing enough of a workforce to stay at the forefront of cyber defense?

**Senator Masto, thank you for your insightful question. It is the motivation for the work of the National Security Agency's (NSA) National Initiative for Education and Training Program (NIETP) in collaboration with DHS and NIST. It's also the motivation for my cybersecurity pedagogical research.**

**ANSWER**

Unfortunately, we are not developing a workforce in sufficient size and depth to cope with the numbers and severity of cyberattacks we are experiencing. This is especially true for critical infrastructure that competes with salaries that the hi-tech companies will pay for this talent. 100,000's of jobs are going unfilled based on reputable reports.

This deficit is well documented in many credible sources. I would recommend the Burning Glass study from 2015 which is often cited in this regard.<sup>7</sup> I would also recommend exploring the Cyberseek website<sup>8</sup> that provides detailed, actionable data about supply and demand in the cybersecurity job market by state/by county.

We need a Scholarship for Service (SFS)<sup>9</sup> program for cybersecurity graduates that provides a year of educational funding in exchange for a year of work in critical infrastructure. The SFS website describes the current program that funds students for government employment. It should be extended to include critical infrastructure (even if largely owned by the private sector) with increased funding to significantly increase the numbers of scholarships from the few hundred authorized /year at current levels.

---

<sup>7</sup> Burning Glass. Job Market Intelligence: Cybersecurity Jobs (2015). Retrieved April 15 at: [http://burning-glass.com/wp-content/uploads/Cybersecurity\\_Jobs\\_Report\\_2015.pdf](http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf)

<sup>8</sup> <http://cyberseek.org/>

<sup>9</sup> <https://www.sfs.opm.gov/>

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
**to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure**  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovskiy**

## ANNEX I

Proceedings of the 2005 IEEE  
 Workshop on Information Assurance  
 United States Military Academy, West Point, NY  
 June 2005

### Community Security Awareness Training

Barbara Endicott-Popovskiy, Ivan Orton, Kirk Bailey, Deb Frincke, *Member, IEEE*

*NIST Special Publication 800-50 outlines standards for the development and implementation of security awareness training. [1] Recognizing that the "people factor" is the weakest link, NIST recommends that all users of any information system be made aware of their roles and responsibilities in maintaining security. [1] Further, to be effective, any awareness event should be designed for the intended audience, built around a message and desired outcomes and gain attention. [1]*

*Such a security awareness event was conducted for the business community leadership in Seattle, Washington. The purpose was to alert them to the risks of identity theft through misuse of online search engines. The means adopted for focusing attention, was a Google-hacking contest. It was anticipated that object lessons from this demonstration would (1) alert community leaders to take appropriate measures to ensure protection of personal and private information stored in their organizations' databases and (2) to open the way to influencing legislative change in the State, where the event sponsors contend the statutes are outpaced by technological advances.*

*The contest outcomes were significant. In a little over an hour, the winning team identified over one hundred million potential opportunities for identity theft. The results drew local and national attention. [ 2, 3] In addition, discussions have begun with the State's Attorney General's office regarding possible legislative reforms.*

*Based on observations of this trial, the authors suggest that a security awareness program, based on NIST standards, can be effective, not only for organizations, but for specifically defined communities, as well. This paper describes the event, the outcomes and the authors' conclusions. The approach presented in this paper could be repeatable in any community for a variety of purposes.*

#### I. INTRODUCTION

On the morning of March 4, 2005, in Seattle, Washington, members of the Agora, a forum for airing current issues of concern among information assurance professionals, held a security awareness event modeled along NIST guidelines. The Agora leadership had devised a creative approach to raising the local community's consciousness regarding the degree to which sensitive information can be vulnerable to compromise on systems linked to public networks. They staged a Google-hacking<sup>10</sup> contest to demonstrate the problem. [1]

---

*Barbara Endicott-Popovskiy, Lecturer, Seattle University;*  
*Ivan Orton, JD, Senior Deputy Prosecuting Attorney with the Fraud Division of the King County Prosecutor's Office in Seattle*  
*Kirk Bailey, Chief Information Security Officer, City of Seattle*  
*Deb Frincke, Ph.D., Chief Scientist Cybersecurity, Pacific Northwest National Laboratory and Associate Professor (on leave),*  
*Computer Science Department, University of Idaho*

---

<sup>10</sup> "Google-hacking" commonly refers to obtaining anything exploitable, including usernames, passwords, credit card numbers and other personal identifiable information using the search engine, Google.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

Meeting quarterly in the Northwest for the last ten years, the Agora has been responsible for solving problems arising from the unintended consequences resulting from the proliferation of digital infrastructure accessing insecure public networks. [2, 4] Most recently, the Agora successfully tackled legislative change, at the State level, regarding cyber stalking, one of the fastest growing crimes on the Internet.<sup>11</sup> [4]

Having gained the attention of State legislators and local government officials by tackling a serious incident arising from misuse of public networks, the group has begun focusing on the broader issue of the vulnerability to identity theft of personal and private information housed in systems accessible through the Internet. Through security awareness training, they are attempting a two-pronged approach designed to 1) bring attention to the need to improve network and data management and 2) influence helpful legislative change.

As shown in Table 1, the Agora awareness event met the criteria outlined in NIST Special Publication 800-50, which provides standards for the development and implementation of security awareness training. [1] Recognizing that the "people factor" is the weakest link, NIST recommends that all users of any information system be made aware of their roles and responsibilities in maintaining security. [1] Further, to be effective, any awareness event should be designed for the intended audience, built around a message and desired outcomes, and gain attention. [1]

Table 1 NIST Guidelines for Security Awareness Event

NIST Guidelines	Google Hacking Event Attributes
Designed for specific audience	Business and community leaders in Seattle
Built around a message	"Alarming vulnerability of public and private information to compromise on public networks"
Built around desired outcomes	<ul style="list-style-type: none"> <li>● Gain attention</li> <li>● Influence legislation</li> </ul>
User awareness of roles / responsibilities	Event summation focused on roles and responsibilities regarding the online identity theft problem

<sup>11</sup> Responding to a particularly egregious case involving an employee of the City of Seattle, members of the Agora undertook a two-year project of tracking down, and assisting in, the eventual prosecution of the stalker, but not before becoming the impetus behind some of the first cyber-stalking legislation in the nation. [4]

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

The March 4 security awareness event was designed specifically for an audience of community and business leaders who could effect change. It was designed to be "attention-getting" and to move attendees to action.

Based on observations of this trial event, the authors suggest that a security awareness program, based on NIST standards, can be effective, not only for organizations, but for specifically defined communities, as well. This paper describes the event in detail, the outcomes and the authors' conclusions. The approach presented in this paper could be repeatable in any community.

## II. A WIDESPREAD COMMUNITY PROBLEM

Identity theft is a widespread and growing community problem affecting governmental and business infrastructure, as well as the individuals directly impacted.

The news media now regularly features stories about database break-ins that result in the theft of thousands of names with associated credit card numbers, driver's licenses and/or social security numbers, treasure troves for identity thieves. [5, 6, 7, 8] The Federal Trade Commission reports that 1 in every 20 Americans has been a victim of identity theft in the last year. [9]

While most financial institutions don't publish data on the annual amounts of such losses, an FTC report estimates the overall impact to the U.S. economy in the hundreds of millions of dollars, [10, 11] which the consumer ultimately pays through higher prices and fees.

Although most financial institutions cover consumer losses resulting from unauthorized purchases on stolen credit cards, they don't take responsibility for costs related to clearing one's credit. Each incident averages \$1000 in coping costs. [9] These costs associated with coping with restoring one's credit following the theft of one's identity are largely born by the victim.<sup>12</sup>

## III. ADDRESSING THE LACK OF AWARENESS

Having direct experience with responding to a growing number of incidents of identity theft, members of the Agora view the escalation of identity theft as a community problem requiring solutions that involve business and government leadership combined with technical expertise. Lack of awareness on the part of business and government leaders was determined to be the primary impediment to developing such a partnership to solve this problem.

As a result, Agora decided to create a security awareness event that would demonstrate how much personal and private information is accessible through public networks and how little skill

---

<sup>12</sup> This is true regardless of whether the theft occurs as a result of an individual's carelessness in the release of personal data or from a hacker's intrusion into a poorly managed network that allowed theft from a database housing that information. The latter seems particularly unfair since the consumer has little control over his/her personal information once it is stored in private or public databases

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

is needed to acquire it. Business and government leaders and the press were invited to a Google-Hacking Contest for the purpose of experiential learning. The event planners hoped to gain interest from these community leaders in exploring possible solutions.

#### IV. GOOGLE HACKING

Search engines, while conceived for benign purposes, can be used effectively as hacking tools. There is no inherent flaw in Google that led to its being the search engine selected for this demonstration, simply its widespread use and familiarity with the general public and the fact that it is 'alarmingly simple to use.' [12]

##### *A. Requires Little Skill*

A hacker with little or no programming skills can employ a search engine such as Google to discover information, residing in Web-connected servers and machines connected to those servers, that they shouldn't be able to find. To be successful requires knowledge of a minimal list of Google operators and how to concatenate a Google string.

That information is readily available by searching for "Google hacking" on Google itself! The first site in the search results is <http://johnny.ihackstuff.com/> with its database of over one thousand Google queries and sample results. [13]

Having entered two student teams in the Agora Google Hacking Contest, one of the authors can attest to how easy it is to become proficient. Students with no technical background required one to two hours of reading (the *johnny.ihackstuff* site or the first 3 chapters of *Google Hacking* by Johnny Long<sup>13</sup>[14]) and a few hours of online practice to discover names, social security numbers, driver's license and passport numbers online.

##### *B. Poorly Configured Systems*

The security community is aware that hackers can gain useful information about their targets through Google Hacking<sup>14</sup> techniques that take advantage of badly configured and poorly administered systems. Yet, systems exist that allow directory indexing, for example, which can expose file paths and files that are very useful to an intruder.

To properly exercise their responsibility for taking private, sensitive information out of the reach of web crawlers, those responsible for connecting servers to the Internet should understand how search engines operate to the same degree that hackers do. The fact that there is sensitive information that can be found easily through Google indicates that there are those managing

---

<sup>13</sup> A book written by the *johnny.ihackstuff* web site author.

<sup>14</sup> Readers are referred to those sites mentioned in the preceding paragraph for details on the methods and tools of Google-Hacking. In addition, the Google Help Center, accessed from the Google Home page, provides instructions on both simple and advanced searches, tools hackers can use, as well.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

networks who do not understand, or consider, how to defend against these types of attacks when they design their networks.

Scott Granneman, Security Focus, identifies the problem as "uneducated folks putting content on the web they think is hidden from the world." [15]

*Often Web servers are left configured to list the contents of directories if there is no default Web page in those directories; on top of that, those directories often contain lots of stuff that the website owners don't actually want to be on the Web. That makes such directory lists prime targets for snoopers.* [15]

As a means of attack, Google lately has gained prominence with the appearance of a MyDoom virus variant and the Santy worm, both of which automate Google attacks. [15] Their appearance has led security experts to predict a 'massive increase' in such attacks this year.' [16] All the more reason to raise awareness of Google hacking.

Fixing the problem is not difficult. It requires incorporating an awareness of the problem into the creation of more thoughtfully configured networks. The Google Hacking Contest was designed to create public awareness about the vulnerability of personal and private information to inadvertent exposure through search engines.

#### V. AGORA'S GOOGLE HACKING CONTEST RULES

Holding a Google Hacking contest requires careful design to ensure that no laws are violated and that everyone behaves ethically regarding what is discovered. The list of rules below was circulated before the contest and read to participants to gain their compliance. In addition, monitors and contest judges were assigned to each group to ensure that the rules were followed.

They are provided as a useful guide for anyone considering a similar event. Each rule is stated first, followed by an explanation.

##### *A. Rule #1: Information Protection*

**Rule:** *All contest participants must be VERY CAREFUL to manage and protect any sensitive information they discover from further disclosure beyond the current exposure the data already has online.*

**Explanation:** The intent of the contest was to learn more as professionals about a provocative and troubling public problem, not to embarrass anybody or any institution. Information found during the contest was described as 'for demonstration and instructional purposes only.' Several law enforcement officials attending the meeting served as reminders about obligations to follow this rule.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
**to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure**  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

*B. Rule #2: Required Gear for Competing Gear Heads*

**Rule:** Teams must bring their own 'stuff' in order to play. Teams will need as many mobile computing devices as they feel are necessary to win the contest, depending on what Google hacking strategy they decide to employ. Each team will need at least one box that has 802.11x connection capability, or some CDMA-type enabled service. There will be wireless access to the Internet available.<sup>15</sup> Teams also should bring at least one standard-size (8½" x 11") notepad and several manual writing devices for keeping score. In the event that some of the hacking discoveries are shown to the larger meeting audience, teams should bring a USB-flash drive or a CD burner.

**Explanation:** The Agora collective does not have the resources to provision participants and did not wish to presume on the hosting institution.

*C. Rule #3: Respecting our Host's Internet Connection and Network*

**Rule:** Everyone who even thinks about using the Internet access provided by Seattle University for this Contest **WILL NOT ABUSE THIS SERVICE IN ANY WAY**. You all know what this means. If you don't know what this means, you can't play.

**Explanation:** Internet access was provided by the hosting institution, Seattle University, for the Google hacking contest, only. No other use was permitted.

*D. Rule #4: Judging*

**Rule:** Each team will be assigned a Contest Judge before the contest begins. The assigned Judge has absolute authority over the team's information discoveries, discovery claims and scoring. The judge will also act as an observer of the team's activities to ensure all rules are observed. All judges will be briefed and prepared to apply uniform oversight and scoring tabulation.

**Explanation:** This control was necessary to ensure that each team abided by the rules and that scoring was fair and consistent.

*E. Rule #5: Time Allowed for Hacking and What is to be Considered.*

**Rule:** Teams will be given **45 minutes** to 'have at it' with the Google search engine. When the time is up, the team with the most points wins the contest. Teams must use time wisely and efficiently. It isn't just about locating the targeted information, the discoveries have to be accurately documented and scored during the hacking timeframe. **Discovered data has to be documented (On that 8 ½" x 11" notepad) with a listing of the associated URL, brief**

---

<sup>15</sup> The event host's (Seattle University) IT department provided a wireless LAN connectivity, separated from the University network.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

*description of the discovered document or data file. In addition, the information content has to be reviewed for scoring by the judge. So prepare for how this might best be done before starting the actual event.*

**Explanation:** The amount of time allowed was closer to an hour. At the conclusion of the contest, additional time was taken for discussion and identifying next steps.

*F. Rule #6: Scoring*

**Rule:** *Points will be awarded by judges based on the scoring criteria listed below. (Table 2.) Team judges only can allow points for documented discoveries made during the timed Google hacking period. If participants have been practicing their Google hacking skills prior to the contest and have previously found stuff, they are going to have to find it again during the contest with an assigned judge observing their search and discovery processes.*

**Explanation:** The score card below is similar to ones found on the Internet. Having procedures outlined in advance helped avoid challenges to the results.

*G. Score Card*

Points were awarded based on the following scale:

Table 2 Google Hacking Score Card

<b>Personally Identifiable Information</b>	<b>Points</b>
Name and Social Security Number (SSN) together	1 pt
Name, SSN, Date of Birth (DOB) together:	2 pts
Name, Credit Card number (CCN#) together	1 pt
Name, CCN#, Expiration date together	2 pts
Name, CCN#, Exp. Date, and 3-digit security code (aka CID#) together	3 pts
Name, Bank Account Number or Brokerage Account Number	1 pt
Name, Bank Account Number and PIN	3 pt
Additional data associated with each CCN# & SSN (e.g. address, phone)	0.5 pt
Name, password, and related online account identifier to anything	5 pts

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

Bonus points for anything above associated with a Washington State Citizen	10 pts
--	--------

In addition, an additional 500-point bonus was offered for the "Most Sensitive Document." Each team was asked to select their most provocative and sensitive document. The judges presented these to the audience for a vote.

VI. HACKING APPROACH

An effective Google hacker will concatenate Boolean and advanced operators into queries that will narrow searches and yield results. Some of the more useful advanced operators are given in Table 3.

Table 3 Google Advanced Operators

Advanced Operator	Purpose
InTitle	Restricts search to pages with specified word in its title
InURL	Restricts search to pages with specified word in its URL
Cache	Shows the version of a page in Google's cache
Filetype	Searches can be restricted to filetype. (The xls and mbd filetypes are particularly useful.)
Numrange	Searches for results within a given numerical range

The actual Google query strings developed by participants were collected at the end of the contest for verification of point scores, and then destroyed. Although queries from the winning team are not available, similar complex strings, like the ones below, can be found online at various hacker sites. [17, 18]

- *allintitle: restricted filetype:doc site:gov*  
Searches for pages with all of the following in the title: 'restricted,' .doc files on .gov sites.
- *intitle:"index of" members OR accounts*  
Searches for pages with "index of" in the titles and either member or accounts lists.
- *allintitle: "index of/root"*  
Searches for pages with index of/root in the title. Results in 1490 pages that can be mined for information.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

- *allinurl:auth\_user\_file.txt*

Searches for pages with lists of user names and passwords

- *allinurl: admin mdb*

Searches for pages with administrator's access databases containing usernames, passwords and other sensitive information

The successful teams worked quickly to concatenate strings like the ones above, narrowing search results and thus minimizing the number of pages requiring scanning. The exercise sensitizes participants to vulnerabilities that can be prevented.

#### VII. RESULTS

Results can be divided into results of the contest itself and the level of community awareness created by this event.

##### *A. The Contest*

Eight teams competed, each consisting of eight to twelve contestants. Not all team members participated directly; some were observers or 'coaches.'

There were three teams of students, one from a local technical college and two from local universities. The remaining five teams were fielded from different companies or industries. One of the five was a group of attorneys with significant knowledge of computers and information assurance.

The remainder of the audience of approximately 300 roamed the ballroom where the event was held, observing the results and learning from the experience.

The following is a partial list of contest results [2]. Due to the sensitivity of some of the information uncovered, it will not be reproduced here. Sensitive information was referred to the appropriate parties following the event.

- 1) Credit card numbers of military personnel,
- 2) A million Social Security numbers of recent immigrants, their tax records and addresses,
- 3) Names, birth dates, Social Security numbers, race and religion of deceased military personnel,
- 4) Names, credit card numbers, birth dates and home phone numbers of 388 Americans who appeared to have ordered pornographic movies online from a Brazilian web site,
- 5) More than one hundred million death certificates with Social Security numbers, dates of birth and city of last residence,

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

- 6) Highly personal information of two individuals, along with their level of government security clearance<sup>16</sup>. One was an expert in virology investigations and the other a responder to nuclear emergencies,
- 7) Personal information about people on terrorist watch lists,

The winning group was a team of lawyers and computer-security specialists. They won with over 190 million points. Their group discovered a database containing millions of names and social security numbers of deceased persons. They also won the bonus for the most sensitive information--the personal information of two individuals working sensitive government projects (See above).

A group of penetration testers from a local network security firm came in a distant second, scoring 13 million points. The student groups clustered near the bottom.

From the results, it appeared that having the experience to know where to look was an advantage for the attorneys.

*B. Community Awareness*

The event was attended by a local reporter with an interest in cyber crime. This individual had followed Agora's work on the cyber stalking initiative and was intrigued and concerned about what he learned at the event. [2] A front-page article was published the next day in his morning newspaper that drew both local and national attention. [2, 3] A syndicated columnist is featuring the article on her daily blog. [3] A subsequent article appeared in the Wall street Journal. [19]

Those attending from both the public and private sector appeared to be impacted by the event. As each team's report was read before the audience, audible gasps could be heard when the quantity and sensitivity of the information discovered was particularly significant.

One of the attendees, a CEO of a local network security firm summed up the experience by saying:

*"The problem is not with Google, but with corporate cultures with the attitude, "Nobody is going to find me, nobody cares what's on my computer." These companies allow Google to enter into the public portion of their networks, sometimes called the DMZ, and index all the information contained there." [2]*

An information security specialist added that

*"Google doesn't need to be fixed. Companies need to understand that they are leaving themselves exposed by posting sensitive information in public places .... If they're performing proper security, then their intranet shouldn't be vulnerable to a Google search engine." [2]*

<sup>16</sup> Clearance information isn't classified, up through fairly high levels. It is therefore permissible to have it on resumes, for instance. Nevertheless, that information linked with additional data (such as found in this case) could be problematic in the hands of the wrong individuals.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

These were the lessons those planning the event hoped participants would take from the meeting. Based on comments from the audience, it appears that objective was met.

In addition, government attendees made a report to the new Washington State Attorney General who has made cybercrime a main focus. Agora members expect to explore possible legislative avenues for increasing data security protections in the State.

#### VIII. LESSONS LEARNED

These are several lessons learned from this experience:

- 1) While security awareness training may be thought of as a work place event, the authors believe it can be an effective approach to educating a community about online security concerns.
- 2) The NIST guidelines in NIST Special Publication 800-50 were found to be applicable for designing a community security awareness training event.
- 3) A Google-Hacking contest effectively communicates to non-technical people the vulnerability of personal information to online discovery. It is easier to understand than other kinds of attacks and can provide a memorable hands-on experience.
- 4) Such a contest is easy to stage. It requires a simple wireless LAN that is independent of the host organization's network.
- 5) It helped to notify attendees in advance so they could form teams, work logistics issues (numbers of computers, etc.) and familiarize themselves with Google hacking before coming. (Some student groups made this a school project for the term.)

#### IX. CONCLUSIONS AND FUTURE WORK

The intent of the event outlined in this paper was to raise awareness among a community's leadership about the vulnerabilities of data held in private and public databases to Internet attacks, specifically attacks generated by using a well-known search engine. The planners concluded that the event was a success.

In addition, planners hoped to influence the adoption of further legislation addressing the protection of personal and sensitive data stored in databases over which the owner of that information has little or no control. That work is ongoing.

##### *A. Future Awareness Training Events*

The awareness training conducted by the Agora will be transferred to the University of Washington's Center of Information Assurance and Cyber Security, a newly designated NSA Center of Academic Excellence, as an outreach project. The Center offers more in depth education in information assurance through certificate programs for those interested in increasing their knowledge after attending an awareness session.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
**to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure**  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

Any additional security awareness events will involve the collection of pre- and post-training data that will be useful in evaluating the effectiveness of the content and approach.

*B. Legislative Initiatives*

Members of the Agora are supporting the development of legislation that addresses the inequity of having the victim bear the costs associated with the misuse of their personal information that is stored in trust on public and private databases.

The representation in Figure 1 captures the unfairness of the current situation and has been used to communicate the problem.

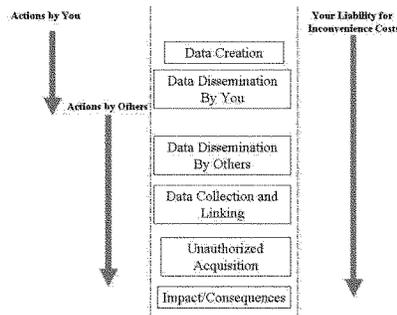


Figure 1 The Unfairness Proposition

Data about an individual will move through several states, from its creation (receiving a social security number when born) to its dissemination, either with or without the individual's consent. Activities resulting in these state changes are largely under the control of others, while liability for the inconvenience costs and impacts<sup>17</sup> due to misuse are born entirely by the individual.

A simple fairness proposition would propose the following:

- Individuals **should bear** the inconvenience costs associated with misuse of the portions of the creation and distribution of any personal information that **they control**.
  - Individuals **should not bear** the inconvenience costs associated with misuse of the portions of the distribution of their personal information that **they do not control**.
- While the fairness proposition appears obvious, it is not reflected in current law. Members of Agora intend to pursue influencing the development of legislative remedies. The desired

<sup>17</sup> Impacts associated with misuse of private data are significant. [10] Aside from the out-of-pocket coping costs identified above, a resulting loss of credit can interfere with the ability to get a job, apply for a mortgage, buy a car, etc.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

outcome is shown in Figure 2 where the parties responsible for storing and forwarding data are the ones held liable for costs arising from misuse.

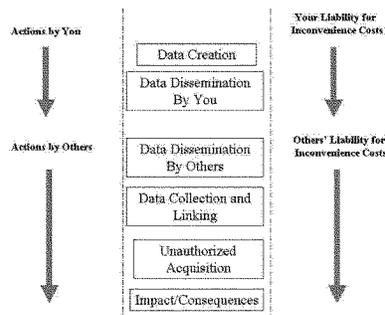


Figure 2 The Fairness Proposition

In conclusion, the security awareness event discussed in this paper achieved its goals to: (1) alert community leaders to take appropriate measures to ensure protection of personal and private information stored in their organizations' databases and (2) to begin the process of influencing legislation that will address problems arising from identity theft.

#### X. REFERENCES

- [1] Wilson, M. and Hash, J. (2003). "Building an Information Technology Security Awareness Training Program." U.S. Department of Commerce, NIST Special Publication 800-50.
- [2] Shukovsky, P. " 'Good guys' show just how easy it is to steal ID." Seattle Post Intelligencer. March 5, 2005. (Retrieved from the Web March 19, 2005). [http://seattlepi.nwsource.com/local/214663\\_googlehack05.html](http://seattlepi.nwsource.com/local/214663_googlehack05.html)
- [3] Malkin, M., "Google Hacking." Michelle Malkin's Blog. (Retrieved from the Web March 19, 2005). <http://michellemalkin.com/archives/001680.htm>
- [4] Shukovsky, P. "Law banning cyberstalking is a victory for a victim." Seattle Post Intelligencer. March 25, 2004. Retrieved from the Web March 19, 2005. [http://seattlepi.nwsource.com/local/166204\\_cyberstalk25.html](http://seattlepi.nwsource.com/local/166204_cyberstalk25.html)
- [5] InfoSec News. "Audit: State voter system left information vulnerable." March 18, 2005. (Retrieved from the Web March 19, 2005) [isn@c4i.org](http://isn@c4i.org)
- [6] CBS News.com "Alleged Database Hacker Arrested," Sept. 10, 2003. (Retrieved from the Web March 19, 2005) <http://www.cbsnews.com/stories/2003/09/10/tech/main572449.shtml>
- [7] Wired.com. "How to Foil Data Thieves, Hackers," Jan. 20, 2003. (Retrieved from the Web March 19, 2005). <http://www.wired.com/news/infrastructure/0,1377,57302,00.html>

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

- [8] McWilliams, B. "Hackers Arrested for E-Commerce Site Break-ins," Internet news.com March 24, 2000. (Retrieved from the Web March 19, 2005). [http://www.internetnews.com/ec-news/article.php/4\\_327181](http://www.internetnews.com/ec-news/article.php/4_327181)
- [9] United Nations report of the Secretary General. "The State of Crime and Criminal Justice World Wide." 10<sup>th</sup> United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Vienna (April, 2000).
- [10] Synovate. "Federal Trade Commission Identity Theft Survey Report." September 2003. (Retrieved from the Web March 19, 2005). <http://www.consumer.gov/idtheft/stats.html>
- [11] Identity Theft Statistics. (Retrieved from the Web March 19, 2005)  
<http://www.bfjs.k12.nj.us/coltech/statistics.htm> .
- [12] Ong Boon Kiat "Google hacking for beginners." Cnet Asia, November 8, 2004. (Retrieved from the Web March 19, 2005). <http://www.zdnet.co.uk/zdnetuk/comment/other/0,39020682,39172957,00.htm>
- [13] Googledorks. (Retrieved from the Web March 19, 2005) <http://johnny.ihackstuff.com/index.php?module=prodreviews>
- [14] Long, J., Skoudis, E., van Eijkelborg, A. (ed.) (2004). *Google Hacking, for Penetration Testers*. San Francisco: Syngress Publishing, Inc.
- [15] Gramman, S. "The Perils of Googling." Security Focus (Retrieved from the Web March 19, 2005). [http://www.theregister.co.uk/2004/03/10/the\\_perils\\_of\\_googling/](http://www.theregister.co.uk/2004/03/10/the_perils_of_googling/)
- [16] Kotadia, M. (1977). "Protect yourself from 'Google hacking' ". Silicon.com, Jan. 14, 2005. (Retrieved from the Web March 19, 2005). <http://networks.silicon.com/webwatch/0,39024667,39127080,00.htm>.
- [17] ComSec, "Google, A Dream Come True," (Retrieved from the Web March 19, 2005).  
<http://www.governmentsecurity.org/comsec/googletut1.txt>
- [18] i-Hacked.com, "Google Hacking at its Finest," (Retrieved from the Web April 15, 2005).  
<http://www.i-hacked.com/content/view/23/42/>
- [19] Delaney, K.J. "Identity Theft Made Easier." The Wall Street Journal, March 29, 2005. (Retrieved from the Web April 15, 2005).  
[http://www.choicepoint.com/privacyatchoicepoint/consumers\\_article\\_032905a.html](http://www.choicepoint.com/privacyatchoicepoint/consumers_article_032905a.html)

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
**to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure**  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

## ANNEX II

### A Probability of I

By Dr. Barbara Endicott-Popovsky

**Note: The following information is presented for those who struggle communicating what we see and know with our senior leadership.**

If you protect a luscious, valuable, amazingly tempting data object, the probability of its being stolen is 1. It's as sure as death and taxes. It's only a matter of an attacker's time and resources before it's gone; these are no obstacles to determined adversaries like nation states and organized crime. So why don't our corporate leaders 'get' this certainty? Why are so many like Target, caught off guard?

This question has bugged me ever since I attended a professional conference that featured a panel of top executives from the Fortune 500 congratulating themselves on their unbreakable perimeter defenses that 'no attacker could penetrate.' As I listened I had images of the Titanic going down and couldn't help raising my hand to ask if any had considered how to defend against other kinds of exploits that avoid firewall penetration, like Stuxnet (which I briefly explained). Why bother when compromising humans is so easy? Or as a colleague is fond of saying, 'there is no firewall for stupid!' [1]

There was stunned silence from the speaker and then a mumbled 'we probably need to explore other scenarios.' One of the panelists under his breath muttered, 'we just installed a USB port in....' and proceeded to describe a sensitive installation that would be a delightful target for the ill-intended.

How did we get here? How are so many aspects of society so blind when the consequences of cyber theft and compromise are so stark?

#### Lagging behind in the Information Age

I think you can agree that we all struggle to stay current with technology and often don't grasp the unintended consequences of the shiny new innovations that we embrace. We're transitioning to the Information Age, watching the Industrial Age fade in the rear view mirror. According to Covey [2, 3], this transforms our way of living in profound ways—how we advance in the world, how we work, our sense of time, how we problem solve, how we learn.

To gain appreciation for the enormity of what we've done to ourselves with our embrace of technology, I've been reflecting on the table below, imagining myself in each age, visualizing my life in every detail. I marvel at the unintended consequences I've discovered as a result, and I work in this field!

I'm not suggesting we become luddites and live by candlelight; I am suggesting that we consider where we've come from and where we're now living. Morris Massey's training seminar called '*What You Are Is Where You Were When*' makes the case that our values are fixed in the paradigm existing when we turned age 10 [4]. From then on, we interpret what we see and weigh our decisions through that lens. Where were you at 10?

I invite you to take quiet time and contemplate this question. While you may be among the enlightened, technically, way ahead of most in 'getting' technology, ask yourself how likely is it that those who are leading us politically and economically really do understand the impacts of the transformation we are still in the

Table 1. Transformative Paradigms Source: Adapted from [2]

Attribute	Agricultural Age	Industrial Age	Information Age
<b>Wealth</b>	Land	Capital	Knowledge
<b>Advancement</b>	Conquest	Invention	Paradigm Shifts
<b>Time</b>	Sun/Seasons	Factory Whistle	Time Zones
<b>Workplace</b>	Farm	Capital equipment	Networks
<b>Organization Structure</b>	Family	Corporation	Collaborations
<b>Tools</b>	Plow	Machines	Networked Computers
<b>Problem-solving</b>	Self	Delegation	Integration
<b>Knowledge</b>	Generalized	Specialized	Interdisciplinary
<b>Learning</b>	Self-taught	Classroom	Online

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
**to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure**  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovskiy**

A PROBABILITY OF I (CONT.)

middle of accomplishing. An exercise such as this might help you gain insight into why cybersecurity is something those at the top rarely grasp. Most likely, when they were 10, they were in the heart of the Industrial Age developing their world view from that paradigm. Is it any surprise they need extra help in thinking through cyber risk?

**Surrounded by Oceans and 'Soft' Countries**

At the heart of this transformation is our symbiotic relationship with the Internet. Table 2, brings home its pervasiveness; and we're only at the beginning! With only 25% of the world's population surfing the Net today, think how our lives will change as saturation increases and we move increasingly online. Further, consider the continued effects of the clash of cultures as radically different countries become side-by-side neighbors online.

In this country we have had the luxury of two oceans on either side, left and right, with two 'soft' countries above and below us that are basically cooperative and 'like us.' This can inure us to what we have done by becoming virtual next door neighbors with all of our friends online in the Table below. I'm fond of telling my students that my mother named six kids that I was absolutely to avoid like the plague when I was growing up. I still remember the name of the boy at the top of the list. These were perennial troublemakers in the neighborhood; if you hung around them, you were assured of no-good. (I can attest to it, having smashed a church window, by accident, playing softball with a couple of them!)

Now we are side-by-side with cultures and countries radically different from our own, with very different world views about PI, freedom, ethics, etc. (Read The Lure [5].) Why do we expect them to behave like us? Why should they?

As we smash Industrial Age infrastructure, replacing it with Information Age interconnectedness, unintended consequences will continue to unfold: online fraud, illegal downloads, continuing threats to security and privacy, wrongful prosecution for misunderstood Internet crimes, and on and on [4,5,6,7]. Like Mickey Mouse, as the Sorcerer's Apprentice in *Fantasia*, we have assumed the wizard's powers without anticipating the risks [8]!

What was meant for good has ushered in unexpected troubling dislocations.

**References**

- [1] Hamilton, M., CISO of the City of Seattle. (2013). Guest Lecture INEX571 Seminar on Information Assurance, University of Washington.
- [2] Covey, S. (1989) *7 Habits of Highly Successful People*. New York: Free Press.
- [3] Covey, S. (2005) *The 8th Habit: From Effectiveness to Greatness*. New York: Free Press.
- [4] Massey, M. 'What You Are Is Where You Were When'
- [5] Schroeder, S. (2011). *The Lure*.

**About the Author**

**Barbara Endicott-Popovskiy**, Ph.D. CRISC (University of Washington), Executive Director Center for Information Assurance and Cybersecurity; Professor UW Institute of Technology Tacoma; Academic Director Masters in Infrastructure Planning and Management in Urban Planning; Fellow Aberystwyth University, Wales; member American Academy of Forensic Scientists. Her 20-year career in industry encompassed executive and consulting positions in IT architecture and project management. Her research interests include enterprise-wide information systems

security, forensic-readiness, secure coding practices. She earned her Ph.D. in Computer Science/Computer Security (University of Idaho, 2007); MS in Information Systems Engineering (Seattle Pacific University, 1987); MBA (University of Washington, 1985); BA (University of Pittsburgh). **19**

Table 2: World Internet Usage (Source: Internet World Stats: <http://www.internetworldstats.com/stats.htm>) [3]

World Regions	Population (2012 Est.)	Internet Users Dec. 31, 2009	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2012	Users % of Table
Africa	1,073,380,925	4,514,400	167,335,676	15.6 %	3,606.7%	7.0 %
Asia	3,922,066,987	114,304,000	1,076,681,059	27.5 %	841.9 %	44.8%
Europe	820,918,446	105,096,093	518,512,109	63.2 %	393.4 %	21.5%
Middle East	223,608,203	3,284,800	90,900,455	40.2 %	2,639.9%	3.7 %
North America	348,280,154	108,096,800	273,785,413	78.6 %	153.3 %	11.4%
Latin America/ Caribbean	593,688,638	18,068,919	254,915,745	42.9 %	1,310.8%	10.6%
Oceania / Australia	35,903,569	7,620,480	24,287,919	67.6 %	218.7 %	1.9 %
<b>WORLD TOTAL</b>	<b>7,017,846,922</b>	<b>360,985,492</b>	<b>2,405,518,376</b>	<b>34.3%</b>	<b>566.4 %</b>	<b>100.0%</b>

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

## ANNEX III

Communications Security, Reliability and Interoperability Council  
 Working Group 7 – Cybersecurity Workforce Development  
 DRAFT Final Report

### I Executive Summary

Cybersecurity refers to the technologies and techniques used to protect information and systems from being stolen, compromised or attacked. This includes unauthorized or criminal use of electronic data, attacks on networks and computers, and viruses and malicious codes. Cybersecurity is a national priority and critical to the well-being of all organizations.<sup>1</sup>

Over the past five years, cyberattacks have been on the rise in frequency and impact. Headline grabbing attacks at Sony Pictures exposed copyright content, company confidential data and personal privacy information that forced Sony to shut down their online services for weeks. The Ashley Madison data breach resulted in the exposure and public posting of some very personal data. And, the Office of Personnel Management was the target of a persistent breach that compromised tens of millions of records of personal information related to current and past federal workers including security clearance information.

However, it is not just data that is being stolen. Researchers demonstrated the ease with which they were able to wirelessly exploit and gain control of the steering, brakes and transmission of a Jeep Cherokee. Recently, suspected state sponsored cyberattacks in the Ukraine caused a six hour power outage for some 80,000 customers. This sophisticated and highly coordinated attack combined Telephone Denial of Service (TDOS), hacked control systems, and compromised monitoring to attack the critical infrastructure while “blinding” the utility operator from detecting the problem. It is believed to be the first critical infrastructure attack of its kind and underscores the national security implications of cybersecurity.

Anticipating the potential kinetic impacts of a cyberattack on critical infrastructure, President Obama released Executive Order 13636, Improving Critical Infrastructure Cybersecurity, citing the need for improving cybersecurity in response to the repeated cyber intrusions into critical infrastructure.<sup>2</sup> The cornerstone of this order is the enhancement of security and resilience of critical infrastructure through the voluntary, collaborative efforts of federal agencies and commercial industry.

Cybersecurity professionals have unique skills, are in short supply, and are vital to our nation's security. As a result, competition for talent is fierce and establishing a strong team is essential. This requires organizations to tailor how they plan for their cybersecurity workforce so they have the right people in the right positions. In the White House Executive Order 13636, Improving Critical Infrastructure Cybersecurity, the President assigned the Department of Homeland Security (DHS) the leadership role to work with Federal Agencies and sector specific regulators to help ensure we have skilled cybersecurity workers today and a strong pipeline of future cybersecurity leaders. One of the results of this mission, is the collaborative effort with the National Initiative for Cybersecurity Education (NICE) that resulted in the development of the National Cybersecurity Workforce Framework (NCWF).<sup>3</sup>

<sup>1</sup> Cybersecurity Workforce Development Toolkit, How to Build a Strong Cybersecurity Workforce, <https://niccs.us-cert.gov/>

<sup>2</sup> Executive Order 13636 dated February 12, 2013

<sup>3</sup> In November, NIST released for comment an update in partnership between NICE and DHS that changes the nomenclature back to the NICE Cybersecurity Workforce Framework

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

**Communications Security, Reliability and Interoperability Council**  
**Working Group 7 – Cybersecurity Workforce Development**  
**DRAFT Final Report**

The mission of the Communications Security, Reliability and Interoperability Council (CSRIC or Council) is to provide recommendations to the Federal Communications Commission (FCC) to ensure, among other things, optimal security and reliability of communications systems.<sup>4</sup> Furthermore, the Council's recommendations specifically address the prevention and remediation of detrimental cyber events. Working Group 7 of the CSRIC V is specifically chartered to provide recommendations for the CSRIC's consideration regarding any actions the FCC should take to promote improvements in cybersecurity workforce development.<sup>5</sup>

The CSRIC V Working Group 7 has been tasked to examine and develop recommendations for the CSRIC's consideration regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field.

Specifically, this working group will leverage existing work in this context to enhance the volume and quality of the workforce, including<sup>6</sup>:

- (1) demonstrating the application of the National Cybersecurity Workforce Framework (NCWF) to the common and specialized work roles within the communications sector;
- (2) identifying any gaps or improvements in the NCWF for evolving work roles or skill sets that should be included in sector members' workforce planning; and
- (3) identifying, developing, and recommending best practices and implementation thereof to mitigate insider threats, including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities within the communications sector and particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. In this respect, the working group should consider means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

This Final Report builds upon the Interim Report that specifically addressed the demonstration of the applicability of the NCWF to the Communications Sector and the identification of gaps or improvements to the NCWF. Further, it documents the approach that the Working Group 7 applied to identify, develop and recommend best practices for consideration by the CSRIC V membership for inclusion in the Final Report. In order to manage the scale of the task, Working Group 7 chose to segment the information gathering and analysis process with targeted findings specific to each segment. We then identified best practices based on our analysis for each segment for consideration. This Final Report presents those Best Practices deemed to be most appropriate and impactful for consideration by the CSRIC V as recommendations to the FCC and the Communications Industry as a whole.

<sup>4</sup> Charter of the FCC's Communications Security, Reliability and Interoperability Council

<sup>5</sup> CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016

<sup>6</sup> The FCC CSRIC Working Group Description references the NICE CWF; Working Group 7 has opted to refer to this framework using the April 2014 NICCS designation of the National Cybersecurity Workforce Framework (NCWF) for external consistency

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

Communications Security, Reliability and Interoperability Council  
 Working Group 7 – Cybersecurity Workforce Development  
 DRAFT Final Report

The National Cybersecurity Workforce Framework (NCWF)<sup>7</sup> provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Competencies, and KSAs.

1. **Categories** are common major functions regardless of job titles or other occupational terms.
2. **Specialty Areas** are common types of cybersecurity work which are grouped with similar areas under a specific Category.
3. **Competencies** are areas of expertise required for the successful performance of a job function; these are defined in the framework through the association of specific KSAs.
4. **Knowledge, Skills and Abilities (KSAs)** are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training experience, education, or training.

Working Group 7 (WG7) leveraged the prior NCWF analysis and process completed by the Financial Sector as a best practice to accelerate our task of evaluating the NCWF. The summary conclusions are that the NCWF is a viable, flexible framework that can and should be applied to the Communications Sector for Cybersecurity Workforce Development Planning. Building on this finding by the Working Group members, we proceeded to complete the initial evaluation of the “building blocks” – Categories, Specialty Areas, Competencies, and KSAs – for gaps and improvements that should be included in the application of this dataset to the Communications Sector. Our work product is attached to this Final Report as Appendices 1 and 2. It was also delivered to the FCC as a working database in Microsoft Excel format for unrestricted use.

We recognize that cybersecurity workforce development is undergoing rapid change and evolution. This Final Report provides a lexicon that can be used to articulate the specific Workforce needs of the Communications Sector for roles involving cybersecurity. However, it is a static dataset and needs to evolve as the NCWF matures and Cybersecurity Workforce Development Planning gains maturity in our respective organizations. As part of the Final Report, WG7 provides specific recommendations for consideration by CSRIC on a process for adaptation and improvement of the sector specific dataset.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

## ANNEX IV

### Searching and Developing Cybersecurity Talent

Barbara E. Endicott-Popovsky\*  
 endicott@uw.edu  
 Viatcheslav M. Popovsky\*\*  
 dr\_popovsky@hotmail.com

University of Washington\*  
 Seattle, Washington  
 University of Idaho\*\*  
 Moscow, Idaho

#### Abstract -

*The lack of talent in the field of cybersecurity is keenly felt across all sectors of the economy—industry, government, military, academia [1]. While cybersecurity education has been a national priority, there still are thousands of cybersecurity jobs going unfilled and the gap will take a long time to close [1]. Of further concern, the authors have gathered anecdotal evidence that employers in both government and industry consider many recent cybersecurity graduates woefully unprepared for the realities of the workplace, taking too long to become effective. This paper describes one university's approach to address both the supply and preparedness problems, beginning with the application of the theory of pedagogical systems and methodology from sport and physical culture science and pedagogy to introducing the first iteration of a cooperative learning model—inspired by this theoretical base and experience with its application—designed specifically to develop and graduate 'breach-ready' cybersecurity professionals.*

#### Categories and Subject Descriptors

K.3.2 [Computers and Education]: *Computers and Information Science Education.*

**General Terms:** *Cybersecurity education, pedagogy, cooperative learning*

**Keywords:** *Cybersecurity talent selection, pedagogical system, career development, cooperative learning pilot program*

#### 1. INTRODUCTION

Responding to the well documented deficit in cybersecurity talent in the U.S. [1], the Center for Information Assurance and Cybersecurity (CIAC) at the University of Washington, an NSA/DHS CAE-CDE, has created a unique laboratory for unleashing student potential by leveraging the interdisciplinary science and system-activity approach ingrained in the theory and methodologies of physical culture science and advanced sports pedagogy and applying that construct to cybersecurity education [2]. This

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

scientifically-proven sport talent search system, developed by such luminaries as V.M. Zatsiorsky, N.G. Bulgakova, U.F. Kuramshin , and etc., allows individuals to find their appropriate physical activity aligned with their level of performance, authentic nature, and unique abilities [3, 4, 5, 6, 7]. This inevitably leads to superior performance and a fulfilling sport career, culminating in the athlete's personal happiness and sense of well-being.

Historically, sport orientation and selection science were rooted in psycho-physiological research from professional orientation studies, especially for selecting those for high risk, stressful, performance-demanding careers like airline pilot, special-forces military, and air traffic controller. The authors hypothesized that the field of cybersecurity, being similarly stressful,<sup>18</sup> would benefit from the application of this same research and have spent over a decade in actualizing this idea through individual courses and programs, writing extensively about their results in numerous publications referenced in [2]. The synthesis of that work into a repeatable methodology, and the initial draft of a cooperative learning model designed to address developing and producing 'breach ready' graduates, is discussed in this paper.

## 2. COMMON FACTORS FOR DEVELOPING TALENT

Studying the development of athletic talent through the work of physical culture educators [3, 4, 5, 6, 7], the authors identified four common factors that are applicable to achieving success in any field and have applied them to their cybersecurity education programs:

**FACTOR 1. Talent Search Process.** Talent search is a continuous process, not a single event. Once talent is identified and selected, it must be continuously developed in a process that unifies nature and nurture described by W. Kistler, Founder of the Foundation for the Future [7]. Kistler suggests that nature and nurture co-exist in successful individuals as a 'unity of multiplication.'<sup>3</sup> Attention to both in the talent search process amplifies growth and development.

The authors have applied this concept to developing an approach that helps students select their ideal cybersecurity career pathway that leverages their nature—in-born skills/ abilities—with an appropriate plan to nurture those talents through continuous mentoring. An example of one of the tools used in this approach is the National Initiative for Cybersecurity Education (NICE) framework,<sup>19</sup> US National Institute of Standards and Technology (NIST) which provides guidance regarding necessary knowledge, skill, and abilities (KSA's) required for 32 different career pathways in cybersecurity.<sup>4</sup> Their students are asked to identify pathway/s that resonate with their interests, do a gap analysis with their current conditions and design a way forward to eliminate those gaps with a professionalization plan augmented with continuous mentoring from professionals and staff which direct students to free online courses and resources to fill in any gaps they may discover based on assessments provided each student.

<sup>18</sup> One CISO, Chief Information Security Officer, from a major local firm indicated that after 3 major incidents employees need a sabbatical to recover!

<sup>19</sup> Found at <http://csrc.nist.gov/nice/index.htm>

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

**FACTOR 2. Intense Personal Interest.** An athlete's passion for their chosen sport is accompanied by a desire, almost a craving, to work enthusiastically hard on self-improvement, allowing them to succeed and flourish in their field. The authors share the opinion of some researchers [5, 7, 8] that a person's commitment to persevere, in spite of obstacles, and their resilience to overcome setbacks in order to strive for their dreams are a reflection of their internal nature. In other words, intensity to succeed works from the inside out, leveraging passion and predisposition to a preferred activity.

In cybersecurity education programs at the Center for Information Assurance and Cybersecurity (CIAC),<sup>20</sup> students are offered a wide array of outside professional activities to experiment with finding their passion in cybersecurity and are encouraged to take multidimensional career assessment tests that measure interests, skills and work styles to help them identify what they like to do and what they are good at doing. These activities focus students on finding their ideal pathway in cybersecurity. When a student is passionate about their choice they become dedicated to learning—a basis for becoming a lifelong learner which is essential for success in this fast-moving field. Passionate students join cyber competitions, spend extra time on homework and seek mentors—all of which accelerates their learning and growth.

**FACTOR 3. Individualized Approach to Coaching and Mentoring.** The availability of willing coaches and mentors who provide personalized individual feedback for continuous improvement—both good and corrective—additionally accelerates an athlete's growth.

For the cybersecurity student in the Center's programs, mentoring is designed-in through a professional development service that works with students individually to partner with industry and government that provide advising, monitoring, and feedback throughout the learning experience. The authors are in the early stages of exploring ways in which the labor intensive nature of this process can be reduced so significant scaling is possible.

**FACTOR 4. Well-Structured Nurturing Pedagogical Process.** Integrating highly motivated individuals (students, athletes, professionals) into a valid cooperative and competitive educational environment, combined with a well-designed pedagogical progression for achieving measurable personal (and team—in the case of sports) goals, accelerates an athlete's learning and improvement.

Applying this factor to cybersecurity education, a pedagogical process has been developed that combines work in the real world with existing studies in one of several academic degree programs and professional certificates designed to move students in planned stages from textbook knowledge to advanced problem solving of current cases presented by role model practitioners. Assignment assessments often include practitioner feedback, providing students measurable results that can reassure them of their developing competency.

This pedagogical system, designed to produce cybersecurity professionals, views incoming students as raw material to be processed! A unique blending of pedagogical approaches [9, 10, 11, 12], Figure 1 represents the pedagogical process that produces cybersecurity expertise as the outcome. This operational

---

<sup>20</sup> These programs are available for dissemination to other interested cybersecurity educators.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

pedagogical system is derived from intensive research into two schools of thought regarding the theory of pedagogical systems whose originators are Drs. N.V. Kuzmina and V.P. Bespalko, respectively.<sup>21</sup> This is a high-level metasystem that, when applied to developing a specific course or program, produces a specific instantiation, many of which have been published as described in [2].

KBP is composed of five elements—**students, teachers, goals, content** and **didactic processes**—the first two are intelligent elements, the **teacher** and the **student**; the remaining three are infrastructure elements—the **goals, content, and didactic processes** of the curriculum. All elements are subject to varying rates of change and adaptation over time requiring that programs continually update. All elements function as an integrated whole and operate within a larger dynamic environment with constantly evolving threats, vulnerabilities and technical innovation. Context informs the elements of the model.

In any given context, a specific instructor with their own specific slice of cybersecurity expertise is responsible for organizing content and selecting didactic processes designed to address the needs of students who are central to the pedagogical process. The orientation of the instructor will affect content delivered and didactic processes engaged. Students enter the learning experience with potential, and graduate with a professional orientation.

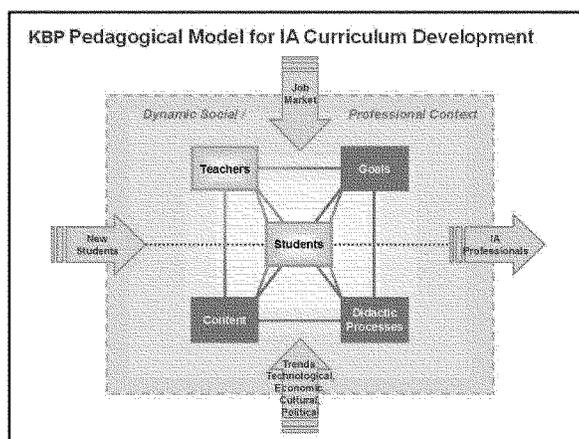


Figure 1: The KBP Pedagogical Model for Production of Cybersecurity Professionals

By describing each component of the model in relation to goals drawn from the current context, an educational plan is developed, iteratively. According to Bespalko and Kuzmina, the

<sup>21</sup> In acknowledgement, the authors named the model KBP (Kuzmina-Bespalko-Popovsky).

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

more precisely the five components are characterized—along with the connections among them—the more repeatable and predictable the learning results [9, 10].

Over time, as context changes, the entire system is affected, as well as any resulting curriculum. Each element must be re-defined with any update until all five are specified in relation to one another. By continuously updating the curriculum in this manner, students are kept current and graduates remain competitive. It is also an efficient approach to curriculum maintenance in a constantly changing field.

The Didactic Processes element deserves particular attention. The authors incorporate an activity-based learning approach developed in partnership with the regional cybersecurity community, academic researchers, and industry [13]. Since emphasis is placed on professional development, students are encouraged to learn from every possible resource: educational partners throughout the State, certifications, the Center's vast network, professional memberships. Knowledge is treated, not as an end goal in and of itself, but rather as a tool for solving real world problems, creatively and independently. Tools need continual sharpening.

A major feature of curriculum design is integration of cybersecurity practice into student experience everywhere possible. Active incorporation of this perspective helps students triage between the classroom and the real world so they can solve problems creatively, as opposed to applying a checklist from a book. Techniques for accomplishing this include:

- Recruit recognized cybersecurity experts as instructors.
- Employ guest lecturers for currency, role models, and job sources.
- Incorporate capstone projects from industry and academic research to develop problem-solving capabilities in students.
- Offer internships so students can immediately apply what they learn.

The end result is production of critical thinkers who are able to reflect on practical experiences, extrapolate generalizations through induction—extending their knowledge. Criteria for measuring results include students' contributions to science and industry.

### 3. RESULTS OF APPLYING THE KBP MODEL

The supply deficit of adequate numbers of skilled cybersecurity professionals is a well-recognized problem.<sup>22</sup> For more than ten years, the authors have applied the above four factors to this problem in order to develop sufficiently trained, ready-to-work, professional cybersecurity graduates. The educational approach that the authors created has a proven track record for producing talent in significant quality and quantity to have earned national recognition.

University of Washington programs following this approach have consistently earned a top-10 ranking in cybersecurity education from various authorities in the field [14]. Further, one of the programs, a

<sup>22</sup> There are many studies that confirm an extreme deficit of needed cybersecurity talent. For this paper, the authors refer readers to the following 1) Cybersecurity skills gap: <https://securityintelligence.com/five-must-read-articles-on-the-cybersecurity-skills-gap/> and 2) Burning Glass study: [http://burning-glass.com/wp-content/uploads/Cybersecurity\\_Jobs](http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs).

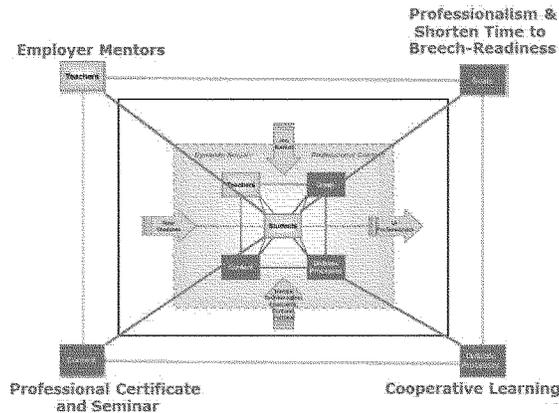
**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
**to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure**  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

professional certificate,<sup>23</sup> has earned US Western Regional awards from the University Professional and Continuing Education Association (UPCEA) for teaching and curriculum/pedagogy, as well as numerous individual teaching awards for instructors. More importantly, over 600 students have graduated from this one certificate program, alone, many of whom have now moved into senior management ranks and are reaching back to hire program graduates.

The authors have relied on physical culture and sports pedagogy research to identify those factors that enhance talent development and have applied them to the forming profession of cybersecurity. The results have demonstrated the efficacy of transferring physical culture science and pedagogy to another field.

**4. COOPERATIVE LEARNING PILOT**

Recently, the Center has moved beyond internships to develop a cooperative learning<sup>24</sup> pilot in partnership with local industry which extends the pedagogical model (*Figure 2*) where the original KBP Pedagogical Model overlays a repeat pedagogical model, consisting of the four-elements from the employer's view representing the coop program. The fifth element, students, is the same for both layers of the model.



*Figure 2: The KBTP Pedagogical Model in Partnership with Employers*

<sup>23</sup> The Information Security and Risk Management (ISRM) certificate.

<sup>24</sup> By cooperative learning, the authors mean a structured approach that combines classroom-based education with practical, aligned experience in a real world environment.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

The didactic process of incorporating cooperative learning in the student's employment is structured to address the goal of shortening the time to 'breach-readiness' through the active involvement of employer mentors and content from a professional certificate and seminar.

<b>I. PERFORMANCE</b>		
<b>Professionalism</b>	<b>Problem Solving Efficacy</b>	
	Individual	Team
<b>Continuous Learning</b>		
<b>II. KNOWLEDGE - SKILLS</b>		
<b>Policy</b>	<b>Procedures</b>	<b>Technology</b>
<b>III. ABILITIES</b>		
<b>Interest &amp; Motivation</b>	<b>Education</b>	<b>Experience</b>
	(Degree, GPA, Certifications)	

*Figure 3: Cybersecurity Professional Readiness Model (CPRM)*

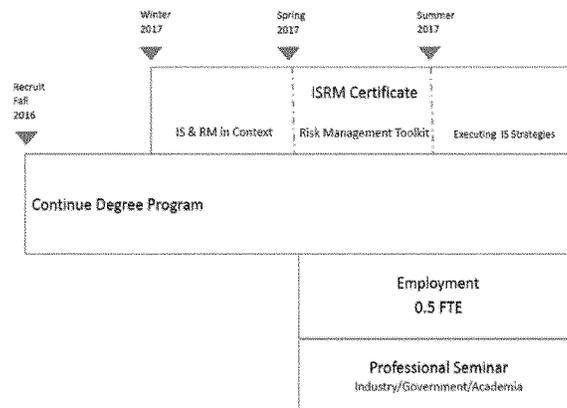
Another stated goal for this expanded pedagogical model is achieving professionalism as defined in *Figure 3*. There are three dimensions of professionalism developed in any Center program. (Professional preparation is the reason given for naming the Center among the top 10 best places to study cybersecurity in the nation in 2014 [14].) These are:

- **PERFORMANCE** is defined as exhibiting professionalism and problem solving efficacy on the job, and indulging in a program of continuous learning.
- **KNOWLEDGE – SKILLS** acquisition is defined as understanding policy development and implementation and effective application of procedural and technological controls—the 'rules and tools' of cybersecurity.
- **ABILITIES** as evidenced by the following: a student's interest and motivation, their educational accomplishments and their experience—especially experience relevant to cybersecurity and the level of responsibility they have attained.

Application of the Cybersecurity Professional Readiness Model (CPRM) could be applied as a measuring instrument and can guide careers toward preparation for positions at the operating, managerial

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

or executive levels, as well as identify gaps in preparedness, so that they can build plans to eliminate and compensate for any deficiencies. This is both a tool for selection and continuous guidance.<sup>25</sup>



*Figure 4: Cybersecurity Cooperative Learning Pilot*

Combining the models in *Figures 2 and 3*, the authors devised a cybersecurity cooperative learning pilot (*Figure 4*) where students maintain their current academic load in the last year of their degree programs and, in addition, opt into an integrated program of professional instruction and half-time industry employment. The additional professional education includes: 1) an information security and risk management (ISRM) certificate that covers all the necessary KU's required of a CAE-CDE and 2) a professional seminar conducted by the university in partnership with industry to help students triage their work experience with what they've learned formally in the classroom. The addition of the professional seminar and certificate elements in the pilot are expected to accelerate student work readiness when they formally graduate and give students the opportunity to reflect on what they are learning in the classroom and learning on the job, including teamwork, and the experience of adjusting to the working world. Table 1 provides an overview of the pilot program for AY 2016-17.

<sup>25</sup> CPRM is derived from the work of a Russian sports pedagogical research group who used these three levels—Performance, Knowledge/Skills, and Abilities—for managing and selecting high performance athletes. The authors have adapted and applied this model for the selection and management of cybersecurity talent [15, 16].

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: Private Sector and Government Challenges and Opportunities**  
**to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure**  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

*Table 1. Cooperative Learning Pilot Project Plan*

<b>Cooperative learning program 2017</b>		
<b>Quarter</b>	<b>UWB CIAC contributions</b>	<b>Employer contributions</b>
Fall 2016	Recruit students (4 Business, 4 STEM), assess proficiencies, create individual plans for meeting requirements. Establish cohort. Establish assessment and review process for the cooperative learning program.	Participate in selection of students and establishment of cohort. Participate in plan for program assessment and review.
Wtr 2017	ISRM-1: <i>Business context for cybersecurity.</i> Fulfilling ISRM prerequisites Host cohort meetings	On-site 0.5 FTE employment Host cohort meetings.
Spr 2017	ISRM-2: <i>Risk management.</i> Capstone course (for some) Host cohort meetings	On-site 0.5 FTE employment Host Professional Development Seminar
Sum 2017	ISRM-3: <i>Solving problems.</i> Award ISRM certification. Capstone course (for. some students) Program review and assessment. Host cohort meetings	On-site 0.5 FTE employment Host Professional Development Seminar Participate in program review and assessment.

#### 5. CONCLUSION AND FUTURE WORK

In addition to support from industry, government is also a partner in this pilot. The National Information Assurance Education and Training Program (NIETP) is interested in the development and dissemination of the cooperative learning model and the lessons learned during the pilot period. This is conceived as a two-year pilot. This first year 10 students, constituting one cohort, are engaged with one employer. Students were selected based on technical foundation, interpersonal skills, team participation, and collaborative problem-solving. ISRM certificate scholarships were provided. A second year of the pilot will be conducted with more industry partners for the purposes of incorporating lessons learned from the first year and refining and generalizing the model.

In the second year, 2 new industry partners will be added to test the ability of the program to scale allowing for 3 cohorts of 10 students each. Recruiting is planned for Summer 2017 with admittance into the pilot for AY 2017-2018. The professional education elements will run in three consecutive quarters, this year beginning in Fall 2017 – Winter 2018 – Spring 2018. The data collected will provide insight into several questions: 1) whether/how this program will/can be scaled, 2) whether this kind of a program accelerates cybersecurity job readiness, 3) what are best practices for conducting such a program.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
***to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Dr. Barbara Endicott-Popovsky**

**REFERENCES**

- [1] Burning Glass. Job Market Intelligence: Cybersecurity Jobs (2015). Retrieved April 15 at: [http://burning-glass.com/wp-content/uploads/Cybersecurity\\_Jobs\\_Report\\_2015.pdf](http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf)
- [2] Endicott-Popovsky, B. and Popovsky, V. Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. *ACM Inroads*, 5(1), 57-68 (2013).
- [3] Yakhontoff, E.R. Didactical reformation of the content of athletic and pedagogical coaching activities in sports games. *Autorferat of Diss.*, Lesgaft Academy, St. Petersburg: Russia. (1995).
- [4] Popovsky, V. The System of Continuous Pedagogical Practice in IPC. S.P Evseev and Popovsky, V. (Ed.) *Organization and Methodology of Continuous Pedagogical Practicums in the Institute of Physical Culture: Academic Methodological Benefits*, Leningrad: Lesgaft Institute of Physical Culture (1988).
- [5] Kuramshin, U.F. and Popovsky, V. *Find your Talent*. Leningrad: Lenizdat (1987).
- [6] Agevec, V.U., Popovsky, V., Filippov, S.S. *The Mini-Department of the Institute of Physical Culture—A New Form of Student Work. Theory and Practice of Physical Culture*, Moscow: Russia, No 11 (1984).
- [7] Il'in, E.P. *Psychophysiology of Physical Education*. Prosvetshinie: Moscow, Russia (1980).
- [8] Kistler, W. *Reflections on Life*. Presentation: Foundation for the Future: Bellevue, WA (2003):
- [9] Kuzmina, U. F. *Fundamentals of Pedagogy of Higher Education*. Leningrad: Lenizdat (1972).
- [10] Bepalko, V. P. *Fundamentals of Theory of Pedagogical Systems*. Voronege: Voronege University (1977).
- [11] Bloom, B.S., Mesia, B.B. and Krathwohl, D.R. *Taxonomy of Educational Objectives*. New York: David McKay 1964).
- [12] Hutton, G. *Backward curriculum Design Process*. Retrieved May 1, 2003 from the World Wide Web: [http://www.g4v.com/~glen.hutton/ED3601/BackwardDesignFeb11\\_03.pdf](http://www.g4v.com/~glen.hutton/ED3601/BackwardDesignFeb11_03.pdf)
- [13] Endicott-Popovsky, B. and Popovsky, V. Activity-based approach to developing professionals within higher education programs. 1st Annual Conference at the Department of Physical Education. St. Petersburg, State Institute of Film and Television. St. Petersburg, Russia (2015).
- [14] Ponemon Institute. 2014 Best Schools for Cybersecurity (February 2014). [http://www.hp.com/hpinfo/newsroom/press\\_kits/2014/RSAConference2014/Ponemon\\_2014\\_Best\\_Schools\\_Report.pdf](http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf)
- [15] Kuznetsov, V.V. Novikoff, A.A. *To the Problem of Modeling the Characteristics of High Performance Athletes. Theory and Practice of Physical Culture*. Vol.1. Moscow, USSR. pp. 50-62 (1975).
- [16] Shustin, B.N. and Bryankin, C.B. Using "Models of High Performance Athletes" for Selection and Sport Orientation. *Proceedings of Problems of Selection of Young Athletes*. Moscow, USSR. pp. 11-13 (1976).

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. William Sanders**

**Questions from Chairman Lisa Murkowski**

**Question 1: Cyber Resiliency** – Your assessment that the focus of the majority of research has been on the prevention of cyber intrusions on our grid strikes me as correct. Thus far our country has not suffered an interruption of power because of a cyberattack. However, cyber threats are constantly evolving and the focus of your research – cyber resiliency – is an important next phase. What can the federal government do to help improve outcomes and increase cyber resiliency? Do you share Mr. Lee's concerns that more regulation at this time could be counterproductive to our cybersecurity?

*As stated in my prepared comments, work to define such cyber resiliency architectures that protect against, detect, respond to, and recover from cyberattacks that occur is critically needed.*

**To do this, I urge that the committee work to implement Overarching Recommendation Number 5 in the National Academy report that was the subject of the hearing, namely:**

**“The Department of Energy should embark upon a research, development and demonstration program that makes use of the diverse expertise of industry, academia, and national labs that results in a prototypical cyber-physical-social control system architecture for resilient electric power systems. The program would have the following components: 1) A diverse set of sensors (spanning the physical, cyber, and social domains), 2) a method to fuse this sensor data together to provide situational awareness of known high quality, and 3) an ability to generate real-time command and control recommendations for adaptations that should be taken to maintain the resiliency of an electric power system.”**

**An effective cyber-physical-social control system architecture will only be realized with the integrated work of academia, industry, and government, and a “moon-shot effort” is needed to achieve the goal. Significant research work to date has shown us that achieving this goal is possible, but a much more intense effort is needed now. Time is running out.**

**Question 2: Training Staff in Control Rooms** – Mr. Lee (DRAGOS) has made the point that we cannot overlook the critical role that effective cyber security professionals must play. One of the best ways to be prepared for an attack of any sort is to be prepared and trained for responding to that attack.

- I can envision two types of training for an attack. The first would involve the Information Technology (IT) specialists that work behind the scenes in keeping computers up and running throughout the grid. The second would involve the actual operators of those computers. Are both receiving the best training that they can get?

**The training of both types of specialists is critical, as you hypothesize. This training is currently very uneven, with good training being provided in some companies, and very little in others. Appropriate tools are also critically needed to enable IT**

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Dr. William Sanders**

**specialists and operators to have the situational awareness they need to understand and react to attacks that occur. More specifically, in addition to the cyber-physical-social control system architecture described above, software tools are needed to provide situational awareness in real time to grid operators, and software tools are needed to discover vulnerabilities (e.g., firewall and device misconfigurations) that are present. Improvements in this area can be made almost immediately, and policies should be developed that cause these improvements to happen.**

- Is the cyber –security training for our grid operators sufficient? What needs to be improved? Is this training reaching down to all grid operators? Or is it only reaching the biggest companies with the greatest resources?

**As stated above, it is uneven, and not uniformly given to all grid operations. Part of the problem is that NERC-CIP regulations only apply to a portion of the transmission grid system, and not very little (if any) of the distribution side. Policies and technologies must be developed so that the entire grid is protected.**

- Since the Ukraine attacks are real-world events where control room operators were forced to handle an unexpected situation --- an event where we've heard that operators discovered that somebody else had remotely hijacked their computers, to what extent are the lessons learned about Ukraine being taught in training classes here in America?

**I do not know the extent to which the lessons learned about Ukraine being taught in training classes the United States.**

**Question 3: Interagency Cooperation** – The National Academies report that you contributed to includes six capabilities that are required to improve cyber resiliency and highlights that these capabilities can only be successful if government agencies, the private sector, and academic institutions work collaboratively to focus the research and development efforts. What do you see as the biggest barrier to getting all of these groups to work together – intragovernmental cooperation, private sector concerns, or are there additional roadblocks?

**There is a genuine desire and willingness for the government, academia, and industry to work together. The success of joint research and development projects in DOE's Office of Electricity clearly shows that this is the case. Additional funding should be provided for more programs of this type, and forums should be convened to ensure that the three groups are connected.**

**Questions from Senator Catherine Cortez Masto**

**Question 1:** What would you suggest the Federal government do to promote the early adoption of the state-of-the-art technologies to protect our electrical infrastructure?

U.S. Senate Committee on Energy and Natural Resources  
March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities  
to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
Questions for the Record Submitted to Dr. William Sanders

**This is a very important question, but one that does not have a simple answer. The complexity of the situation comes from the fact that the power grid spans many governmental jurisdictions (Federal and State) and that the regulation of the pricing of electricity causes free market incentives to not work. The question would be better answered by an economist rather than an engineer, but promoting adoption will clearly require regulation in addition to investment in the development of cost-effective cyber security and resiliency technology.**

**Question 2:** While smart building infrastructure that is connected to the internet is incredibly exciting in its potential for huge energy savings to homeowners and businesses, what protections are in place, or will need to be put in place, to protect them from cyberattacks?

**You are correct in assuming that while smart building infrastructures provide the potential for significant energy savings, they also increase the attack surface of, and hence, risk of a successful cyber attack to the power grid. While it is not clear how far an attack on an individual system could spread, it is clear that the protections that are currently in place, and those that are mandated to be in place, are not sufficient. Standards, and technology to support those standards, must be developed to make building energy management systems more secure and resilient. This will require a two-pronged approach – both through technological advances that make such systems more secure and resilient, and through the development of policies and standards that require the developed technology to be used. As with the other recommendations that I have made in response to these questions, it is essential that academia, industry, and government (both Federal and State) work together to develop the required technologies and standards.**

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities***  
*to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Mr. Robert M. Lee**

**Questions from Chairman Lisa Murkowski**

**Question 1: Strategic Challenges** – You raised two strategic challenges in your testimony. First, you said that, “we do not understand the industrial threat landscape,” and second, you said that, “we do not have enough trained professionals focusing on industrial control cybersecurity.” These statements are very clear.

- Please elaborate. Do we understand enough about the industrial threat landscape so that our systems meet a minimally acceptable level of security? Or is the situation more challenging still?

**Answer:** There are baseline minimums for security that have been taken from more general enterprise security and adapted, tried, and tested in the industrial community. As an example, ensuring two-form authentication for connections into industrial environments is a base level of security that is equally applied to enterprise as well as industrial networks. However, much of the guidance in enterprise networks do not apply to industrial networks because the threats and risks are different as well as the mission. As an example, an over focus on patching does not make sense in industrial. There, to date, has been 0 vulnerabilities exploited for disruption or espionage in industrial networks. The functionality adversaries require is already available by a requirement from the mission. In short, we do not have a minimally acceptable level of security for industrial networks to be protected against human adversaries but we do have a minimally acceptable level of security for industrial networks in regards to what is applicable from enterprise security.

- How do we fix these problems? From your testimony, it does not seem that more law or regulation would be helpful at this stage. What steps should this Committee take?

**Answer:** For the second part of the question the only way we really address this, in my assessment, is to take an intelligence-driven approach. That is to say we should learn from what the adversaries are actually doing, what risks they actually pose, and set standards and best practices against those risks appropriate for our different missions and technologies in industrial networks. Because that intelligence-driven approach and the exploration of the threat landscape is in its infancy I do not think more regulations or laws are appropriate. Mandating that utilities report incidents as an example would incentivize them to continue to not look in those networks, if they were to build programs to look for threats they would not become reportable. The Committee should move to incentivize the private sector including the adoption of industrial security specific technologies and approaches in the community especially whereas they are considering threats and not simply compliance and resilience. The Committee should also seek to encourage FERC to either freeze additional regulations, which NERC would support, or focus regulations on program building instead of performance based auditing. The community does not know what performance based auditing against human threats would look like, but programs such as requiring that a "threat

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Mr. Robert M. Lee**

management program" exist at utilities would allow them to address the threats through their own innovation. That would lend to the insights and best-practices we need.

There is currently legislation from Senator King and Senator Risch titled Securing Energy Infrastructure Act that is waiting on action in the upcoming omnibus. I have contributed my thoughts and insights into this legislation through the appropriate process. It prioritizes working with American private sector companies like mine that have unique insights into the threat landscape but does so by providing resources to the utilities in return for insights to be shared to the government. Executing this legislation and ensuring the pilot programs success will be a valuable step forward in understanding the threat landscape and actions needed to address it.

**Question 2: A Human, Not Regulatory Threat** – You testified that, “[m]alware and vulnerabilities are not the threat, the threat is the human adversary and we cannot regulate them away.” Further, you explained that many “patches” designed to protect industrial control systems are of limited value, indicating that there are better ways to allocate what are, after all, and limited resources.

- Please explain how these patch programs can sometimes be counterproductive?

**Answer:** Patching often addresses flaws in software or hardware. In enterprise security that can deny access and functionality over the systems to adversaries. In industrial networks though the flaws often, 64% of the time to be precise against 2017 vulnerabilities advisories, do not deny access or functionality though by fixing them. In other words, the software or hardware already has the functionality the adversary needed. In 2015's attack on the Ukraine power grid there was no flaw exploited in the software to let the adversary remotely open the circuit breakers to disconnect the power. That is functionality the operators of the grid need and use every day, it was just used maliciously. Many times vulnerabilities in industrial just highlight existing proper functionality. In this case there could be a vulnerability that allows an adversary to use the system to open circuit breakers. But to be blunt, who cares? The system's purpose is to open circuit breakers. The adversary would be inefficient to exploit that vulnerability and defenders would reduce no risk by patching it. But by patching the system there is the chance of taking it down or out of use while patching it which can add risk to the operations in that environment. Many industrial networks cannot simply be updated like enterprise networks and the whole operation must come to a halt. This, in some industries, can not only introduce risk but also safety issues. Doing this to patch away vulnerabilities that do not contain risk is an ineffective use of resources.

- Please tell us more about your proposed regulatory freeze, which I gather is intended to allow existing cyber regulations to settle in, so that security professionals can focus on new and evolving threats, and not focus solely on compliance with ever-changing regulations?

**U.S. Senate Committee on Energy and Natural Resources**

**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Mr. Robert M. Lee**

**Answer:** To the second part of the question your statement is absolutely correct. We are in a mode of constantly coming up with new regulations in the electric power sector. Every 2-3 years utilities have to go through new regulations and apply the changes. This does not allow organizations to catch up effectively nor does it allow for a time to evaluate the measures and understand innovative ways forward. Moreover, the regulations to date have all been reasonable requests, but we have exhausted the available reasonable requests. Until we learn more of what we need to do against the adversaries, by taking an intelligence-driven approach and understanding the threat landscape, the regulations may be out of tune with the risks we are trying to reduce. A compliance mentality can quickly form across the sector and given the heavy lifting over the last decade it is appropriate to take a short 3-4 year pause to evaluate where we are and where we are going while allowing organizations to catch up to existing standards.

**Question 3: Five Active Threat Teams** – You testified that, “there are five such threat activity groups active this past year alone who are specifically targeting industrial control networks at infrastructure companies.”

- And while I wouldn't want you to identify the nations where these teams come from— can you give us an idea of your ability to identify the source of those teams? Do you have the technology to say, for example, this team is part of the military of this nation, and they are working in this location?

**Answer:** Dragos often does not take a stance on attribution not because we are not capable of doing so, many of our analysts come from the National Security Agency where we routinely performed that type of analysis, but because it does not provide value to our customers but can be distracting because of media headlines. As an example, the technical defenses needed against an adversary do not change based on their nationality but instead only on their capabilities and tradecraft. That being said, attribution is important for political purposes especially when acted upon. We can confirm that of the groups we are tracking that Russian, Iranian, and North Korean state actors are amongst them. In addition, it is in our assessment at least one of the groups is a previously unknown team and may represent an entirely new threat not currently being tracked in terms of national level adversaries. We have also observed an African nation-state based team targeting small electric and water cooperatives.

**Question 4: E-ISAC and the Private Sector** – I note from your testimony that you work with the E-ISAC a great deal. Please elaborate on how that relationship works.

**Answer:** The E-ISAC has been an immensely useful partner and we work with them a great deal. They are a trusted organization in the electric power community and have an ability to quickly amplify warnings to the sector. Our firm sells technology as its primary revenue generator but we also sell intelligence reports and insights. However, we often assess that some threats the community needs to know about further than our customer base. It is in those

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing: *Private Sector and Government Challenges and Opportunities to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure***  
**Questions for the Record Submitted to Mr. Robert M. Lee**

instances we forgo revenue and try to inform the community; we do that through the E-ISAC. They have the channels in place to inform the community of immediate insights needed as a trusted voice. In addition, we are currently exploring with the E-ISAC an opportunity to put our technology into smaller electric, water, and gas utilities at a near loss but for the purpose of providing technology and intelligence to those smaller players. This would also allow us to glean insights into the threats those utilities face while not compromising their privacy. This fully anonymous network would help us understand the threat landscape, promote real information sharing from industrial networks, and provide security for these utilities all led from the private sector. We do not need E-ISAC approval for this but have determined them to be the right trusted voice to promote this to the smaller utilities.

**Questions from Senator Catherine Cortez Masto**

**Question 1:** As a firm that specializes in industrial cyber security, how are the threats to our water and power infrastructure assets evolving over time?

**Answer:** The threats to our water and power infrastructure are becoming more numerous, sophisticated, and aggressive. It is our assessment that the attack on the power grid in Ukraine in 2015 set off a sort of arms race where numerous nation-states are leveraging teams to specifically target industrial networks in a way they have not before. It is in our assessment this is in a desire to have a equatable capability to the ones effectively being advertised globally such as the Ukraine attack. The second Ukraine attack in 2016 on their power grid and the attack on the petrochemical facility in Saudi Arabia in 2017 have quickened the efforts of these states.

**Question 2:** In your view, do the relevant government agencies have the resources required to meet the threat today and in the future?

**Answer:** No. There is still confusion on roles and responsibilities as well as coordination between adjacent teams within government agencies. Additionally, the resources are not simply one of funding but of talent acquisition. Without attempting to be arrogant the quality of my team at Dragos in terms of industrial threat detection and response far outweighs anything I ever had access to at the National Security Agency. Only a true public-private partnership will ensure success in this space. Additionally, we are concerned by seeing some government teams including National Guard teams seek to provide free services to industrial asset owners and operators outside of state owned infrastructure. These competitive actions are not only concerning because it equates to tax payer teams competing with tax paid teams, but more importantly the innovation and insights the US Government is largely depending on in this space is coming from the private sector and this type of competition will destroy that ecosystem. Sector specific agencies, such as the DOE to the power grid, should have the lead on engaging the sector and all other agencies, such as the DHS and DOD, should serve a supporting role to those sector specific agencies. The resources allocated should also highly encourage finding, promoting, and leveraging innovation that already exists in the private sector.

**U.S. Senate Committee on Energy and Natural Resources**  
**March 1, 2018 Hearing:** *Private Sector and Government Challenges and Opportunities  
to Promote the Cyber Security and Resiliency of our Nation's Critical Energy Infrastructure*  
**Questions for the Record Submitted to Mr. Robert M. Lee**

**Question 3:** As more devices are being integrated into online networks, what are some of the threats you see that aren't getting enough attention?

**Answer:** Adoption of monitoring and response technology into industrial networks is almost non-existent. Outside of the top % of leaders in the industry there just seems not to be the budget and procurement channels in place today to quickly move to get security into industrial networks for monitoring (threat detection) and response. As the networks get more interconnected devices such as industrial internet of things (IIoT) technologies and smart meters this lack of visibility and response capability will amplify the risks.

**Question 4:** What practices can considerably reduce customers' risk profiles, making them less of a target for cyber-crime and attack?

**Answer:** Organizations and their defenders get to choose almost everything about the battlefield they are walking onto. The infrastructure, the design, the defenses, etc. They call the shots for the world the adversaries have to play in. The only thing they do not get to do is determine whether or not they are a good target. The mindset needs to shift from one of avoiding targeting to one of being able to detect and respond to targeting effectively and efficiently. Prevention is nice but response is key. This can be done through the proper allocation of resources to these efforts and encouragement of these practices by the federal government.

○