

**PROTECTING CRITICAL INFRASTRUCTURE FROM
CYBER ATTACKS: EXAMINING EXPERTISE OF
SECTOR-SPECIFIC AGENCIES**

HEARING
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND
INVESTIGATIONS
OF THE
COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS
FIRST SESSION

MAY 16, 2023

Serial No. 118–37



Published for the use of the Committee on Energy and Commerce
govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

56–055 PDF

WASHINGTON : 2025

COMMITTEE ON ENERGY AND COMMERCE

CATHY McMORRIS RODGERS, Washington

Chair

MICHAEL C. BURGESS, Texas	FRANK PALLONE, JR., New Jersey
ROBERT E. LATTA, Ohio	<i>Ranking Member</i>
BRETT GUTHRIE, Kentucky	ANNA G. ESHOO, California
H. MORGAN GRIFFITH, Virginia	DIANA DeGETTE, Colorado
GUS M. BILIRAKIS, Florida	JAN SCHAKOWSKY, Illinois
BILL JOHNSON, Ohio	DORIS O. MATSUI, California
LARRY BUCSHON, Indiana	KATHY CASTOR, Florida
RICHARD HUDSON, North Carolina	JOHN P. SARBANES, Maryland
TIM WALBERG, Michigan	PAUL TONKO, New York
EARL L. "BUDDY" CARTER, Georgia	YVETTE D. CLARKE, New York
JEFF DUNCAN, South Carolina	TONY CARDENAS, California
GARY J. PALMER, Alabama	RAUL RUIZ, California
NEAL P. DUNN, Florida	SCOTT H. PETERS, California
JOHN R. CURTIS, Utah	DEBBIE DINGELL, Michigan
DEBBIE LESKO, Arizona	MARC A. VEASEY, Texas
GREG PENCE, Indiana	ANN M. KUSTER, New Hampshire
DAN CRENSHAW, Texas	ROBIN L. KELLY, Illinois
JOHN JOYCE, Pennsylvania	NANETTE DIAZ BARRAGAN, California
KELLY ARMSTRONG, North Dakota, <i>Vice</i>	LISA BLUNT ROCHESTER, Delaware
<i>Chair</i>	DARREN SOTO, Florida
RANDY K. WEBER, SR., TEXAS	ANGIE CRAIG, Minnesota
RICK W. ALLEN, Georgia	KIM SCHRIER, Washington
TROY BALDERSON, Ohio	LORI TRAHAN, Massachusetts
RUSS FULCHER, Idaho	LIZZIE FLETCHER, Texas
AUGUST PFLUGER, Texas	
DIANA HARSHBARGER, Tennessee	
MARIANNETTE MILLER-MEEKS, Iowa	
KAT CAMMACK, Florida	
JAY OBERNOLTE, California	

PROFESSIONAL STAFF

NATE HODSON, *Staff Director*
SARAH BURKE, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

H. MORGAN GRIFFITH, Virginia
Chairman

MICHAEL C. BURGESS, Texas	KATHY CASTOR, Florida
BRETT GUTHRIE, Kentucky	<i>Ranking Member</i>
JEFF DUNCAN, South Carolina	DIANA DEGETTE, Colorado
GARY J. PALMER, Alabama	JAN SCHAKOWSKY, Illinois
DEBBIE LESKO, Arizona, <i>Vice Chair</i>	PAUL TONKO, New York
DAN CRENSHAW, Texas	RAUL RUIZ, California
KELLY ARMSTRONG, North Dakota	SCOTT H. PETERS, California
KAT CAMMACK, Florida	FRANK PALLONE, JR., New Jersey (<i>ex</i>
CATHY McMORRIS RODGERS, Washington	<i>officio</i>)
<i>(ex officio)</i>	

C O N T E N T S

	Page
Hon. H. Morgan Griffith, a Representative in Congress from the Commonwealth of Virginia, opening statement	1
Prepared statement	4
Hon. Kathy Castor, a Representative in Congress from the State of Florida, opening statement	10
Prepared statement	12
Hon. Cathy McMorris Rodgers, a Representative in Congress from the State of Washington, opening statement	14
Prepared statement	16
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	19
Prepared statement	21
WITNESSES	
Puesh Kumar, Director, Office of Cybersecurity, Energy Security, and Emergency Response, Department of Energy	23
Prepared statement	26
Answers to submitted questions	102
Brian Mazanec, Ph.D., Deputy Director, Office of Preparedness, Administration for Strategic Preparedness and Response, Department of Health and Human Services	32
Prepared statement	34
Answers to submitted questions	106
David Travers, Ph.D., Director, Water Infrastructure and Cyber Resilience Division, Environmental Protection Agency	40
Prepared statement	42
SUBMITTED MATERIAL	
<i>Inclusion of the following was approved by unanimous consent.</i>	
List of documents submitted for the record	78
Letter of April 24, 2023, from the American Water Works Association and the United States Conference of Mayors to Michael Regan, Administrator, Environmental Protection Agency, and Richard Revesz, Administrator, Office of Information and Regulatory Affairs	79
Letter of March 17, 2023, from American Water Works Association, et al., to Michael Regan, Administrator, Environmental Protection Agency, and Richard Revesz, Administrator, Office of Information and Regulatory Affairs	83
Letter of January 25, 2023, from American Water Works Association, et al., to Michael Regan, Administrator, Environmental Protection Agency	87
Letter of December 9, 2021, from G. Tracy Mehan III, Executive Director, Government Affairs, American Water Works Association, et al., to Radhika Fox, Assistant Administrator for Water, Environmental Protection Agency ..	95
Letter of May 16, 2023, from Desmarie Waterhouse, Senior Vice President of Advocacy and Communications and General Counsel, American Public Power Association, to Mr. Griffith and Ms. Castor	97

PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER ATTACKS: EXAMINING EXPER- TISE OF SECTOR-SPECIFIC AGENCIES

TUESDAY, MAY 16, 2023

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 2:23 p.m., in the John D. Dingell Room 2123 Rayburn House Office Building, Hon. Morgan Griffith (chairman of the subcommittee) presiding.

Members present: Representatives Griffith, Guthrie, Duncan, Palmer, Lesko, Crenshaw, Cammack, Rodgers (ex officio), Castor (subcommittee ranking member), DeGette, Schakowsky, Tonko, Ruiz, Peters, and Pallone (ex officio).

Also present: Representative Kelly.

Staff present: Sean Brebbia, Chief Counsel, Oversight and Investigations; Sarah Burke, Deputy Staff Director; Jerry Couri, Deputy Chief Counsel for Environment; Lauren Eriksen, Clerk, Oversight and Investigations; Christen Harsha, Senior Counsel, Oversight and Investigations; Tara Hupman, Chief Counsel; Peter Kielty, General Counsel; Emily King, Member Services Director; Chris Krepich, Press Secretary; John Strom, Counsel, Oversight and Investigations; Joanne Thomas, Counsel, Oversight and Investigations; Austin Flack, Minority Junior Professional Staff Member; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Liz Johns, Minority GAO Detailee; Will McAuliffe, Minority Chief Counsel, Oversight and Investigations; Elysa Montfort, Minority Press Secretary; Christina Parisi, Minority Professional Staff Member; Greg Pugh, Minority Staff Assistant; Harry Samuels, Minority Oversight Counsel; and Caroline Wood, Minority Research Analyst.

Mr. GRIFFITH. All right, I'll ask all of our guests and people in the audience to please take their seats. The Subcommittee on Oversight and Investigations will now come to order.

The Chair recognizes himself for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. H. MORGAN GRIFFITH, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

Thank you all for appearing before us at today's hearing of the Energy and Commerce Committee, Subcommittee on Oversight and

Investigations. Defending our Nation's critical infrastructure from cyber attacks is an increasingly difficult endeavor for Federal regulators and cybersecurity experts. Over the past few years, escalating geopolitical tensions, an uptick in ransomware use, and increased criminal and foreign cyber attack capacity have raised Congress' concerns.

The increased interconnectedness of critical infrastructure, such as hospitals, pipelines, and wastewater plants has furthered the proliferation of operational technology monitored by and connected to online computer systems, which has also heightened risks. Malicious actors are demonstrating an increased willingness and a growing capacity to execute cyber attacks.

For example, the Director of National Intelligence reported that China is almost certainly capable of launching cyber attacks that could disrupt critical services in the United States and would almost certainly consider doing so if it feared that a major conflict with our Nation was imminent. Russia also remains a top cyber threat and seeks to improve its capabilities to target critical infrastructure. Also, hacking tools are now widely available to criminal organizations seeking to attack businesses, large and small.

Critical infrastructure is a broad term that refers to physical or virtual systems and assets vital to the United States. Their destruction would debilitate the national economy, public health, and/or security. Often-used examples include our highways, utilities, dams, food manufacturing facilities, and emergency medical services.

According to the Federal Bureau of Investigations 2022 Internet Crime Report, of the 2,385 reported ransomware attacks, 870 affected critical infrastructure organizations. Healthcare and public health infrastructure were the most common types of critical infrastructure attacked. Presidential Policy Directive 21 has previously suggested a national framework on monitoring critical infrastructure.

Under the Fiscal Year 2022 National Defense Authorization Act, there are currently 16 defined critical infrastructure sectors. Each sector is assigned a so-called Sector Risk Management Agency. Importantly, Presidential Policy Directive 21 noted that each critical infrastructure sector possesses unique characteristics and risks, and therefore benefits from the specialized knowledge of Federal agencies most familiar with regulating that sector.

That brings up the witnesses. Joining us today we have the Department of Energy, which carries out the Sector Risk Management Agency duties for the energy sector composed of electricity, oil, and natural gas segments, including their production, refining, storage, and distribution facilities. Nearly every industry depends on electricity and fuel. In fact, Presidential Policy Directive 21 identified the energy sector as uniquely critical due to its enabling function for all other critical infrastructure sectors.

Subcommittee welcomes Mr. Puesh Kumar. Did I get close?

Mr. KUMAR. That's pretty good.

Mr. GRIFFITH. All right. Director of the Department of Office of Cybersecurity, Energy Security, and Emergency Response.

Additionally, we are pleased to have Dr. David Travers from the Environmental Protection Agency's Office of Water. The EPA

serves as the Sector Risk Management Agency for water and wastewater—sector—the sector on water and wastewater. Safe drinking water is essential human health and our Nation’s economy. But water systems face increasing threats from malicious actors.

Last but not least, the subcommittee welcomes Dr. Brian Mazanec from the Department of Health and Human Services Administration for Strategic Preparedness and Response that performs the Sector Risk Management Agency role for the healthcare and public sector—for the—for healthcare in the public sector—public health sector. This sector encompasses a diverse array of both publicly and privately owned entities such as the healthcare facilities, research centers, and medical materials supply chains.

Today we hope to learn more about the emerging cybersecurity challenges that specifically threaten each of these sectors and what actions these agencies are taking to prepare for ever-evolving cyber threats. Also, much of our Nation’s critical infrastructure network includes many non-Federal entities like municipalities and private enterprises.

We hope to learn more about how agencies partner with other system operators to share information and coordinate efforts across their sectors. We will also examine some of the recent cybersecurity activities at these agencies to identify any legislative opportunities for them to improve their efforts or serve as more effective partners with stakeholders and with those of us in Congress.

I thank our witnesses for being here today.

[The prepared statement of Mr. Griffith follows:]

**Energy and Commerce Committee
Subcommittee on Oversight and Investigations
Hearing, “Protecting Critical Infrastructure from
Cyberattacks: Examining Expertise of Sector Specific
Agencies”
May 16, 2023**

Good afternoon, and welcome to today’s hearing of the Energy and Commerce Committee’s Subcommittee on Oversight and Investigations.

Defending our nation’s critical infrastructure from cyberattacks is an increasingly difficult endeavor for our federal government due to many factors, including escalating geopolitical tensions and the growing interconnectivity of critical infrastructure systems. Malicious actors are demonstrating an increasing willingness and growing capabilities to execute cyberattacks. For example, the Director of National Intelligence reported that China is

almost certainly capable of launching cyberattacks that could disrupt critical infrastructure services in the United States and would almost certainly consider doing so if it feared that a major conflict with our nation was imminent. Russia will also remain a top cyber threat and seeks to improve its capabilities to target critical infrastructure. Hacking tools and services are now widely available to criminal organizations seeking to disrupt crucial activities and strike businesses.

The term “critical infrastructure” refers to “systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” This includes our highways, utilities, dams, food manufacturing facilities, and emergency

medical services. Under Presidential Policy Directive-21, which established a national policy on critical infrastructure in 2013, there are currently sixteen critical infrastructure sectors, with a Sector Risk Management Agency assigned to each sector. Importantly, Presidential Policy Directive 21 noted that each critical infrastructure sector possesses unique characteristics and risks, and therefore benefits from the specialized knowledge of the federal agencies most familiar with that sector. Witnesses representing three of our Sector Risk Management Agencies have joined us today.

The Department of Energy carries out the Sector Risk Management Agency duties for the Energy Sector, composed of the electricity, oil, and, natural gas segments, including their production, refining, storage, and distribution facilities. Nearly every industry depends on access to electricity or

fuel. In fact, Presidential Policy Directive 21 identified the energy sector as uniquely critical due to its enabling function for all other critical infrastructure sectors. The Subcommittee welcomes Mr. Puesch Kumar, Director of the Department's Office of Cybersecurity, Energy Security, and Emergency Response.

Additionally, we are pleased to have Mr. David Travers from the Environmental Protection Agency's (EPA) Office of Water. The EPA serves as the Sector Risk Management Agency for the Water and Wastewater Sector. Safe drinking water is essential to human health and our nation's economy, but water systems face increasing threats from malicious actors.

Last, but not least, the Department of Health and Human Services performs the Sector Risk Management Agency role

for the Healthcare and Public Health Sector. This sector encompasses a diverse array of both publicly and privately owned entities, such as healthcare facilities, research centers, and the medical materials supply chain. The Subcommittee welcomes Dr. Brian Mazanec from the Department's Administration for Strategic Preparedness and Response.

Today, we hope to learn more about the emerging cybersecurity challenges that threaten each of these sectors and what actions these agencies are taking to prepare for ever-evolving cyber threats. As our nation's critical infrastructure network includes many non-Federal entities, including private sector critical infrastructure owners and operators, we hope to learn more about how these agencies partner with these allies to share information and coordinate efforts across the sector. We will also examine some of the

Page 6 of 6

recent cybersecurity activities at these agencies to identify any opportunities for them to improve their efforts or serve as more effective partners for stakeholders in each sector.

I hope this hearing will inform the Committee's efforts to monitor our Sector Risk Management Agencies' efforts to shield our critical infrastructure from increasingly sophisticated cyber threats and to ensure our federal cybersecurity enterprise effectively harnesses the valuable expertise of these agencies.

I thank our witnesses for being here today and sharing their experience with us.

Mr. GRIFFITH. I now yield back my time and recognize the ranking member of the subcommittee, Ms. Castor, for her 5-minute opening statement.

OPENING STATEMENT OF HON. KATHY CASTOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Ms. CASTOR. Well, thank you, Mr. Chairman, and good afternoon. I'm glad we're having this important hearing to get a better understanding from the agency experts as to the threats to critical infrastructure and how they are addressing those threats and how we can support their efforts.

Everyday folks in my district and across the country count on being able to turn on the lights, have easy access to clean water, and ensure that they can receive confidential and life-sustaining medical treatment. Yet the critical infrastructure that makes these things possible is increasingly under threat from criminals and foreign adversaries who carry out cyber attacks to steal people's personal information and disrupt our way of life.

So we must prepare and protect critical infrastructure now from more common and sophisticated cyber attacks. They target not only the agencies here before us today but also the utilities companies and healthcare providers throughout the sectors that they oversee. Every hospital and utility is a target for bad actors seeking to profit from sensitive information or undermine our national security.

Criminal networks have targeted hospitals and public health agencies in ransomware attacks because they know that these organizations store our neighbors' most personal information. So I want to do all that I can to protect my neighbors and the hospitals and health systems that serve them.

Foreign adversaries like Russia have used cyber attacks to steal information from hundreds of Federal agencies in critical infrastructure organizations. Just last year at the start of Putin's unprovoked invasion of Ukraine, Russian hackers tried to take control of energy facilities in the United States, and while those hackers were ultimately thwarted by the Department of Energy and its Federal and sector partners, it demonstrates the seriousness of cyber threats and the risks that they pose.

Many critical infrastructure organizations can take steps to prepare for and prevent cyber attacks. In doing so, the impact of an attack can be mitigated, but it takes an understanding of sector-specific cybersecurity threats to ensure that the finite resources that we have are spent on the most effective measures. That's why the work that the Department of Energy, the Environmental Protection Agency, and the Department of Health and Human Services, the work that they do to develop cybersecurity best practices and educate their sector partners, is so important.

The agencies have the expertise necessary to identify sector- and sometimes facility-specific cyber threats and can use their existing regulatory authorities to make sure that countermeasures reach the organizations that need them the most. And as we tackle the rising cost and risks of the climate crisis, cybersecurity will only become more important. Clean energy resources will help us reduce climate pollution while new technologies that replace legacy systems can help existing power sources operate more efficiently.

But new technologies can also give hackers new angles to attack our energy security, so we need to make sure that the energy and other critical infrastructure resources are well protected so that at the same time we can benefit from technological innovation. Agencies are already taking steps to address foreseeable cyber threats, and Congress can and should continue to support their efforts in a bipartisan manner. By listening and learning from our experts, Congress can make sure agencies have the tools they need to keep our neighbors safe, counter cyber threats, and protect critical infrastructure.

So I look forward to hearing from our witnesses today about their important cybersecurity work and see how Congress can be helpful in supporting the most effective cybersecurity tools.

[The prepared statement of Ms. Castor follows:]

Committee on Energy and Commerce

**Opening Statement as Prepared for Delivery
of**

Subcommittee on Oversight and Investigations Ranking Member Kathy Castor

***Hearing on "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of
Sector Specific Agencies"***

May 16, 2023

Thank you, Mr. Chairman. I'm glad we're having this important hearing to get a better understanding from the agency experts as to the threats to critical infrastructure, how they are addressing those threats, and how we can support their efforts.

Every day, folks in my district and across the country count on being able to turn on their lights, have easy access to clean water, and ensure that they can receive confidential and life-sustaining medical treatment. Yet, the critical infrastructure that makes these things possible is increasingly under threat from criminals and foreign adversaries who carry out cyber attacks to steal people's personal information and disrupt our way of life.

So we must prepare, and protect critical infrastructure now from more common and sophisticated cyber attacks. They target not only the agencies that are here today but also the utilities, companies, and healthcare providers throughout the sectors they oversee. Every hospital and utility is a target for bad actors seeking to profit from sensitive information or undermine our national security.

Criminal networks have targeted hospitals and public health agencies in ransomware attacks because they know that these organizations store our neighbors' most personal information. I want to do all I can to protect my neighbors and the hospitals and health systems that serve them.

Foreign adversaries like Russia have used cyber attacks to steal information from hundreds of federal agencies and critical infrastructure organizations. Just last year at the start of Putin's invasion of Ukraine, Russian hackers tried to take control of energy facilities in the United States. While those hackers were ultimately thwarted by the Department of Energy and its federal and sector partners, it demonstrates the seriousness of cyber threats and the risks that they pose.

Many critical infrastructure organizations can take steps to prepare for and prevent cyber attacks. In doing so, the impact of an attack can be mitigated, but it takes an understanding of sector-specific cybersecurity threats to ensure that finite resources are spent on the most effective measures.

That is why the work that the Department of Energy, Environmental Protection Agency, and Department of Health and Human Services do to develop cybersecurity best practices and

May 16, 2023

Page 2

educate their sector partners is so important. These agencies have the expertise necessary to identify sector- and sometimes facility-specific cyber threats and can use their existing regulatory relationships to make sure that countermeasures reach the organizations that need them the most.

As we tackle the rising costs and risks of the climate crisis, cybersecurity will only become more important. Clean energy resources will help us reduce climate pollution, while new technologies that replace legacy systems can help existing power plants operate more efficiently, but new technologies can also give hackers angles to attack our energy infrastructure.

We need to make sure that energy and other critical infrastructure are well protected so that we can benefit from technological innovation.

Agencies already are taking steps to address foreseeable cyber threats and Congress can and should continue to support their efforts in a bipartisan manner. By listening and learning from our experts, Congress can make sure agencies have the tools that they need to keep our neighbors safe, counter cyber threats and protect critical infrastructure.

I look forward to hearing from our witnesses about their important cybersecurity work they do and see how Congress can be helpful in supporting the most effective cybersecurity tools.

Thank you, I yield back.

Ms. CASTOR. Thank you, and I yield back.

Mr. GRIFFITH. Thank you, gentlelady, for yielding back. I now recognize the gentlelady who is The Chair of the full committee, Ms. McMorris Rodgers, for her 5 minutes.

**OPENING STATEMENT OF HON. CATHY McMORRIS RODGERS,
A REPRESENTATIVE IN CONGRESS FROM THE STATE OF
WASHINGTON**

Mrs. RODGERS. Thank you, Chair Griffith. Today we are here to learn more about cyber attacks that threaten essential services and products that we as a Nation need to survive, attacks that could deprive us of access to emergency services, food and water, and the ability to communicate with one another. As Chair Griffith described, our critical infrastructure is essential to the security of our Nation, our economic prosperity, and our way of life.

We depend on critical infrastructure to power our homes, ensure that we get to work, call for help in an emergency, supply us with clean water, and produce our food. With technological advances, this network has become increasingly more complex and interconnected. However, as our physical infrastructure and digital systems become more intertwined, new opportunities bring them new challenges. Bad actors, whether criminal organizations or foreign adversaries, have demonstrated a growing interest in launching cyber attacks on critical infrastructure, and unfortunately, many have demonstrated that they have the capability to do so.

For example, the number of yearly cyber attacks on United States hospitals reportedly doubled between 2016 and 2021. Hospitals have increasingly become targets for ransomware gangs which assume control of online networks and then demand a ransom to unlock them. This means care and treatments are delayed when lives are on the line.

Additionally, in 2021 a hacker altered the chemical levels in the water supply at a water treatment facility in Florida. Last June, another report concluded that 89 percent of electricity, oil and gas, and manufacturing firms experienced cyber attacks affecting population and energy supply over the previous 12 months.

Securing our critical infrastructure from cyber threats and responding quickly to minimize and contain interruptions to these services will require the unique skills and resources of nearly all of our Federal agencies. Each of our Sector Risk Management Agencies possess specialized knowledge and expertise to help them identify new and evolving cyber threats in each of the infrastructure sectors. Through their experiences, regulating and communicating with critical infrastructure owners and operators, these agencies have gained extensive knowledge of the utilities, industries, and facilities that comprise each sector.

For example, the Department of Health and Human Services is uniquely well positioned to respond to emerging threats to our hospital system online record systems because HHS is the agency already in direct communications with the healthcare sector. Similarly, we plan to explore whether our Sector Risk Management Agencies effectively partner with private entities, utilities, and non-Federal Government entities that make up the critical infrastructure network.

Many of these entities, especially small businesses, local governments, or small utilities, may not have the resources to address the constantly shifting cyber attacks that they face and can benefit greatly from the resources and technical assistance our Sector Risk Management Agencies can provide. Our Federal agencies are also well positioned to provide leadership, coordinate efforts, and information sharing among members in each critical infrastructure sector.

Much of our critical infrastructure is owned or operated by the private sector, so we hope to learn more from our management agencies the strategies for forging partnerships across relevant industries. We hope to learn more about how these agencies listen to non-Federal partners and receive their feedback to ensure Federal cybersecurity programs appropriately serve those they seek to protect.

In the same vein, in carrying out their cybersecurity responsibilities, Federal agencies should incorporate their expertise they gather from their regulated entities and other non-Federal partners to inform their efforts. As we've discussed, many of our critical infrastructure sectors are heavily intertwined and rely on each other to function properly. As such, we hope to learn more about our Sector Risk Management Agencies' efforts to coordinate with each other and share expertise, lessons learned, and best practices.

Cyber threats to our critical infrastructure present a serious threat to our national security. We can be prepared for these threats if we effectively harness the expertise and creativity of our Federal agencies, non-Federal governments, utilities, and industry.

Again, I thank our witnesses for sharing their perspectives today, and I look forward to this discussion.

[The prepared statement of Mrs. Rodgers follows:]

**Opening Statement for Chair Cathy McMorris Rodgers
Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
“Protecting Critical Infrastructure from Cyberattacks: Examining
Expertise of Sector Specific Agencies”
May 16, 2023**

Thank you, Chair Griffith

EMERGING THREATS AND GROWING VULNERABILITIES

Today, we are here to learn more about cyberattacks that threaten the essential services and products that we, as a nation, need to survive.

Attacks that could deprive us of access to emergency services; food and water; and the ability to communicate with one another.

As Chair Griffith described, our critical infrastructure is essential to the security of our nation, our economic prosperity, and our way of life.

We depend on critical infrastructure to power our homes, ensure we can get to work, call for help in an emergency, supply us with clean water, and produce our food.

With technological advances, this network has become increasingly more complex and interconnected. However, as our physical infrastructure and digital systems become more intricately intertwined, new opportunities bring with them new challenges.

Bad actors, whether criminal organizations or foreign adversaries, have demonstrated a growing interest in launching cyberattacks on critical infrastructure. And unfortunately, many have demonstrated that they have the capability to do so.

For example, the number of yearly cyberattacks on United States hospitals reportedly doubled between 2016 and 2021.

Hospitals have increasingly become targets for ransomware gangs, which assume control of online networks and then demand a ransom to unlock them.

This means care and treatments are delayed when lives are on the line.

Additionally, in 2021, a hacker altered the chemical levels in the water supply at a water treatment facility in Florida.

Last June, another report concluded that 89% of electricity, oil & gas, and manufacturing firms experienced cyberattacks affecting production and energy supply over the previous twelve months.

SECTOR RISK MANAGEMENT AGENCY EXPERTISE

Securing our critical infrastructure from cyber threats and responding quickly to minimize and contain interruptions to these services will require the unique skills and resources of nearly all of our federal agencies.

Each of our Sector Risk Management Agencies possess specialized knowledge and expertise to help them identify new and evolving cyber threats to its particular infrastructure sector.

Through their experiences regulating and communicating with critical infrastructure owners and operators, these agencies have gained extensive knowledge of the utilities, industries, and facilities that comprise each sector.

For example, the Department of Health and Human Services is uniquely well-positioned to respond to emerging threats to our hospital systems' online record systems because HHS is the agency already in direct communications with the health care sector.

CROSS-SECTOR PARTNERSHIPS

Similarly, we plan to explore whether our Sector Risk Management Agencies effectively partner with the private entities, utilities, and non-federal government entities that make up the critical infrastructure network.

Many of these entities, particularly small businesses, local governments, or small utilities may not have the resources to address the constantly shifting cyberthreats they face and can benefit greatly from the resources and technical assistance our Sector Risk Management Agencies can provide.

Our federal agencies are also well positioned to provide leadership, coordinate efforts, and information sharing among members of each critical infrastructure sector.

Much of our critical infrastructure is owned or operated by the private sector, so we hope to learn more about our Sector Risk Management Agencies' strategies for forging partnerships across relevant industries.

We hope to learn more about how these agencies listen to their non-Federal partners and receive their feedback to ensure federal cybersecurity programs appropriately serve those they seek to protect.

In the same vein, in carrying out their cybersecurity responsibilities, federal agencies should incorporate the expertise they gather from their regulated entities and other non-Federal partners to inform their efforts.

As we have discussed, many of our critical infrastructure sectors are heavily intertwined and rely on each other to function properly.

As such, we hope to learn more about our Sector Risk Management Agencies' efforts to coordinate with each other and share expertise, lessons learned, and best practices.

CONCLUSION

Cyber threats to our critical infrastructure present a serious risk to our national security.

We can be prepared for these threats if we effectively harness the expertise and creativity of our federal agencies, non-federal governments, utilities, and industry.

Again, I thank our witnesses for sharing their perspectives today, and I look forward to the discussion.

Mrs. RODGERS. I yield back.

Mr. GRIFFITH. The gentlelady yields back. I now recognize the gentleman from New Jersey, the ranking member of the full committee, Mr. Pallone, for his 5-minute opening statement.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman. Today the subcommittee continues its important bipartisan oversight of cybersecurity and protecting our Nation's critical infrastructure from cyber attacks. Federal agencies within our committee's jurisdiction and their partners in the private sector face serious cybersecurity threats to critical energy, water, and health systems. Major cyber incidents have repeatedly shown how harmful attacks on critical infrastructure can be to our Nation.

We all remember the ransomware attack on the Colonial Gas Pipeline. The attack triggered panic buying that contributed to fuel shortages and higher gas prices across the East Coast and the South. At the end of last year, cyber criminals stole the electronic patient records of more than 3 million patients from a California hospital system. That breach exposed sensitive personal information, including patients' Social Security numbers, test results and diagnoses, and prescription history. And then earlier this year, the personal healthcare information of Members and staff was stolen when DC Health Link was breached.

Cyber threats to critical energy, water, and health infrastructure are unfortunately becoming more common, and attacks are more costly. In 2022, hundreds of cyber attacks cost healthcare organizations billions of dollars and made it harder for doctors and other healthcare providers from caring for patients for months afterwards. Companies that own critical infrastructure face thousands of cyber attacks every year.

While many of these attacks are unsuccessful thanks to the cyber defenses these companies have established, successful cyber attacks can have devastating consequences. During the early days of Russia's invasion of Ukraine, Russian hackers unsuccessfully targeted America's energy grid. Experts have said that this incident is the closest we have come to losing control of grid infrastructure and that the methods used represent an unprecedented threat.

That's why bipartisan efforts in this committee are so important to bolster cybersecurity for critical infrastructure overseen by the Department of Energy, the Environmental Protection Agency, and the Department of Health and Human Services. We worked together on the bipartisan America's Water Infrastructure Act of 2018, and this law requires water systems to complete risk assessments and develop emergency response plans that account for cybersecurity risks.

But despite these efforts, there are still gaps in the ability of Federal agencies to prevent potential cyber attacks. In 2020, Russian hackers gained access to an updated—an update server at SolarWinds, a software company serving critical infrastructure companies and Federal agencies. For months the attackers were able to use SolarWinds systems to penetrate networks at hundreds

of organizations and dozens of Federal agencies. And while the method of attack was not necessarily new, the scale and scope was unprecedented. It exposed vulnerabilities and cybersecurity gaps that put critical infrastructure at risk.

I strongly believe that DOE, EPA, and HHS are best equipped to handle internal and sector-relevant cybersecurity concerns. Much of our critical infrastructure relies on unique systems and specialized workforces. These agencies have the institutional knowledge and expertise to engage with their private-sector partners to address complex sector-specific threats. We must focus on giving these agencies the resources they need to fight constantly evolving threats.

But the Republicans' Default of America Act threatens indiscriminate cuts to Federal agencies overseeing infrastructure. I'm concerned that it could seriously hamstring cybersecurity efforts at a time when we must be ramping up our defenses against cyber threats from criminal and foreign adversaries. And Federal agencies need tools that enable them to leverage sector-specific expertise and institutional knowledge to prevent and respond to cybersecurity concerns.

With bipartisan congressional support, DOE, EPA, HHS, and other Federal agencies can continue to develop more efficient and robust cybersecurity defenses while also partnering with the private sector to protect our critical infrastructure systems. So I hope to continue this committee's important bipartisan work on this topic.

Well, I look forward to hearing from our witnesses on the progress they've made and the challenges that they continue to face.

[The prepared statement of Mr. Pallone follows:]

Committee on Energy and Commerce**Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.*****Hearing on "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of
Sector Specific Agencies"*****May 16, 2023**

Today, the Subcommittee continues its important bipartisan oversight of cybersecurity and protecting our nation's critical infrastructure from cyberattacks. Federal agencies within our Committee's jurisdiction and their partners in the private sector face serious cybersecurity threats to critical energy, water, and health systems. Major cyber incidents have repeatedly shown how harmful attacks on critical infrastructure can be to our nation.

We all remember the ransomware attack on the Colonial gas pipeline. The attack triggered panic buying that contributed to fuel shortages and higher gas prices across the East Coast and the South. At the end of last year, cyber criminals stole the electronic patient records of more than three million patients from a California hospital system. That breach exposed sensitive personal information, including patients' Social Security Numbers, test results and diagnoses, and prescription history. And then earlier this year, the personal health care information of Members and staff was stolen when DC Health Link was breached.

Cyber threats to critical energy, water, and health infrastructure are unfortunately becoming more common and attacks are more costly. In 2022, hundreds of cyberattacks cost health care organizations billions of dollars and made it harder for doctors and other health care providers from caring for patients for months afterwards.

Companies that own critical infrastructure face thousands of cyberattacks every year. While many of these attacks are unsuccessful thanks to the cyber defenses these companies have established, successful cyberattacks can have devastating consequences. During the early days of Russia's invasion of Ukraine, Russian hackers unsuccessfully targeted America's energy grid. Experts have said that this incident is the closest we have come to losing control of grid infrastructure and that the methods used represent an unprecedented threat.

That is why bipartisan efforts in this Committee are so important to bolster cybersecurity for critical infrastructure overseen by the Department of Energy (DOE), the Environmental Protection Agency (EPA), and the Department of Health and Human Services (HHS). We worked together on the bipartisan America's Water Infrastructure Act of 2018. This law requires water systems to complete risk assessments and develop emergency response plans that account for cybersecurity risks.

Despite these efforts, there are still gaps in the ability of federal agencies to prevent potential cyberattacks. In 2020, Russian hackers gained access to an update server at

May 16, 2023
Page 2

SolarWinds, a software company serving critical infrastructure companies and federal agencies. For months, the attackers were able to use SolarWinds' systems to penetrate networks at hundreds of organizations and dozens of federal agencies. While the method of attack was not necessarily new, the scale and scope was unprecedented. It exposed vulnerabilities and cybersecurity gaps that put critical infrastructure at risk.

I strongly believe that DOE, EPA, and HHS are best equipped to handle internal and sector-relevant cybersecurity concerns. Much of our critical infrastructure relies on unique systems and specialized workforces. These agencies have the institutional knowledge and expertise to engage with their private-sector partners to address complex, sector-specific threats.

We must focus on giving these agencies the resources they need to fight constantly evolving threats. But the Republicans' Default on America Act threatens indiscriminate cuts to federal agencies overseeing infrastructure. I am concerned that it could seriously hamstring cybersecurity efforts at a time when we must be ramping up our defenses against cyber threats from criminals and foreign adversaries.

Federal agencies need tools that enable them to leverage sector-specific expertise and institutional knowledge to prevent and respond to cybersecurity concerns. With bipartisan congressional support, DOE, EPA, HHS, and other federal agencies can continue to develop more efficient and robust cybersecurity defenses while also partnering with the private sector to protect our critical infrastructure systems.

I hope to continue the Committee's important bipartisan work on this topic, and I look forward to hearing from our witnesses on the progress they've made and the challenges that remain.

Thank you, I yield back.

Mr. PALLONE. With that, Mr. Chairman, thank you, and I yield back.

Mr. GRIFFITH. Thank the gentleman for yielding back. That concludes Members' opening statements. I would like to remind all Members that their opening statements can be made a part of the record pursuant to committee rules.

All right, we want to thank all of our witnesses for being here today and taking your time to testify before this subcommittee. Each witness will have the opportunity to give an opening statement of 5 minutes followed by a round of questions from Members. Our witnesses today are Puesh Kumar, Director of Office of Cybersecurity, Energy Security, and Emergency Response, Department of Energy; Dr. Brian Mazanec, Deputy Director, Office of Preparedness, Department of Health and Human Services; David Travers, Director of Water Infrastructure and Cyber Resilience Division, Environmental Protection Agency. We appreciate all of you being here today, and I look forward to hearing from you on this important issue.

As you are aware, this committee is holding an oversight hearing, and when doing so, we have the practice of taking testimony under oath. Do any of you have any objection to testifying under oath?

[No response.]

Mr. GRIFFITH. Seeing no objections, we'll proceed. The Chair also advises you you're entitled to be advised by counsel pursuant to House Rules. Do any of you desire to be advised by counsel during your testimony today?

[No response.]

Mr. GRIFFITH. Seeing that none have requested that, would each of you rise and raise your right hand, please?

[Witnesses sworn.]

Mr. GRIFFITH. Seeing that all witnesses answered in the affirmative—you are—you may seat—be seated.

Seeing all witnesses have answered in the affirmative, you are now sworn in and under oath subject to the penalties set forth in title 18, section 1001 of the United States Code.

With that, we will now recognize Puesh Kumar for his 5-minute opening statement.

STATEMENTS OF PUESH KUMAR, DIRECTOR, OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE, DEPARTMENT OF ENERGY; BRIAN MAZANEC, PH.D., DEPUTY DIRECTOR, OFFICE OF PREPAREDNESS, ADMINISTRATION FOR STRATEGIC PREPAREDNESS AND RESPONSE, DEPARTMENT OF HEALTH AND HUMAN SERVICES; AND DAVID TRAVERS, PH.D., DIRECTOR, WATER INFRASTRUCTURE AND CYBER RESILIENCE DIVISION, ENVIRONMENTAL PROTECTION AGENCY

STATEMENT OF PUESH KUMAR

Mr. KUMAR. Good afternoon.

Mr. GRIFFITH. You have to push your button there.

Mr. KUMAR. All right, can you—

Mr. GRIFFITH. There we go.

Mr. KUMAR. All right. Good afternoon, Chair McMorris Rodgers, Chair Griffith, and Ranking Member Castor, and distinguished members of the subcommittee. Thank you for the opportunity to testify on behalf of the Department of Energy on the unique role we play as the Sector Risk Management Agency for the U.S. energy sector. I appreciate the interest and support from this committee on this critical issue.

From 2019 through 2023, each Annual Threat Assessment of the U.S. intelligence community from the Director of National Intelligence has pointed to persistent and malicious cyber threats facing U.S. infrastructure. These reports are clear. Our adversaries are targeting U.S. energy infrastructure, and it is a threat to national security.

In May 2021, Colonial Pipeline proactively shut down its pipeline system for 5 days after a cyber criminal group compromised the company's IT network with ransomware. The shutdown ultimately led to a disruption in the supply of petroleum products across multiple States. During the Colonial Pipeline incident, DOE coordinated a whole-of-government response which restored operations quickly and safely while moving field supplies to impacted areas, mitigating impacts to consumers. This response reflects our understanding of consequence management for the U.S. energy sector, our knowledge of the relevant forensics, and our deep appreciation of the impact of energy disruptions for the American public.

Given the immense gravity of the threats we face, it is imperative that we employ a whole-of-government approach to risk management and mitigation. The SRMA model allows us to scale and to work in concert with our counterparts and with partners across the entirety of the Federal Government. As the SRMA for the energy sector, DOE has the day-to-day responsibility and sector-specific expertise to work within the sector and collaborate with the Cybersecurity and Infrastructure Security Agency, or CISA, as the national coordinator.

We value our partnership with CISA. While we bring a depth of knowledge of the energy sector and the tactical and technical elements that keep power and fuel flowing to Americans, CISA serves an important coordinator function and has a unique perspective that is invaluable to DOE's risk management activities.

DOE is uniquely qualified to manage the ever-changing risk landscape for America's energy sector because we have a depth of knowledge specific to generation, transmission, distribution, and consumption of energy of all forms. We also have tremendous expertise on cybersecurity. Additionally, we have an exceptional breadth of capabilities across the department from nuclear physicists and security specialists to subject matter experts in renewable energy and deployment. We regularly avail ourselves to the immense trove of knowledge readily available across the entire department.

My office, the Office of Cybersecurity, Energy Security, and Emergency Response, or CESER, executes our SRMA responsibilities. CESER is built upon a foundation of strong partnerships with industry, State, local, territorial, and Tribal communities, regulators, suppliers, and manufacturers, and the world-class experts at the DOE national laboratories, in addition to academia. It is

through these trusted partnerships that we are able to execute our responsibilities on behalf of DOE as the SRMA for the energy sector.

Through these many efforts ranging from our Energy Threat Analysis Center, or ETAC, pilot to work on securing energy systems were recently highlighted in the President's National Cyber Strategy. The ETAC will bring innovative and robust capabilities to the energy sector and will help us keep pace with the cyber threats headed towards us as a nation. ETAC provides an excellent example of the new and innovative capabilities that our Nation needs to build to effectively collaborate between industry and government to defend our critical infrastructure.

DOE is adept at deploying innovative solutions to complex problems and will continue to do so in the service of the American people, ensuring that U.S. energy sector becomes secure and resilient.

In closing I would like to thank the members of the subcommittee once more for your continued support for SRMAs and for DOE, and CESER specifically. Your commitment to protecting America's critical infrastructure is essential to our continued success. You understand that energy security is critical to our national security.

I am proud of the work that we are doing in DOE and CESER to ensure that the U.S. energy sector remains secure and resilient for Americans today and for generations to come.

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

[The prepared statement of Mr. Kumar follows:]

Testimony of Director Puesh Kumar
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
May 16, 2023

Introduction

Chairman Griffith, Ranking Member Castor and distinguished members of the Subcommittee, thank you for the opportunity to testify on behalf of the Department of Energy (DOE) on the unique role we play as the Sector Risk Management Agency (SRMA) for the United States energy sector. I appreciate the interest and support from the Committee on this critical issue.

My testimony today will focus on the value of SRMAs, the need for specialization by sector, and the role that DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) plays in fulfilling the Department's duties as an SRMA.

The energy sector provides the power and fuel that all other U.S. critical infrastructure sectors depend on to operate. A disruption in the energy system can have a devastating impact to national security, the U.S. economy, and the safety and livelihoods of millions of Americans.

CESER is focused on securing the Nation's energy infrastructure against all hazards, reducing the risks and impacts of cyberattacks, physical incidents and other disruptive events, and supporting state, local, tribal, and territorial governments (SLTT), as well as industry, with response and restoration when a disruption occurs.

The Evolving Threat Landscape

The U.S. energy sector faces three major types of threats: cyber threats, physical threats, and climate-related or natural threats. As the SRMA for the sector, DOE takes an all-hazards approach to risk mitigation, strategically addressing each risk individually and considering points of compounding risk, as when a natural disaster makes energy systems more vulnerable to a physical or cyber-attack.

Cyber risks to energy systems continue to increase, both from Nation states and criminal actors. From 2019 through 2023, each Annual Threat Assessment of the U.S. Intelligence Community from the Director of National Intelligence has pointed to persistent and malicious cyber threats facing U.S. infrastructure. These reports are clear: the cyber actors targeting U.S. energy infrastructure are a threat to national security.

The reports note that both Russia and the People's Republic of China have the capability to launch cyber-attacks against U.S. energy infrastructure that could disrupt critical energy services. The 2019 Annual Threat Assessment states that, "Russia has the ability to execute cyber-attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours..." while the 2023 Assessment says, "China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines..."

Physical threats to the energy sector come in many forms, including petty vandalism, theft, and, as we've seen more recently, targeted gun fire. Physical attacks that result in the disruption of energy flow have both economic and national security impacts and therefore this threat type cannot be underestimated or discounted.

These threats are matched, if not outpaced, by the wrath of climate-related threats such as hurricanes, wildfires, and extreme winter storms, which are happening with greater frequency and intensity year over year. DOE remains committed to working alongside our partners in the energy industry, as well as state emergency managers and community-level representatives, to plan for, prepare for, and ultimately respond to these disasters and their impacts on energy infrastructure and service. CESER and DOE more broadly are working to build resilience into the grid via new technologies, but also via strong and active partnerships that enable swift and strategic collaboration when it is needed most.

Given the immense gravity of the threats currently facing U.S. critical energy infrastructure, it is imperative that we employ a whole-of-government approach to risk management and mitigation. The SRMA model allows us to scale and to work in concert with our counterparts and with partners across the entirety of the federal government.

The Need for SRMAs

Protecting and securing America's critical infrastructure is a multifaceted undertaking and is best managed by those familiar with sector-specific nuances and challenges. As each SRMA is responsible for day-to-day oversight and coordination of the Federal response to risks, it is sensible to divide and conquer, putting those with the most experience and greatest expertise to meet threats head-on in leadership positions in each respective sector.

Presidential Policy Directive 21 (PPD-21), which established the SRMA structure and function within the federal government, states that "each critical infrastructure has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector."

As the SRMA for the energy sector, DOE has the "day-to-day responsibility and sector-specific expertise" to work within the sector and collaborate with the Cybersecurity and Infrastructure Security Agency (CISA) as the National Coordinator for Critical Infrastructure Security and Resilience. We value our partnership with CISA; while we bring a depth of knowledge of the energy sector and the tactical and technical elements that keep power and fuel flowing to

Americans, CISA serves an important coordinator function and has a unique perspective that is invaluable to DOE's risk management activities.

In addition, the Department of Energy has an additional responsibility to the nation as the energy sector is a critical infrastructure sector relied upon by all other sectors. In fact, PPD-21 notes "energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors." Throughout PPD-21, and policies put forth by multiple administrations, the intention that SRMAs would leverage sector-specific expertise to devise and deploy solutions to some of America's greatest security challenges is clear, and the Department of Energy has consistently been recognized for our leadership in this regard.

DOE is uniquely qualified to manage the ever-changing risk landscape for America's energy sector precisely because we have a depth of knowledge specific to the generation, transmission, distribution, and consumption of energy in all its forms. We also have an exceptional breadth of capabilities across the Department, including cybersecurity and emergency response capabilities that reside within CESER, and we do not hesitate to call on the full complement of experts as needed to fulfill our duties. From nuclear physicists and security specialists to subject matter experts in renewable energy development and deployment, we regularly avail ourselves of the immense trove of knowledge readily available within DOE.

In early March, President Biden released the 2023 National Cybersecurity Strategy. In this document DOE was noted as an exemplary SRMA, pointing to the advances the Department is making in operational collaboration, the model that we set for other SRMAs, and the leadership we consistently display. DOE is not only an SRMA but is also an owner and operator of energy systems that fall under SRMA jurisdiction. With this perspective, we are able to identify issues and develop processes that efficiently and effectively address concerns across the sector.

Finally, CESER executes both Emergency Support Function #12 (ESF #12) and SRMA responsibilities on behalf of DOE in close coordination with other offices across the Department and with our interagency partners, including CISA, the FBI, the Federal Emergency Management Agency (FEMA), the Department of Defense (DOD), other agencies, and elements of the Intelligence Community.

The Value of DOE as the SRMA

DOE's work as the SRMA for the energy sector extends to all hazards. In recent years, several examples of the value of the SRMA have emerged from incidents or activities under DOE's purview.

In May 2021, Colonial Pipeline Company proactively shut down its pipeline systems for five days after a cyber-criminal group compromised the company's information technology (IT) network with ransomware. The shutdown ultimately led to a disruption in the supply of petroleum products across multiple states. During the Colonial Pipeline incident, DOE activated its emergency response organization to coordinate with industry, interagency, and state partners, providing situational awareness, analysis of impacts, and supporting response efforts. DOE

coordinated a whole-of-government response to help Colonial resume operations quickly and safely, while moving fuel supplies to impacted areas to mitigate impacts to consumers.

In December 2022, two separate incidents involving gun fire targeting electricity substations in Moore County, North Carolina knocked out power to more than 40,000 customers. In response to these incidents, CESER worked closely with local, state, and federal law enforcement authorities, while also supporting the affected utility as they made every effort to restore power quickly. In emergent situations such as this, DOE plays a particularly critical role, serving as a hub of information flow and communication to provide utilities and other owners and operators of critical energy infrastructure visibility into potential threats and support should they be targeted.

I would be remiss if I did not mention CESER's hurricane response efforts, as we are on the brink of another hurricane season, starting on June 1. The growing intensity of hurricanes is a matter of great concern, as is their detrimental impact on American cities and communities. The provision of energy during an emergency is paramount to the rapid recovery of those affected. CESER's ESF #12 response team stands ready to deploy, to help manage restoration of power and the flow of fuel to those in need. From cyber-attacks to physical attacks, to hurricanes, and beyond, the Department of Energy is very well prepared to respond to and to manage threats to the U.S. energy sector. The work we do domestically also allows us to step up and aid our allies in times of need.

In February 2022, Putin's Russia brutally, illegally, and immorally began its full-scale invasion of the sovereign nation of Ukraine. Even before Russia attacked with tanks and troops on the ground, it had already used energy as a weapon to terrorize the Ukrainian people. Russia's use of energy as a weapon has backfired. It has spurred an international response unprecedented in the history of global energy cooperation. The United States has been a leader in this response. As part of the U.S. effort, DOE has become a reliable partner to the Ukrainian people. The Department was able to leverage our sector expertise and partnership with U.S. energy companies to support Ukrainian energy companies on both cybersecurity and grid restoration efforts during this great time of need. Further, DOE provided energy system cybersecurity training to our allies in Europe.

All this work is reliant on the health and strength of our relationships, both at the state and local levels, and with the owners and operators of America's energy infrastructure.

An SRMA Powered by Partnerships

In addition to working in collaboration with experts from across DOE, CESER is built upon a foundation of partnerships with industry; SLTT communities; regulators like the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC); suppliers and manufacturers; and academia. It is through these trusted relationships that we are able to execute our responsibilities on behalf of DOE as the SRMA for the energy sector.

A large majority of the critical energy infrastructure in the United States is owned and operated by private companies. It is crucial that lines of communication between the Federal government

and these companies remain open and that we approach risk management for the sector with a sense of shared responsibility. CESER facilitates both the Electricity Subsector Coordinating Council (ESCC) and the Oil and Natural Gas Subsector Coordinating Council (ONGSCC) in partnership with DHS and other agencies, bringing representatives from the energy sector together regularly in conversation to identify security and resilience challenges and advance policy, technology, and preparedness solutions.

Similarly, CESER is extremely active on the SLTT front, providing resources and technical assistance to state-level energy and emergency managers, hosting and conducting meetings to connect the dots for state and local leaders on complex issues, and seeking opportunities for collaboration to further our collective mission of realizing a more secure, reliable, and resilient energy sector for all Americans.

Finally, CESER frequently interfaces with the DOE National Labs, organizing, funding, and leading projects to advance the security of the nation's energy systems through advanced research, development, and demonstration. The world-class subject matter experts at the Labs are part of the extensive network of resources that make the DOE the best possible SRMA for the energy sector.

It is fundamentally true that our success as an SRMA is powered by partnerships and bolstered by our unparalleled expertise and the tactical knowledge we can deploy to address incidents in real time. DOE is undoubtedly the most qualified agency to execute the role of the SRMA for the United States energy sector, both now and in the future.

What Lies Ahead

Within the United States energy sector, an incredible transition is underway. New sources of energy generation are coming online; new digital tools and technologies are being leveraged to improve reliability and efficiency; and new market forces are shaping how we interact with energy daily, in vehicles, in homes, and in businesses across the country.

As this transition takes place, CESER is committed to ensuring that DOE, as the SRMA for the sector, keeps pace with evolving and emerging security needs. We are actively involved with the Department's overall grid modernization activities, bringing our security expertise and experience to bear as new technology is deployed and advocating for security by design throughout the grid of tomorrow.

The value DOE brings as the SRMA in this evolving environment will be a concerted focus on innovation, collaboration, and efficiency. On behalf of the Department, CESER will continue to update our risk assessments and response operations and invest in tools and technologies to address the ever-evolving threat landscape.

According to the National Cybersecurity Strategy, the DOE pilot of the Energy Threat Analysis Center (ETAC) provides an example of the new and innovative capabilities that the nation needs to effectively collaborate at the scale and speed needed to defend critical infrastructure. Through this new, operational approach to cyber collaboration, we will close gaps in our collective

situational awareness of threats, improve our ability to mitigate and defend against them, and support the nation's response to incidents within the energy system.

DOE is adept at deploying innovative solutions to complex problems and will continue to do so in service to the American people, ensuring the U.S. energy sector becomes only more secure and resilient with time.

Conclusion

In closing, I would like to thank the members of this Subcommittee once more for your continued bipartisan support for SRMAs across sectors, and for DOE and CESER specifically. Your commitment to protecting America's critical infrastructure is essential for our continued success.

You understand that energy security is critical to our national security. DOE is committed to ensuring that the U.S. energy sector remains secure and resilient for Americans today and for generations to come. Thank you for the opportunity to testify today. I look forward to your questions.

Mr. GRIFFITH. Thank you so much. I now recognize Dr. Mazanec for his 5 minutes of opening statement.

STATEMENT OF BRIAN MAZANEC, Ph.D.

Dr. MAZANEC. Thank you, Mr. Chairman.

Good afternoon, Chairman Griffith, Vice Chair Lesko, Ranking Member Castor, distinguished members of the committee, and staff. Thank you for the opportunity to discuss the Department of Health and Human Services Administration for Strategic Preparedness and Response, known as ASPR's, efforts to strengthen the healthcare and public health sector's preparedness for and response to cyber attacks. ASPR is the department Sector Risk Management Agency, or SRMA, lead. My testimony today summarizes the growing cyber threat, the role of ASPR as the SRMA lead, and our approach to strengthening the sector's cybersecurity.

As you are all too well aware, the healthcare and public health sector continues to experience increasingly sophisticated cyber attacks that exploit complex hospital infrastructures, underfunded cybersecurity functions, and numerous vulnerable legacy medical—medical devices. These cyber attacks against the sector are growing both in number and severity.

The frequency of cyber attacks on hospitals, as has already been noted, more than doubled from 2016 to 2021, with ransomware being the largest threat. Of note, last week the Journal of the American Medical Association published a study indicating that cyber attacks against hospitals not only affect the targeted institution but have a blast radiuslike effect on the surrounding area, similar to conventional disasters.

ASPR is responsible for coordinating healthcare and public health SRMA activities, which we do working as a team with key partners across HHS to include the HHS 405(d) Program and the Health Sector Cybersecurity Coordination Center, known as HC3, and the FDA, to name a few. ASPR in its SRMA role and with active involvement from stakeholders across the department proactively confronts these growing cyber threats and strengthens the Healthcare and Public Health Sector's cyber security posture. Doing so is critical as cyber attacks in this sector have a very real impact on the health and safety of individual Americans.

Imagine the impact on patients as a hospital is forced to abruptly shift to paper records following a ransomware attack on its electronic health records system or loses its ability to conduct MRIs. Cyber safety is patient safety. I'll highlight a few examples of what we are doing to combat this threat.

First, jointly with our interagency and private-sector partners, we develop resources to support risk mitigation activities. We recently published the 2023 edition of the Health Industry's Cybersecurity Practices, known as the HICP, and the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide.

Second, we facilitate sector coordination and in doing so leverage these resources I just mentioned as well as others and collaborate on initiatives to strengthen the sector's cyber posture. Internal to HHS, ASPR manages the Healthcare and Public Health SRMA Cyber Working Group, which brings together experts from across HHS each week to coordinate activities. External to the depart-

ment, multiple HHS divisions work with the Healthcare and Public Health Sector through various sector-focused councils and venues. For example, we regularly coordinate with over 15 government and over 300 private-sector partner organizations through the Healthcare Sector Coordinating Council Joint Cybersecurity Working Group.

The third area of SRMA activities that I want to highlight today focus on leading response planning and supporting incident response. Response planning for cyber incidents is critical as the frequency and intensity of these attacks increase. HHS recently completed a Healthcare and Public Health Sector Cyber Incident Response Plan. Additionally, HHS has organized with CISA and other interagency partners over a dozen tabletop exercises to improve incident response processes.

In responding to cyber threats facing the sector, ASPR coordinates closely with our staff in the regions as well as with CISA and the FBI to inform response operations and mitigate the impacts of patient care and safety. In addition to these activities, the department also utilizes its regulatory role to strengthen the sector's cyber posture.

While I have touched on the efforts within ASPR and across HHS that seek to move the needle forward to strengthen in cybersecurity in the sector, more work needs to be done to meet this growing threat. We are in the process of establishing a dedicated cyber division within ASPR's Office of Critical Infrastructure Protection. If ASPR is granted direct higher authority, as requested through the Pandemic and All Hazards Preparedness in Advancing Innovation Act, PAHPA, reauthorization process, we would be able to more quickly bring on board critical staff with cyber expertise.

Dedicated resources are needed to implement and operate supporting systems, as included in the President's 2024 budget request, to ensure ASPR and HHS are best positioned to execute its SRMA responsibilities to prepare for and respond to cyber attacks on the healthcare and public health sector.

Chairman Griffith, Vice Chair Lesko, Ranking Member Castor, that concludes my statement. I look forward to your questions.

[The prepared statement of Dr. Mazanec follows:]

THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
ADMINISTRATION FOR STRATEGIC PREPAREDNESS AND RESPONSE

Testimony before the
House Energy and Commerce Subcommittee on Oversight and Investigations

Hearing Titled
“Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific
Agencies”

Brian M. Mazanec, PhD
Deputy Director, Office of Preparedness
Administration for Strategic Preparedness and Response

May 16, 2023

Chairman Griffith, Vice Chair Lesko, Ranking Member Castor, and distinguished members of the Committee, it is an honor to testify before you today on the Department of Health and Human Services' (HHS) efforts to strengthen the Healthcare and Public Health (HPH) critical infrastructure sector's preparedness for and response to malign cyber activity.

I am grateful for this opportunity to address this subcommittee and appreciate your continued support in this important area for national and health security. My testimony today summarizes (1) the growing cyber threat facing the HPH sector; (2) the role of HHS and the Department's Administration for Strategic Preparedness and Response (ASPR) as the Sector Risk Management Agency (SRMA) in addressing this threat; and (3) our current approach to strengthen the sector's cybersecurity today and into the future.

As you are all too aware, the HPH sector continues to experience an array of increasingly sophisticated cyberattacks that exploit complex, interconnected hospital infrastructures, historically underfunded cybersecurity functions, and an often-unwieldy number of vulnerable legacy systems and network-connected medical technologies, including medical devices. These cyberattacks against the HPH sector are growing both in numbers and severity, with the frequency of cyberattacks on hospitals and health systems more than doubling from 2016 to 2021.¹ Specific to ransomware, according to the Federal Bureau of Investigation's (FBI) Internet Crime Reports, the HPH sector experienced a 42 percent increase in ransomware attacks compared to 2021.² There are, on average, six or more significant cyber incidents impacting the sector every week. Ransomware is currently the largest threat to the HPH sector and the Administration has identified it as a key sector, alongside the transportation, banking, and water sectors.³ The bad actors conducting these cyberattacks against the HPH sector generally have a few known motivations influencing their actions, including financially motivated crime; state-sponsored attacks for the purposes of exfiltration of sensitive information or to generate currency; and hacktivism to influence or inflict reputational impacts.

Cyberattacks directed at hospitals can impact patient care and safety, including extended disruptions caused by multi-week outages; patient diversion to other facilities; and strain on acute care provisioning and capacity, causing the cancellation of medical appointments, non-rendered services, and delayed medical procedures (particularly elective procedures). Further, a recent study reported data from an unaffected hospital geographically adjacent to an institution that had been hit by ransomware and found that the emergency room of the unaffected hospital had significant increases in the numbers of patients arriving for treatment, the number of ambulances diverting patients, the amount of time that patients waited to receive care, and an increase in time-sensitive, resource-intensive medical conditions like stroke requiring treatment.⁴ This data demonstrates that cyberattacks against hospitals not only affect the targeted institution, but have "blast radius" effects on the surrounding region, similar to conventional disasters like earthquakes or hurricanes.

¹ *JAMA Health Forum*. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873

² Federal Bureau of Investigation, *Internet Crime Report 2021*, and *Crime Report 2022*

³ <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/>

⁴ <https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585>

A recent study from IBM reports that the average cost of health care cyberattacks averaged \$4.35 million in 2022.⁵ The average cost has climbed 12.7 percent since 2020, making health care cyberattacks the most expensive data breaches out of any industry.

ASPR Serves as the HHS Lead Sector Risk Management Agency for the Healthcare and Public Health Sector

ASPR's mission is to help the country prepare for, respond to, and recover from public health emergencies and disasters. A part of that responsibility as the SRMA, ASPR helps prepare the health care sector for disasters and emergency events through the Health Care Readiness and Recovery program.

In 2013, Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience established the federal government's strategy to protect the critical infrastructure that underpins American society.⁶ PPD-21 defined 16 critical infrastructure sectors and identified specific agencies to support the management of threats and hazards faced by each sector, including the HPH sector. The 2021 National Defense Authorization Act then codified core responsibilities for each of these lead agencies, redefining them as SRMAs. HHS is the designated SRMA for the HPH sector, responsible for providing specialized sector-specific expertise and supporting programs and associated activities for the sector.

As directed by HHS, ASPR carries out this SRMA function through our Office of Critical Infrastructure Protection within our Office of Preparedness. ASPR coordinates regularly with our colleagues across HHS, including the Food and Drug Administration (FDA), the HHS 405(d) Program and Health Sector Cybersecurity Coordination Center (HC3) within the Office of the Chief Information Officer (OCIO), the Office for Civil Rights (OCR), the Office of the National Coordinator for Health Information Technology (ONC), the Centers for Medicare & Medicaid Services (CMS), and the HHS Office of the Inspector General (OIG), to name a few.

Working as a team, all HHS agencies and divisions bring together their unique cybersecurity perspectives, expertise, and authorities as a single collaborative effort to assist the HPH sector, from direct engagement with the HPH sector on cybersecurity activities to collaborative regulatory actions with the goal of HPH sector protection. For example, OCR collaborates with ONC on development of and enhancements to the Security Risk Assessment (SRA) Tool that provides small- and medium-sized HPH sector organizations a tool to identify and assess security risks to health information within their organizations. HHS is best positioned to serve as SRMA for the HPH sector, as we leverage existing relationships in the regions and with HPH sector partners and utilize our resident expertise in the Department.

HHS—in Coordination with Key Partners—is Working to Strengthen the Cybersecurity of the Healthcare and Public Health Sector

⁵ IBM, *Cost of a Data Breach 2022 Report*; <https://www.scmagazine.com/analysis/ransomware/scripps-health-cyberattack-ehr-downtime-caused-112-7m-in-lost-revenue-recovery#>

⁶ *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*, February 12, 2013

HHS—with ASPR coordinating in its SRMA role, coupled with active involvement from other stakeholders across the Department—is undertaking numerous proactive measures to ensure we are well-positioned to address these growing cyber threats and strengthen the HPH sector’s cybersecurity posture. SRMA responsibilities involve activities focused on sector risk management and assessing sector risk; sector coordination; facilitating information sharing; supporting incident management; and contributing to emergency response.

Developing Resources and Supporting Risk Mitigation Activities

HHS—jointly with our interagency and private sector partners—creates detailed resources and materials for the sector providing best practices and recommendations for building and maintaining cyber resilience and preparedness. HHS recently published the 2023 edition of the Health Industry Cybersecurity Practices (HICP), the Hospital Resiliency Landscape Analysis, and the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide. HHS now offers free cybersecurity training and resources on its website through an education platform called “405(d)’s Knowledge on Demand” and ASPR’s Technical Resources, Assistance Center, and Information Exchange (TRACIE), which provides online technical resources on health care cybersecurity. These resources are widely distributed and utilized; for example, in the first week of release, the 2023 version of the HICP had over 7,600 downloads and the Hospital Resiliency Landscape Analysis had over 6,800 downloads. HHS also collaborates with federal partners to provide actionable, credible threat intelligence to the sector to help it better strengthen the security posture of the HPH infrastructure. The HHS Office of National Security, HC3, and ASPR work together, along with our interagency partners, on identifying, collating, and analyzing threat intelligence. For example, over the past three years, HC3 has released over 190 products to support the HPH sector, including alerts, threat actor profiles, and threat briefings. HHS also recommends a Department of Homeland Security (DHS)-created cybersecurity checklist and primer as well as a no-cost Cyber Resilience Review, which is a voluntary, non-technical assessment to evaluate an organization’s operational resilience and cybersecurity practices.

Facilitating Sector Coordination

HHS leverages these previously mentioned resources and closely coordinates and collaborates on cyber-related initiatives intended to strengthen the HPH sector’s cybersecurity posture with DHS’ Cybersecurity and Infrastructure Security Agency (CISA) and other relevant federal departments and agencies; with critical infrastructure owners and operators; with independent regulatory agencies where appropriate; and with State, local, tribal, and territorial (SLTT) entities. OCR, FDA, OCIO, ONC, ASPR, and other HHS divisions work closely with the HPH sector through the Healthcare Sector Coordinating Council (HSCC) by collaborating with peers in the private sector to develop and publish resources and best practices on protecting the HPH sector, including documents on securing legacy devices and implementing a cybersecurity framework. For example, we coordinate with over 15 government and over 300 private sector partner organizations via the HSCC Joint Cybersecurity Working Group—which has 16 active task groups—to align security approaches, assess risks and share mitigation measures.

Internal to HHS, ASPR manages the HPH SRMA Cyber Working Group, which brings together cyber experts from across HHS each week to coordinate HHS activities related to private sector coordination and to address critical information requests and policy issues identified internally or by HHS leadership, CISA, the National Security Council, and the Office of the National Cyber Director. These efforts are part of the larger HPH sector efforts, supporting and being supported by the broader all-hazards Sector Coordinating Council and Government Coordinating Council.

Leading Response Planning and Supporting Incident Response

Response planning for cyber incidents is critical as the frequency and intensity of these attacks increase. HHS recently completed a *Healthcare and Public Health Sector Risk Management Agency Cyber Incident Response Plan*, which provides the framework to coordinate processes for HPH sector cyber incident management within HHS. HHS is also developing a public-private sector partnership playbook to promote collaboration during all-hazards events, including cyber events. HHS has engaged with CISA and other sector partners to support over a dozen tabletop exercises to improve sector incident responses process and procedures. During these exercises, HHS provides subject matter expertise on how the entity could be better prepared—for example, by advising an entity to include a communications plan for how to engage staff and the public on the incident and expectations for recovery.

In responding to actual cyber incidents facing the HPH sector, HHS reaches out to over 8,000 government and private sector partners across the sector during cybersecurity incidents to inform response operations and mitigate impacts to patient care. From January 1, 2023, to May 8, 2023, we triaged 69 cybersecurity incidents, working closely with CISA and the Federal Bureau of Investigation (FBI) and conducting outreach to multiple organizations for information and data analyses to determine potential impacts to patient care and safety. We work closely with our FBI and CISA colleagues to identify technical information that can be shared with the private sector and providing actionable intelligence to them so they can evaluate their systems to eliminate or mitigate related vulnerabilities.

Utilizing Regulations to Enhance Cybersecurity

HHS also has a regulatory role over certain elements of the HPH sector, and this role helps strengthen the sector's cyber posture. OCR administers and enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules. The HIPAA Security Rule establishes national standards to protect electronic protected health information (ePHI) created, received, maintained, or transmitted by HIPAA-regulated entities. The Security Rule requires appropriate safeguards to ensure the confidentiality, integrity, and availability of ePHI. Further, regulated entities that can adequately demonstrate that recognized security practices—such as the current version of the HICP and the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide—have been in place for the previous twelve months or more may be able to mitigate certain penalties following a cyber incident.

With respect to medical devices, the FDA clears, authorizes, and approves devices to be marketed when there is a reasonable assurance that the devices are safe and effective for their intended use, which includes the cybersecurity of such devices. FDA provides guidance

regarding the cybersecurity expectations of medical devices for medical device manufacturers, which is also useful for health care delivery organizations as they review their management of medical device cybersecurity. Additionally, section 3305 of the Consolidated Appropriations Act, 2023 granted FDA additional statutory authority to provide for the reasonable assurance of cybersecurity within medical devices, by requiring that medical devices meet select cybersecurity requirements.

Challenges Going Forward

HHS is working diligently to strengthen cyber security and address the impacts of cyberattacks on the health care system. As we move forward, there are additional authorities and resources that would advance ASPR's ability to fully implement its plan to bolster HHS's cyber SRMA activities. For example, we are in the process of establishing a dedicated Cyber Division within ASPR's Office of Critical Infrastructure Protection. If ASPR is granted direct hire authority, as requested through the Pandemic and All-Hazards Preparedness Act (PAHPA) reauthorization process, we would be able to bring critical staff with cyber expertise into the organization more quickly and move forward to address challenges without delay. We would also be better positioned to immediately expand and enhance our efforts as the SRMA lead for the HPH sector. Additionally, we are looking to establish a new HHS cyber incident ticketing system to better track incidents and strengthen threat intelligence sharing through embedded liaisons within CISA and the FBI. Dedicated resources are needed to implement and operate supporting systems, as included in the FY 2024 President's Budget request. We continually assess and identify whether any additional authorities are needed to support our role as SRMA for the HPH sector, and I look forward to working with all of you if any other needs arise.

Conclusion

As increasingly sophisticated and pervasive cyber threats continue to grow and evolve, ASPR remains committed to executing its SRMA responsibilities to prepare for and respond to cyber threats in the HPH sector. Thank you again for inviting me to testify before you today. I look forward to answering your questions and working with you and your staff to strengthen the cybersecurity of the HPH sector.

Mr. GRIFFITH. Thank you so much. Now I recognize Mr.—Dr. Travers for his 5-minute opening statement.

STATEMENT OF DAVID TRAVERS. Ph.D.

Dr. TRAVERS. Great. Good afternoon, Chairman Griffith, Ranking Member Castor, and members of the committee. I am David Travers, and I serve as the Director of the Water Infrastructure and Cyber Resilience Division at USCPA. Thank you for the opportunity to speak to you today about the agency's work with our partners to improve the security and resilience of America's water systems to the threat of cyber attacks. This mission is among EPA's highest homeland security priorities.

Water systems are frequently targeted for cyber attacks by both state-sponsored actors and criminal groups. These attacks have stolen valuable financial and customer information, destroyed information networks, and disabled communication systems. Recovery costs have ranged into the millions of dollars. Importantly, cyber attacks can also manipulate and disable the process control networks for the treatment and distribution of water, which has the potential to endanger public health. The adoption of cybersecurity best practices by water systems to reduce the risk of these attacks is essential.

EPA is the Sector Risk Management Agency for the water and wastewater system sector. We are responsible for enhancing the sector's security and resilience against all hazards, including cyber attacks. Multiple Federal statutes, directives, and Executive orders mandate the agency's cybersecurity mission.

The water and wastewater system sector includes just under 150,000 drinking water systems and 16,000 wastewater systems across the United States and territories. The utilities range in size from serving less than 500 to over 8 million customers. Most water systems are small and face unique challenges with the resources and expertise needed for providing safe drinking water.

EPA fulfills its mission in cybersecurity in coordination with DHS, the Water Sector Coordinating Council of industry representatives, and other Federal, State, local, Tribal, territorial and private-sector partners. EPA has worked with these partners for over 10 years to promote the adoption of cybersecurity best practices by water and wastewater systems. We provide training, develop guidance tools and resources, and offer technical assistance.

For instance, we have trained thousands of water systems nationwide on cybersecurity risks and resilience. EPA has given one-on-one technical assistance by subject matter experts to hundreds of water and wastewater systems to identify gaps in cybersecurity practices and implement remediation actions tailored to the utility's resources and goals. EPA has created a suite of cybersecurity guidance materials and tools specifically for the water sector in key areas like cyber incident planning and emergency response.

While the work of EPA and its partners have made important gains in cybersecurity, the most significant cyber risk in the water sector remains the failure of many utilities to adopt best practices. This critical vulnerability is apparent both from a recent industry survey, which showed that most utilities had not taken key steps to protect their operations, and from cyber incidents at water sys-

tems which have exploited the failure to implement cybersecurity best practices.

Due to this continued vulnerability, the increasing frequency of cyber attacks on critical infrastructure facilities as reported by the FBI and DHS, and the public health risk of a cyber attack on a water system, EPA has recently used existing regulatory authority to improve cybersecurity in the sector. In March, EPA issued a memo stating that regular State audits of water system operations, called sanitary surveys, must include an evaluation of cybersecurity. If the State finds a significant deficiency in cybersecurity during the sanitary survey, then the water system must correct it. States determine how they evaluate their water systems and what actions their water systems take to correct deficiencies.

The use of sanitary surveys to improve cybersecurity at water systems builds on the provisions of 2018 America's Water Infrastructure Act, or AWIA. Under EPA's policy, cybersecurity practices are assessed at all water systems not just the subject to AWIA. And the State ensures that water systems take corrective actions to address deficiencies.

EPA knows that many States lack capacity to assist water systems in protecting against cyber threats. Consequently, EPA is providing robust guidance, training, and technical assistance to help States. For example, EPA's Water Sector Cybersecurity Evaluation Program carries out assessments of cybersecurity practices at water systems upon request, which can lift the burden for the State to perform the assessment during a sanitary survey.

Moving forward, the agency will continue to strive with our water sector partners in the essential work of ensuring that water systems adopt cybersecurity best practices that will reduce risk, enhance resilience, and protect public health.

Thank you for the opportunity to testify before you today, and I look forward to our discussion.

[The prepared testimony of Dr. Travers follows:]

**TESTIMONY OF DAVID TRAVERS
DIRECTOR OF THE WATER INFRASTRUCTURE AND CYBER RESILIENCE
DIVISION
U.S. ENVIRONMENTAL PROTECTION AGENCY**

**BEFORE THE
HOUSE ENERGY AND COMMERCE COMMITTEE
OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE**

May 16, 2023

Good morning, Chairman Griffith, Ranking Member Castor, and Members of the Subcommittee. I am David Travers and I serve as the Director of the Water Infrastructure and Cyber Resilience Division of the Office of Water at the U.S. Environmental Protection Agency (EPA). Thank you for the opportunity to speak to you today about the Agency's work with our partners to improve the security and resilience of America's water and wastewater systems to the persistent threat of cyber-attacks. This mission is among EPA's highest homeland security priorities.

As reported by the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS), critical infrastructure facilities, including water and wastewater systems, are being targeted for cyber-attacks with increasing frequency by both state-sponsored actors and criminal groups. Cyber-attacks on water and wastewater systems have stolen valuable financial data and customer information, destroyed essential information networks, and disabled communication systems. Recovery costs have ranged into the millions of dollars. More significantly, cyber-attacks can manipulate and disable the process control networks that are responsible for the treatment and distribution of water, which has the significant potential to endanger public health. Accordingly, the adoption of cybersecurity best-practices by water and wastewater systems to reduce the risk of these attacks is essential.

As you know, the federal government has identified 16 critical infrastructure sectors. Each of these sectors has a Sector Risk Management Agency (SRMA), which is the federal lead agency responsible for enhancing that sector's security and resilience against all hazards, including cyberattacks. By Presidential order, EPA serves as the SRMA for the water and wastewater systems sector due to our expertise in this area and the relationships we have cultivated with states and Tribes under the cooperative federalism of the Safe Drinking Water Act and Clean Water Act. Because the statutes allow EPA to treat Tribes as states, my discussion of "states" includes Tribes that are treated as states for purposes of these statutes. Multiple federal statutes, Directives, and Executive Orders mandate the Agency's cybersecurity mission.

The water and wastewater systems sector includes just under 150,000 public water systems (PWSs), which provide drinking water, and 16,000 publicly owned treatment works (POTWs), which treat wastewater, across the United States and territories. They range in size from serving less than 500 to more than 8 million customers. Small PWSs, meaning those that serve 10,000 people or fewer, make up 97% of all PWSs. Many small systems face challenges in reliably providing safe drinking water, including revenue shortfalls, aging infrastructure, and adequate staffing and expertise, and may lack the capabilities necessary to plan for and respond to natural and manmade threats.

EPA fulfills its critical mission in cybersecurity for the water and wastewater systems sector in coordination with DHS, the Water Sector Coordinating Council of industry representatives, and other federal, state, local, tribal, territorial, and private sector partners. EPA has worked with these partners for over 10 years to promote the adoption of cybersecurity best practices by water and wastewater systems through providing training, guidance, and technical assistance. I'm pleased to share with you several of these efforts.

- We have provided training on cybersecurity best practices, as well as threats, vulnerabilities, and incident response, to thousands of water and wastewater systems nationwide.
- Since 2017, EPA has provided direct individual technical assistance to water and wastewater systems using subject matter experts who help to assess the utility's current cybersecurity practices, identify gaps, and implement remediation actions to reduce risk that are tailored to the utility's resources and goals. To date, 235 utilities have participated in this program.
- To support water systems with cyber incident response planning, we have developed a *Cyber Incident Action Checklist* that guides utilities through preparing for, responding to, and recovering from a cyber-attack. This checklist has been incorporated into the Agency's *Water Utility Response On-the-Go* app to assist utilities when they cannot easily access the hardcopy versions of their emergency response plans.
- EPA understands the criticality of exercising emergency response planning and has created the *Water System Cybersecurity Tabletop Exercise* module to guide utilities with testing their readiness for a cyber incident. Additionally, we have conducted cybersecurity tabletop exercises for water systems at both the local and state level. The Agency has also developed the *Cyber Incident Response Plan Template*, which is currently under review by the Water Sector Coordinating Council, to assist water systems with building these sections within their existing Emergency Response Plans, recognizing that many small water systems will need a template to develop a strong plan.

- We continuously work in partnership with the National Security Council, including regular participation in the Cyber Response Group and other interagency work groups, to address cybersecurity policy issues and cyber incidents.
- EPA is currently partnering with the Water Sector Coordinating Council to craft the *Water Incident Severity Schema*, which will help the United States Government appropriately respond with the level of coordination and resources necessary to support water systems that are impacted by cyber incidents. A guide to cybersecurity insurance is under development as well.
- EPA consulted a workgroup comprised of the Water Sector Coordinating Council, Water Government Coordinating Council, and CISA to develop a *Prioritization Framework*, which describes a methodology for prioritizing public water systems for technical cybersecurity support and consulted with the workgroup again during the development of a *Technical Cybersecurity Support Plan* for public water systems, which is based on existing authorities of EPA and CISA for providing support to public water systems and the *Prioritization Framework*. EPA submitted the *Prioritization Framework* to Congress in May 2022 and the *Report to Congress Technical Cybersecurity Support Plan for Public Water Systems* in August 2022, pursuant to the Infrastructure Investment and Jobs Act SDWA amendment Section 1420A, *Cybersecurity Support for Public Water Systems*.
- Lastly, EPA has continued to request, identify, receive, and disseminate cybersecurity intelligence and cyber threat information relevant to the water sector through the EPA Federal Intelligence Coordination Office.

While EPA and its partners have achieved important gains in cybersecurity in the water and wastewater systems sector, the most significant cyber-risk in this sector is the continuing

failure of many utilities to adopt basic cybersecurity best practices. For example, in a self-reported 2021 survey of water systems conducted by water sector associations, only 31% of respondents had identified all their operational technology-networked assets, and just 22% had fully implemented cyber protections. Further, many reported incidents of cyber-attacks on water and wastewater systems have exploited this failure to implement cybersecurity best practices. Consequently, many water and wastewater systems remain highly susceptible to cyber-attacks that could disrupt their operations.

Due to this continued significant vulnerability of many water systems to cyber-attacks, the increasing frequency of cyber-attacks on critical infrastructure facilities, and the potentially significant public health impacts of a cyber-attack on a water system, EPA has leveraged its existing regulatory authority to improve cybersecurity in the sector. Accordingly, on March 3, 2023, EPA released a memorandum titled *Addressing PWS cybersecurity in sanitary surveys or an alternate process*. This memo was designed to ensure that all water systems are taking important steps to strengthen cybersecurity and to acknowledge that states have flexibility on how best to do this based on local needs.

The memorandum conveys EPA's interpretation of its existing regulations that states must include cybersecurity when they conduct regular audits of water systems through sanitary surveys or an alternate process. State sanitary surveys provide the fundamental touchpoint between the government and water systems through which states ensure that water systems are providing safe drinking water. Sanitary surveys are utilized to protect water utilities from physical vulnerabilities, and they should also be used to address modern cyber threats. Using this existing authority is essential to quickly strengthen this sector's cybersecurity across the nation.

At the same time, EPA acknowledged that state co-regulators have flexibility in how they implement the relevant regulations. By confirming and supporting state flexibility, EPA took a balanced approach to quickly and meaningfully reduce cybersecurity risks while avoiding inflexible, uniform, and costly requirements for states and water systems. EPA clarified that under its regulations, states may choose from three options when evaluating cybersecurity:

1. States may allow water systems to conduct a self-assessment or third-party facilitated assessment prior to the sanitary survey and then review the findings during the sanitary survey for unaddressed gaps that may represent significant deficiencies.
2. States may conduct the assessment while performing the sanitary survey in a traditional inspection format.
3. States may use an alternative program to conduct the assessment, but it must be as stringent as the sanitary survey program, occur no less frequently than the sanitary survey, and address gaps consistent with the significant deficiency process described in EPA's regulations.

The use of sanitary surveys to improve cybersecurity at water systems augments, and does not duplicate, the cybersecurity provisions in the 2018 America's Water Infrastructure Act (AWIA). First, EPA's interpretation of its regulations as described in the memo applies to all water systems, rather than the subset of community water systems subject to AWIA. Second, when a state evaluates the adequacy of the cybersecurity for producing and distributing safe water as part of a sanitary survey or alternate program, the state provides an assessment that is independent of the one performed by the water system under AWIA. Third, if the state identifies a significant deficiency in cybersecurity during a sanitary survey or alternate program, the water system must take necessary corrective action to address the deficiency, which is not the case for

risks or other vulnerabilities identified by a water system under AWIA. Water systems that developed risk and resilience assessments and emergency response plans under AWIA may, however, use these documents to support the evaluation of cybersecurity during their sanitary surveys or alternate program.

The approach of using sanitary surveys to assure cybersecurity at water systems has additional benefits. It retains the principle of state oversight of water systems; offers significant flexibility and support to states in how cybersecurity at water systems is evaluated; gives states the discretion to determine when a cybersecurity gap at an individual water system is a significant deficiency that must be addressed; and allows the state to work with the water system to develop a tailored site-specific solution to correct the cybersecurity gap. Moreover, relying on an existing regulatory structure allows for immediate implementation rather than the years-long process that developing a new regulation would entail.

EPA appreciates that while some states have established programs to evaluate water system cybersecurity practices, many states currently have less capacity to assist water systems in building protections against cyber threats. Consequently, EPA is providing guidance, training, and technical assistance, as briefly summarized below, to help states assess cybersecurity at water systems through sanitary surveys or an alternate program and to aid water systems with implementing cybersecurity best practices. These resources, as well as additional information supporting cybersecurity at water systems, are available at <https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector>.

- **Guidance.** EPA has published a primary guidance document, *Evaluating Cybersecurity in PWS Sanitary Surveys*, to help states and water systems assess cybersecurity for critical gaps, including potential significant deficiencies, and select remediation actions

appropriate for the capabilities and circumstances of the water system. EPA developed this guidance using the CISA *Cybersecurity Performance Goals*. Additional guidance covers the protection of security-sensitive information, potential funding, including EPA's *Drinking Water State Revolving Fund* and the CISA *State and Local Cybersecurity Grant Program*, and other recommended public and private-sector cybersecurity assessment methods.

- **Training.** In 2023, EPA is offering training for states and water systems on evaluating cybersecurity in sanitary surveys and implementing cybersecurity best practices. For states, EPA is providing in-person and remote training in each EPA Region. For water systems, EPA is delivering a series of national topic-specific webinars.
- **Technical Assistance.** Under EPA's *Cybersecurity Technical Assistance Program for the Water Sector*, water systems and states can submit questions or consult with a subject matter expert regarding water system cybersecurity, such as identifying whether a cybersecurity gap should be considered a significant deficiency or selecting appropriate risk mitigation actions. EPA's *Water Sector Cybersecurity Evaluation Program* carries out assessments of cybersecurity practices at water systems upon request by the system. The assessment follows the CISA Cybersecurity Performance Goals. The water system receives a report that shows gaps in cybersecurity, including potential significant deficiencies, which the water system can provide to the state to review during a sanitary survey.

EPA guidance also highlights important resources for water systems from water sector partners in both the government and the private sector. Examples include:

- The *Cybersecurity Framework* from the National Institute of Standards and Technology,

- The CISA *Cyber Hygiene Services* program,
- CISA *Cybersecurity Advisors*,
- The United States Department of Agriculture Rural Development Circuit Rider program and Rural Utilities Service Water and Environmental programs that provide loans, grants, loan guarantees, and technical assistance for water systems in rural communities of 10,000 people or less,
- *Water Information Sharing and Analysis Center* (ISAC) threat and response resources,
- *Multi-State ISAC* information sharing and incident response assistance,
- *American Water Works Association* guidance and tools, and
- *National Rural Water Association* training and guidance for small water systems.

EPA notes that prior to issuing the memorandum on cybersecurity in water system sanitary surveys, the Agency engaged water sector stakeholders in multiple venues to solicit input on this policy approach, including with our state co-regulators and water systems and associations. EPA derived valuable insight from these engagements, which the Agency has incorporated into the memorandum and guidance.

Moving forward, EPA will continue our work with our public and private sector partners to help water and wastewater systems become more secure and resilient against both natural hazards and malevolent acts, including the threat of cyber-attacks. These efforts remain an essential component of EPA's mission to protect public health and the environment.

Thank you for the opportunity to testify before you today, and I look forward to our discussion.

Mr. GRIFFITH. Thank you very much for your testimony. And we will now move into the question-and-answer portion of the hearing, and I will begin the questioning and recognize myself for 5 minutes.

Dr. Mazanec, as you discussed in your testimony, hospitals' cybersecurity incidents are particularly expensive and can lead to tremendous patient impact, such as the temporary cancellation of elective procedures and patient diversion to nearby hospitals—when there are nearby hospitals. In some of the rural areas, they aren't there. Much more difficult.

Given these potentially devastating effects, could you give a broad example of what the Administration for Strategic Preparedness and Response does to mitigate a cyber attack when they first hear of it?

Dr. MAZANEC. Thank you, Mr. Chairman, that's an excellent question. As you noted in your question, I think part of the challenge we face with the healthcare and public health sector is the complexity of the sector itself. It's incredibly diverse, you have large hospital systems, you have small, rural hospitals. Very different resource allocations to address the growing and pervasive cyber threat that exists.

One of the things that we're doing I mentioned in my opening statement in terms of developing resources, we tailor those and try to make them as accessible as possible, particularly for those underresourced or smaller hospitals. So the HICP, the Health Industry Cybersecurity Practices Guide that we recently updated, has essentially bifurcated sections that focus and have resources ready to go off the shelf for small hospitals as well as resources tailored to the larger elements of this sector.

But this is something that we need to continue to stay abreast of and focus on, and we're actively working with our partners in the sector to understand their needs, and we'll continue to provide tailored resources as best we can.

Mr. GRIFFITH. Thank you very much.

Dr. Travers, the Water and Wastewater Sector relies on a stable energy supply to power water utilities. Given this interdependence, how does the EPA coordinate with the Department of Energy to prepare for a cyber incident that interrupts the supply of energy to a water system?

Dr. TRAVERS. Thank you for the question, Chairman Griffith. Each of us on the panel today I think represents a sector critical to this Nation. I'm not sure what community could function without power, water, and adequate healthcare. We engage extensively with other Sector Risk Management Agencies, including the Department of Energy and Health and Human Services.

So an example of that coordination, since you asked specifically about energy, we have activities relevant to the Department of Energy where we developed a Power Resilience Guide which enables water systems to build redundancy, understand the countermeasures that are available to them to enhance their resilience if the power should go out, whether because of a cyber attack or because of a natural disaster.

We also host training of both power sector entities and water systems so that each can understand the dependence of one on the

other. As you implied in your question, water systems cannot function generally without a supply of electricity. It's critical for the treatment of water, distribution of water, storage of water—virtually every facet of producing and delivering water systems.

But because of these robust engagements with both DOE, with entities within the energy sector, and with entities within the water sector, I believe we have cultivated a robust level of coordination among our respective sectors.

Mr. GRIFFITH. Thank you.

Mr. Kumar, Colonial Pipeline of May 2021 obviously caused a great deal of disruption. How did the Department's knowledge of and preexisting relationship within the oil and gas sector prepare to assist with a Federal response?

Mr. KUMAR. Chairman, thank you for the question. When it came to Colonial, when you're responding to an incident, that doesn't—that relationship isn't developed during an incident, it's developed during blue sky days, as well call it. We've had a longstanding relationship with Colonial because of natural hazards, because of hurricanes, and other climate-based risks that we were working with them on long before the cyber incident.

And so when Colonial happened, we were one of their first calls. They called us and said, hey, we just had this cyber incident and we think we have to turn off the pipeline. And so we were able to immediately get into gear and work with them to understand what is going to be the potential impact of fuel supply, but also the cyber side.

So it really ended up being two incidents. One was the cyber side in terms of the cyber actors potentially on their networks. The other part that we were concerned about was the consequence of a pipeline, a critical pipeline, being down. And so we were able to not only leverage our own expertise across the Department, across offices such as our office, fossil energy, but also the national laboratories, to really come and support them, and we brought along the entire whole-of-government approach, so we brought DHS, the FBI, and other agencies to ensure Colonial had the support they needed. I was on daily calls with Colonial's CEO.

And so this is really important. We need to have those relationships with the sector well before an incident, whether it's a cyber attack or a physical incident, to be able to carry out our responsibilities.

Mr. GRIFFITH. And help me with my recollection. Did you all coordinate with the other suppliers in the areas close by to try to increase their supply, or was that another agency?

Mr. KUMAR. Absolutely, sir. We worked with all of the suppliers to make sure. We also worked with the States because the States need to be prepared.

Mr. GRIFFITH. Right.

Mr. KUMAR. So it was—we had to work with everyone.

Mr. GRIFFITH. Thank you very much, I appreciate it.

And I yield back. I now recognize the gentlelady from Florida, Ms. Castor, ranking member of this subcommittee, for her 5 minutes of questioning.

Ms. CASTOR. Well, thank you, Mr. Chairman, and thanks again to our witnesses for being here.

I believe that improving grid resiliency and the whole modernization of the grid is an important part of our transition to cleaner, cheaper energy. And while we often think of physical infrastructure as the transformers and the power lines, there are very innovative new digital tools, distributed systems, all sorts of flexible technologies that are also essential to resiliency.

So I want you to help explain what you see going on in the energy sector. I know we're very focused on the—this brazen cyber attack on—like a Colonial Pipeline hack that can bring regions of the country to a standstill, but I think that relying on a diverse mix of clean energy, energy efficiency tools can really help mitigate the reach of cyber attacks on our energy system. What do you see going on across the country now with these new, innovative technologies?

Mr. KUMAR. Ranking Member Castor, thank you for that question. The energy sector is undergoing a tremendous shift. We're looking at new sources of energy that are going to be connecting into the electric grid as we know it. We're going to be looking at new technologies to power all of these connections, and so we're seeing a lot of changes. And from my vantage point, there's some big shifts. Certainly the threats.

We're continuing to see increased cyber threats, but we're seeing digitization. It's not—it's clean energy's fueling it, but it's also consumers wanting more control over their energy usage, whether it's electric vehicles plugging in or smart thermostats. We're seeing a lot more of this connectivity.

And so as we see this connectivity, there's certainly concerns that we have when it comes to cybersecurity. We want to make sure that as we're deploying these new systems we're building in cybersecurity. That has to be a fundamental thing that we do, much like decades ago we built in safety. So cybersecurity, we think, has to be fundamental to this.

Now as we start to think of technologies and architecture such as microgrids and energy storage, there's also an opportunity there, because as we're building out these new types of distribution-connected resources, they could also act as resilience for the grid. So if there's a certain portion on the grid that goes down because of a hurricane or a cyber incident, could we separate that portion so that we can harden another portion?

There's opportunities we have to build in resilience as we go forward, and that's something that we're really focused on working on in partnership with other departments of the agency. So that's—it's a really great point, and I appreciate the question.

Ms. CASTOR. So what is the current status of the law if a utility or an energy supplier undergoes a cyber attack? You said Colonial, for example, contacted DOE, but remind us, what is the current status of the law for those critical infrastructure energy suppliers to notify you about a cyber attack?

Mr. KUMAR. Ma'am, that's a great question. We—at DOE we have a reporting requirement. We've had it for over a decade, where electricity companies have to report to the Department whenever there's any type of disruption to the bulk power system. And again, it's broader than cyber. It's hurricanes and other outages, anything that can cause a disruption on the electricity sector, it needs to be reported to the Department.

And so to that end, we have the reporting requirement for electricity, and we think it's really helpful because we need to understand what could be the cascading impact across the country. And so we get that reporting, we get it through not only directly, the electricity companies, but we also work closely with organizations called the Information Sharing and Analysis Centers, or the ISACs. Those ISACs are comprised of electricity, oil and natural gas companies, and increasingly renewable companies.

And so we work with them on a daily basis, if not a minute-by-minute basis, on what's going on in the sector so we can get ahead of it and be able to take quick action.

Ms. CASTOR. And you feel like the private-sector entities are fully bought in with you, they're—you haven't come across folks that are trying to hide the ball or distract you or—what's the current status of cooperation across the energy sector?

Mr. KUMAR. Generally speaking, what we see is these companies want to let us know what's going on because they also want to share that information and cascade it with their peers across the sector. That's generally what I have seen, and so we need to continue encouraging that because, if something's happening in one part of the country, we need another energy company to know in another part of the country—country. So this is a really important piece. Generally, I am seeing that they are willing to share when there is an incident.

Ms. CASTOR. Thank you very much.

I yield back my time.

Mr. GRIFFITH. The gentlelady yields back. I now recognize the gentleman from Kentucky, Chairman of the Energy Subcommittee—excuse me, of the Health Subcommittee.

Mr. GUTHRIE. Yes, sir.

Mr. GRIFFITH. I got my Energy Subcommittee in the chair coming up.

Mr. GUTHRIE. You got the next one. You get Energy next.

Mr. GRIFFITH. Yes, get Energy next. First it's going to be Health.

Mr. GUTHRIE. First it will be Health.

Mr. GRIFFITH. Mr. Guthrie of Kentucky, 5 minutes.

Mr. GUTHRIE. So thanks.

Mr. Mazanec, that leads into—and thanks for all you guys for being here today. That—the panelists.

That leads into one of my questions. So PAHPA of 2019, the Pandemic Act, included a directive for HHS to create a strategy for public health preparedness in response to address cybersecurity threats. So of that directive, I was just—my questions are, can you explain the process behind the directive? Was ASPR in charge, or did the Secretary lead the point? And what was the opportunity for interagencies across HHS and then outside groups to participate?

Dr. MAZANEC. Thank you, Congressman. So in terms of the specific reporting requirement that you mentioned from the prior PAHPA authorization, we did complete that report in coordination, as we do many of our activities in this area, with our partners across the Department. I believe we delivered that report a little over a year or so ago. Happy to work with you and your staff to make sure you have a copy.

I would note going forward, as my fellow panelists here and many on the committee have mentioned, the threat is not static, it is continuing to evolve, so that is sort of a point-in-time report that we develop. But we are continuing efforts now working, again, very closely across the Department with our key partners with CISA, the FBI, the interagency, and the sector to develop more—the most relevant and timely resources and strategies to address this threat.

Mr. GUTHRIE. OK, thanks. And did the HHS Secretary lead that, or was ASPR the leader of that, or—of that effort?

Dr. MAZANEC. ASPR is the designated SRMA lead for the Department, so we serve as sort of the quarterback role for all of these activities in partnership with the other key participants in the Department.

Mr. GUTHRIE. OK. And then also, Mr. Mazanec, according to a June 2021 GAO study, HHS information security, that ASPR led seven collaborative groups to—looked at seven collaborative groups to fulfill cybersecurity responsibilities that are designed to help agencies to consider when collaborating. So I'll just say the report says, and I quote, about five groups "did not have the mechanisms in place to monitor and evaluate progress. While the charters of these five groups define goals, none describe the process for monitoring and evaluating reporting progress."

How was ASPR working with these five groups specifically?

Dr. MAZANEC. Thank you, Congressman. So I believe the GAO-21-403 report that you're citing focused on the various coordinated mechanisms we had at the Department at the time. We are working through implementation of those recommendations and just recently updated the charter of the SRMA cyber working group, which, as I mentioned in my opening remarks, is that function—that coordinating entity internal to the Department that meets every week to address these issues with key participants from CMS, from FDA, our office of Chief Information Officer, with ASPR, again, in sort of that quarterbacklike role coordinating efforts.

And we're continuing to work through revisions as appropriate based on the GAO recommendations to those various groups and subgroups.

Mr. GUTHRIE. OK, thanks, appreciate that.

And now, Mr. Kumar and Mr. Travers, first with Mr. Kumar—you both would answer this. Last year I had a municipal utility that had ransomware and was shut down for 18 hours for water disruption, the utility provider was. Are there specific risk factors that utility operators in your respective sector need to prepare for, and do you provide cyber best practice for local utility providers? So if you would just go first and then Mr. Travers next, that would be great.

Mr. KUMAR. Representative, absolutely. We actually provide not only tools that the smaller utilities can use to gauge their own cyber posture and then make investment decisions to up their cyber posture, we also provide technical assistance. Currently, my office is executing a program called a Rural and Municipal Utility Grant Program that is specifically focused on providing cybersecurity, technical assistance, and funding directly to rural cooperatives

and municipal utilities across the country to really help them up their cyber posture.

Mr. GUTHRIE. Thank you. And, Mr. Travers, from EPA's perspective?

Dr. TRAVERS. Sure. Thank you, Congressman. You asked about risk factors. In terms of those smaller systems, they tend to be at higher risk than the larger systems, although all water systems certainly could be potentially victims of cyber threats. Water—small water systems generally lack capacity of larger water systems, for example. You can expect a larger water system, for example, to have an entire IT department, whereas for smaller water systems, they are much more constrained in terms of their resources.

Because, however, small systems are critical to sustaining the public health of their communities, EPA has provided very extensive and robust tools, training, direct technical assistance to smaller water systems. And I'll just give you one example. We had a technical assistance provider effort whereby EPA sends out a cybersecurity expert to assess the cybersecurity gaps at small water systems and to develop risk mitigation plans so that those smaller systems can address those gaps.

Mr. GUTHRIE. Thank you, I appreciate your answers.

My time's expired, and I yield back.

Mr. GRIFFITH. The gentleman yields back. I now recognize the gentlelady from Colorado, Ms. DeGette, for her 5 minutes of questioning.

Ms. DEGETTE. Thank you very much.

Well, these questions sort of piggyback on what the previous Member was asking about, because I want to talk a little bit about the experience and technical expertise of the DOE employees in protecting the energy grid. And in particular, I was—when I was preparing for this hearing, I learned that DOE has established the Energy Threat Analysis Center, or ETAC, pilot at the National Renewable Energy Lab, which is just outside my congressional district and is a great source of pride for everybody in Colorado and for a lot of us on this committee.

What ETAC is doing is it's helping to increase collaboration with the industry and between Federal agencies to detect, prevent, and respond to threats to the energy sector, including cybersecurity threats. So, Mr. Kumar, I wanted to ask you, how has the ETAC pilot allowed DOE to leverage its relationships and expertise to protect the energy sector, particularly from emerging cyber threats, and how is that pilot going?

Mr. KUMAR. Representative DeGette, thank you for that question. And the National Renewable Laboratory has been a tremendous leader in helping us stand up this pilot effort that we're undertaking.

Really the ETAC is meant to connect dots. Right now from a cyber perspective, what's happening is individual companies are seeing cyber threats on their individual networks, we're seeing cyber threats to the intelligence community, but we're not putting the pieces together to really understand what is the risk to our national security and what's the larger trends that are happening in

the sector, and we need to be doing that if we're going to stay ahead of the threat that we're facing.

And the ETAC is really meant to do that. It's meant to not only bring the people together, subject matter experts from electric power utilities, petroleum engineers, and the Government together to really understand these threats. And this is where we're not only leveraging the expertise of the entire Department but also the national laboratories. They have tremendous analytical expertise, they have tremendous machine expertise that we can bring to analyze threats, analyze data.

We've used them for the nuclear industry for many years, and they've been tremendous assets for us. We should be doing the same on the cyber front, and so that's where we're leveraging the capabilities of those national laboratories, and we're all certainly leading a lot of the efforts, but we have a number of other laboratories engaged as well.

Ms. DEGETTE. And where are we at with these efforts?

Mr. KUMAR. So we have already been conducting efforts, so we're doing pilot efforts where we're already looking at threats. We've actually—during the Russia/Ukraine conflict, we had identified cyber threats, and we were able to get cyber advisories out to the entire energy sector as a result of this. We're still working through fully standing up the ETAC, and for that we would need help from Congress and others. And so we look forward to working with you on that.

Ms. DEGETTE. What's your timeline, do you think?

Mr. KUMAR. So we're already operationalizing the pilot, but to fully stand it up, we're looking at doing that in 2027. Again, that will require both resources and some authorities to fully stand up the ETAC.

Ms. DEGETTE. Well, we look forward to working with you on it because it's really important that we have an integrated system like the one that ETAC is envisioning.

Just one last question for you: As Sector Risk Management Agency for the energy sector, what is DOE doing to proactively address cyber threats to the U.S. energy sector?

Mr. KUMAR. So, ma'am, we have to take a multifaceted approach to this because the threat is too great. The threats from China, Russia, and even ransomware groups nowadays. And so we really think they fall into three big buckets. One, we need to think about policies. What are the policies—not only do we need to think about policies at a national level but also standards, and so what are some of those policies we need to be implementing to stay ahead of the threat?

The second thing is we need to look at all the training and technical assistance that we can provide to the sector, exercising for cyber events.

And third, and probably one of the most important pieces, is the partnerships. As I mentioned earlier regarding Colonial, it's those partnerships that we need to have during blue sky days that we can leverage to be able to combat these threats when we see them on our networks and when they impact the delivery of energy supply across the country.

Ms. DEGETTE. Great, thank you.

Thank you, I yield back.

Mr. GRIFFITH. The gentlelady yields back. And now I recognize the subcommittee chair of Energy, Mr. Duncan, for his 5 minutes of questioning.

Mr. DUNCAN. Thank you. Thank you for mentioning Energy twice. I'm going to focus on that a little bit here.

The prior administration, Mr. Kumar, issued Executive Order EO 13920 entitled "Securing the United States Bulk Power System." This Executive order implemented critical steps to ensure equipment of the bulk power system was not susceptible to foreign cyber intrusion. The Biden administration suspended this order on day one and since then has taken little or no action to ensure our bulk power system is not susceptible to cyber intrusion from hostile foreign adversaries like China, Russia through critical grid equipment like transformers, capacitors, and electrical relays.

As chairman of the Subcommittee on Energy, protecting our critical energy infrastructure from cyber threats remains a top priority, and I'm extremely concerned that the suspension of this Executive order unnecessarily jeopardizes the integrity of our electrical power system.

What was the rationale for essentially revoking the order?

Mr. KUMAR. Representative, thank you for your question, and thanks for recognizing the importance of supply chain security. That's exactly what that Executive order was focused on, is how do we ensure that our manufacturers and suppliers, and who are they, how are they providing all this critical equipment, and how do we ensure it's secure?

So one of the reasons—this remains a priority for us. We took a step back to take a holistic approach. In that Executive order, we ran into a number of implementation challenges. Also we felt like it didn't truly address the threat we were facing from adversarial nation states out there like China.

And so what we've done is we've taken a step back to review policies, review testing. So my office conducts cyber testing of critical components from all over the sector. But how do we really take a methodical approach to address the threat we are seeing from manufacturers, from places where we don't think we should be looking at infrastructure? So we're working on a lot of those efforts behind the scenes, but supply chain security still remains a top priority for us.

Mr. DUNCAN. So just as a sidebar, a contract was issued as we build out infrastructure to a European country, I believe, that is working to do this work, and infrastructure requirements are about 60,000 capacitors—HVDC capacitors, right? This European company is sourcing those capacitors from Siemens in Germany and an Italian company.

So you talk about onshore and domestic supply, we have a capacitor manufacturer in the United States that does the same thing, but yet this company is sourcing from Europe. And if Europe is continuing to build out their infrastructure, they may decide, "There's not enough capacitors for the U.S., we're going to use them here," and then this company is left shortchanged.

So how do you address that? How do you address future contracts for infrastructure buildout when you're talking about domestic supply chain?

Mr. KUMAR. Representative, so domestic manufacturing is absolutely something we should be prioritizing. It not only is—

Mr. DUNCAN. Why aren't you?

Mr. KUMAR. So that is definitely a priority for the Secretary.

Mr. DUNCAN. Then why issue a contract to a company that's sourcing their capacitors from Europe?

Mr. KUMAR. Representative, I don't know the specifics of that incident, but I'm happy to look into it and get back with you.

Mr. DUNCAN. Yes, please do. The Biden administration set a goal of a carbon-free power sector by 2035. This on top of the numerous tax credits for solar and wind, leading to a massive buildout of renewable generating resources on the grid, I have serious concerns with the cyber vulnerabilities of renewable because of the digital connectivity to manage those systems, whether it's moving the solar panels or coordinating wind. They are more susceptible to cyber attacks. So what is the DOE doing to ensure cybersecurity is built into these devices rather than trying to solve the vulnerabilities after an attack?

Mr. KUMAR. Representative, that's an excellent question, and it's exactly what we need to be doing. So we released a strategy last year called Cyber Informed Engineering, and one of the big focus areas for us at the Department and my office in CESER is to partner with a lot of the renewable energy community to build cybersecurity in.

We actually have an opportunity unlike any other before. We have been bolting on cybersecurity. We now have an opportunity to say, much like we require safety in our products, we should require cybersecurity. And so that is something we're working with standards organizations, with the manufacturers themselves, and the developers out there to build in cybersecurity. So that is absolutely a priority, and I appreciate you recognizing it.

Mr. DUNCAN. In light of emerging technologies like artificial intelligence, what are the departments, all of you, doing to stay ahead of this evolving cyber threat with—from AI?

Mr. KUMAR. Representative, AI and other emerging threats such as quantum are things we need to keep an eye out for, and we need to ensure that we're building it. And so from our end, DOE, my office also has a cyber R&D program, and we prioritize some of our R&D work to look at quantum-resistant technologies but also how do we get ahead of that AI threat, so that's really important.

Mr. DUNCAN. But you're also using cyber learning. You said a minute ago—machine learning, rather. That seems like it's counterproductive, using machine learning to target AI.

Mr. KUMAR. Representative, we—

Mr. DUNCAN. Is it not teaching itself?

Mr. KUMAR. We—so we need to take a—we need to use all these technologies. We not only need to look at how does—machine learning can be used against us, but how can we use machine learning to protect ourselves as well.

Mr. DUNCAN. Yes. Thank you. My time's expired. I appreciate the answers.

Mr. GRIFFITH. I thank the gentleman for his questions. He yields back. I now recognize the gentlelady from Illinois, Ms. Schakowsky, for her 5 minutes of questioning.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, and thank you to our witnesses today.

Dr. Mazanec, you mentioned in your testimony that ransomware attacks have tripled in the last several years, and these attacks have exposed, I understand, nearly 42 million pieces of personal information that health—people who ask for healthcare and have been exposed. In Illinois, cyber attacks have also been a real problem, and, in fact, we had one of our hospitals close because—in—it was the St. Margaret Health in Peru, Illinois, a fairly small town, small area, which I'm sure really suffered because of the closing of that hospital.

So I wanted to ask you, how is the Department of Health and Human Services helping hospitals and various other kind of health facilities to better prepare themselves and prevent where they can these kinds of cyber attacks?

Dr. MAZANEC. Thank you, Congresswoman, for the question. And as I mentioned in my opening statement, we are taking a number of steps to address the threat. And the threat is not static, the sector is evolving. There was a mention of AI. That's—AI is a capability that's being integrated into the public health system in the future, and likely that's going to increase, and that's going to increase the surface space. So the threat is evolving. We need to elevate our game as well in how we address it.

As I mentioned in my opening statement, we do that in a number of key ways. One is developing resources, and those are resources that are tailored and can be used to—by various aspects of the sector to harden their infrastructure with the top 10 best practices, for example, that are tailored to the healthcare public health sector, they're identified in the HICP, the Health Industry Cybersecurity Practices Guide that we put out. We will then—we provide that to the sector, then we facilitate coordination with the sector to raise awareness of these resources to help better understand their needs so we can develop new resources to meet them.

And then we also track incidents as they occur. I don't have the specifics of the St. Margaret Health incident in front of me, but those are the kind of things that we do monitor when they occur—assist working with our interagency partners as we can from an incident response perspective—and that's something we're looking to do more of in the future as well.

Ms. SCHAKOWSKY. Well, let me ask you about data collection. Do you have any estimate over time how many hospitals or healthcare centers actually have closed in part at least because of cyber attacks?

Dr. MAZANEC. That's a complicated and nuanced question, an excellent question. A number of industry groups and others have reported figures associated with the number of attacks. I've seen around 14, 15 hundred attacks a week of various flavors in the sector, so it's a pervasive and growing threat. It's important for us as we, sort of, as the Sector Risk Management Agency to understand those challenges, understand how the threat's evolving, how the sector's evolving.

So one of the key efforts that we have underway, we recently completed the Hospital Cyber Resiliency Initiative Landscape Analysis, which was essentially a case study collecting some actual data and evidence to understand what practices are in place in some of these hospitals, what's the threat they face, how can we best support them. We have some other efforts that are underway now to continue to collect evidence like that to better understand the threat going forward.

Ms. SCHAKOWSKY. And once you have that evidence, what kind of work does HHS do in terms of transferring best practices for these healthcare institutions?

Dr. MAZANEC. Absolutely. So I mentioned HICP already. That's kind of a marquee product that we put out in partnership with the sector and working with the sector directly. They played a key role in developing that resource as well.

Another resource we put out recently was the Healthcare Public Health Sector Cybersecurity Framework, which takes the best practices that NIST puts out in general for cybersecurity and maps them to and explains how to apply them in the context of healthcare and public health. So those are two key resources we put out, but we also go out to the sector, are available, can provide technical expertise if there are questions on how to implement these, and we look to develop additional guidance and resources going forward as well as we—

Ms. SCHAKOWSKY. And, finally, let me just ask you, what is HHS doing in terms of also partnering with the public sector to minimize these kinds of attacks?

Dr. MAZANEC. Thank you, Congresswoman. That's, again, a great question. This is a key partnership. That's been a theme I think today in the questions, but it is a partnership both within HHS, with the interagency, and with the sector directly.

We work very closely through a number of venues with the Health Sector Coordinating Council Joint Cybersecurity Working Group. They have biweekly meetings that we participate in. Those are representatives from across the sector, different types of hospital systems, and we really in that venue hear what their concerns are, hear their feedback on what they're looking for from us, we provide resources. And there's a number of other groups like that that we facilitate.

That's a key part of ASPR's role as the SRMA lead within the Department, is managing that entire process. But it's a critical partnership for us. We cannot do this just on the government side.

Ms. SCHAKOWSKY. Thank you so much.

And with that, I yield back my time.

Mr. GRIFFITH. Thank you, gentlelady, for yielding back. I now recognize the gentlelady from Arizona, the vice chair of the subcommittee, for her 5 minutes of questioning.

Mrs. LESKO. Thank you, Mr. Chair. Let me get out my questions.

My first questions are for Mr. Kumar. Mr. Kumar, the Biden administration, in my opinion, has sought to limit and eventually eliminate the use of coal, oil, and natural gas as fuel. However, many Americans still rely on these resources to heat and power their homes. Has the Biden administration's push to shift to more renewables caused CESER to focus more of its cybersecurity efforts

on incorporating renewable resources into the grid, and will the Department subsequently be investing less resources in securing infrastructure utilizing coal, oil, and natural gas?

Mr. KUMAR. Representative, thank you for the question. CESER looks at all forms of generation, electric—we—whether it's nuclear, whether it's coal. My office is really focused on ensuring regardless of generation source, we are ensuring the security of it. And so to that end, we not only partner on the electricity side with some of the clean energy community because we want to make sure that it is secure, but we also colead an entire group focused on the oil and natural gas industry, on security, and resilience. So there shouldn't be a difference in us working with the oil and natural gas industry or the coal industry.

But, yes, we also need to be focused in on these new sources of generation so we can build cybersecurity into them as well.

Mrs. LESKO. Yes, I was just trying to determine if, because there's more of them, right, I would assume more companies that you're dealing with, if you have to have—if you have a limited amount of resources, and if you're able to cover them all.

Mr. KUMAR. Certainly I would say not only is the fact that we have new market players such as the clean energy community, but the reality is we also have more digitization in the sector, so we do need to do more in general to get ahead of this threat. And then, of course, we're seeing an increased threat. So all of these things we have to stay on top of, and certainly we appreciate Congress and the White House's continued support of our budget request to stay ahead of these threats, ma'am.

Mrs. LESKO. Thank you. I have another question for you, Mr. Kumar. According to BlackBerry's most recent Global Threat Intelligence Report, which I have right here, the U.S. electric and gas industries have been targeted by cyber attacks in the last 6 months, including by Russia-linked malware attempting to compromise energy-sector industrial control systems, an escalation from attacks on business IT systems to include operational technology. Russia has physically and digitally degraded nearly half of Ukraine's power infrastructure.

What is DOE, as Sector Risk Management Agency for the energy sector, doing to proactively address cyber threats to the U.S. energy sector?

Mr. KUMAR. Representative, as you alluded to, the cyber threat is increasing, and it's not just on our business and email networks, it's focused on our operational networks that control our power grid, our pipelines across the country, and that is where we're seeing cyber adversaries focus their efforts. And so we as a department have had to shift where we focus as well, and so the approach that we are taking in CESER is what we call a threat-informed approach.

So where is the adversary headed, where is the threat headed? That's where we want to prioritize our efforts, our resources so that we can stay ahead of that threat, and so that's been our focus is, to really conduct hands-on training to show how a cyber event could impact a pipeline or electric operations. And so we're taking what we learn of those cyber threats that you're alluding to and baking them into everything that we do as a department.

Mrs. LESKO. Good. Mr. Mazanec, did the cybersecurity risks and cyber attacks increase during the height of the COVID pandemic?

Dr. MAZANEC. Thank you, Vice Chair Lesko, it's an excellent question. So the COVID pandemic absolutely heightened the threats that we saw to the sector. The system was stressed generally, separate from just the cyber threats that were present. And, of course, as I mentioned in my opening remarks and I think is widely recognized, cybersecurity is a—generally an underfunded research in healthcare—or resource in healthcare and public health.

So it was already stretched thin, and the pandemic exacerbated that. So we did see an increase. We're seeing year over year even as we end the public health emergency and leave the pandemic, the threat is continuing to grow, and we—certainly that was the case during the pandemic as well.

Mrs. LESKO. Thank you, and I yield back.

Mr. GRIFFITH. The gentlelady yields back. I now recognize the gentleman from California, Dr. Ruiz, for his 5 minutes of questions.

Mr. RUIZ. Hey, thank you, Mr. Chairman.

As it's been mentioned, cybersecurity is among one of the most pressing national security issues that our country is facing. Cyber attacks are on the rise and on pace to shatter record-setting numbers. In the last 5 years alone, the College of the Desert in my district, the Imperial Community College in my district, and the Imperial County, an office that is responsible for critical infrastructure in my district, were hit with cyber attacks. The San Bernardino County was also—Sheriff's Department was also recently hit by cybersecurity attacks.

While, thankfully, no critical infrastructure was damaged in those specific cases, we continue to be concerned about future attacks. One area of specific concern is the vulnerability of our water systems. As a district that is currently struggling with getting access to clean water, any attacks on our water systems would be catastrophic. The reason for this is that breaches in the cybersecurity of a water system can compromise the safety and quality of water supplies as attackers may tamper with treatment processes or introduce harmful substances posing significant health risks.

And living in the desert with 116 degrees, the lack of water or undrinkable water is an emergency, OK. Unfortunately, smaller water systems that serve some of the country's most vulnerable populations, like those in my district, often lack the resources to help them prepare for and mitigate the impacts of water system disruptions, including those caused by cyber attacks.

So, Dr. Travers, can you provide examples how the EPA has helped smaller and underresourced water systems to identify their unique system risks and take steps to mitigate them?

Dr. TRAVERS. Thank you for your question, Congressman Ruiz. The security of small systems is an essential component of our Homeland Security mission. As you cited, these systems, though small, are critical to the viability of the communities they serve, whether they're in a desert community or not. EPA has provided extensive assistance to smaller systems.

I cited earlier, for instance, an effort that we had underway targeted specifically towards smaller and disadvantaged systems, whereby we would dispatch subject matter experts in cybersecurity

to smaller water systems to assess the cybersecurity practices at those communities and to recommend basic cybersecurity measures that they could enact to close those cybersecurity gaps. And these are not resource-intensive steps that they can take, these are steps more related to process like having strong, unique passwords. It's very basic.

Mr. RUIZ. Yes, thank you.

Dr. TRAVERS. Yes.

Mr. RUIZ. Thank you. A robust, well-trained workforce is essential to preparing for and responding to cyber attacks on critical infrastructure, and yet we currently are experiencing a cybersecurity workforce shortage of 700,000 individuals. Cal State University San Bernardino has one of the largest, aside from the Government, of training in cybersecurity experts.

Dr. Travers, how does the EPA plan to address this cybersecurity workforce shortage at a pace that will meet this rapidly growing problem?

Dr. TRAVERS. Thank you for the question, Congressman. EPA, in addition to the assistance that I mentioned earlier, we also provide extensive training to actual circuit riders and train the trainer-type programs, whereby we work closely, for example with the National Water Association, USDA, the Rural Community Assistance Program so that those individuals, who often are a source of technical expertise to smaller systems, have the ability to provide critical assistance on cybersecurity—

Mr. RUIZ. Great.

Dr. TRAVERS [continuing]. To those smaller systems to compensate for that lack of workforce.

Mr. RUIZ. Can I suggest you partner with universities like Cal State San Bernardino—Cal State University San Bernardino to outreach into local communities? Because one of the issues is that we need the workforce also in these smaller, rural areas. And so how are you working to increase the effectiveness of the smaller water systems to increase their expertise and cybersecurity experts and workforce?

Dr. TRAVERS. Yes, thank you, Congressman. We are happy to work with literally any entity that can help us access smaller water systems and to lend assistance to communities who are in need of our assistance, so we are happy to partner with local universities, with States, local community groups to provide assistance.

Mr. RUIZ. Thank you, yield back.

Mrs. LESKO [presiding]. Thank you. And now I recognize the Chair of the Energy and Commerce Committee, Representative Cathy McMorris Rodgers.

Mrs. RODGERS. Thank you, Madam Chair.

The Executive Office of the President released his National Cybersecurity Strategy in March. Include—it includes five pillars, including Pillar 1 on defending critical infrastructure. And I know, Director Kumar, you referenced this in your written testimony, you mentioned the National Strategy.

I just wanted to ask each one of you to speak a little bit more about your agency's role in developing this National Strategy, what your involvement was, what additional actions you think your

agency should be taking, feedback on the strategy, working with the private sector as a place to start.

So, Mr. Kumar, if you would start, that would be great.

Mr. KUMAR. Thank you so much, Chairwoman. The National Cyber Strategy really was bringing together an entire government to say what are our gaps in cybersecurity as a country, what do we need to be doing to address them? CESER represented the Department of Energy as part of the senior steering committee to help develop the report. We helped advise the White House on areas where we think we need to be doing more.

And so to that end, there are a couple of areas where we identified, and thankfully they made their way into the strategy. And so the first was we need to be—we need operational collaboration between industry and government on cyber. We all can't go at it alone. We need to be partnering more closely, we need to shift how we look at cyber threats, we need to be sitting shoulder to shoulder with operators of the electric grid, with the intelligence community. And so to that end, the Energy Threat Analysis Center pilot that we are piloting right now was included.

The second area of focus we suggested was, as we see new renewable energy and other energy sources connecting into the grid, we absolutely have to ensure the cybersecurity of those systems. And so, again, that was also referenced. And we'll be leading an effort to bring together the clean energy community with cybersecurity experts to build cybersecurity into it.

And last but not least, an area where we think there needs to be a tremendous amount of focus is a concept we call cyber-informed engineering. We have to develop cybersecurity into these systems, whether it's large pieces of transformers or whether it is solar panels or anything else, cyber just has to be a part of it. So that end, this national cyber-informed engineering strategy needs to be developed, and we need to do more to work with standards, orgs, manufacturers, suppliers, and everyone to do more in this space.

And so overall, we got a tremendous amount of support, and we're very—it was a very collaborative process.

Mrs. RODGERS. Thank you.

Dr. MAZANEC. Thank you very much for the question. So HHS, similar to the Department of Energy, participated in the inter-agency process that developed the National Cyber Strategy. In terms of the benefits for us going forward and how we're using that strategy, I would say first of all, it's very helpful in that it provides a common lexicon that we can use as we engage in that critical collaboration with our partners to talk about the threat, talk about and frame what we're doing.

It also directed the development of an implementation plan that is currently in development, and that provides a venue for us, along with others in the interagency, to participate and try to use that framework to enhance how we collaborate and work together as a team across the Government.

The last piece I would note as well is the strategy indicated a move towards minimum mandatory standards. That's something for the healthcare and public health sector, as I mentioned in some of my comments, is really complicated and challenging. It's a very

diverse and complicated sector but something that we have heard from our industry partners that they are interested in.

I mentioned earlier some of the resources we put out that provide guidance, voluntary standards, if you will, that they could adopt. But the National Cyber Strategy provides a framework for us to continue to explore in a very thoughtful and evidence-based way how to develop minimum mandatory standards for the sector, if appropriate.

Mrs. RODGERS. And would you—I'm going to keep going, but would you also speak to what kind of feedback we've gotten from the private sector?

Dr. MAZANEC. So from the healthcare public health perspective, the feedback thus far has been very positive. I mentioned the venues we coordinate in. We got very positive feedback from the strategy.

Mrs. RODGERS. OK, good. Thank you.

Mr. Travers?

Dr. TRAVERS. Thank you for the question. So I personally participated in the interagency work group that was responsible for developing the Cybersecurity Strategy. I certainly felt that it was a very collaborative process, felt as the other panelists have expressed, our voices were heard, and that EPA was able to advocate for the sorts of concerns and issues that confront the water sector.

Certainly we appreciated the strategy as it underscored the importance of partnerships with the private sector, working with them to leverage their expertise and experience in providing products, and also leveraging our existing resources so that we don't duplicate efforts. So that—Dr. Mazanec mentioned standards so that we don't all go off in separate directions, developing standards that don't have consistency and aren't based on a fairly uniform approach.

And then, finally, the—we appreciated the fact that the document emphasizes the importance of the sector risk management role, as Sector Risk Management Agencies have a unique understanding of our respective sectors.

Mrs. RODGERS. Thank you.

Dr. TRAVERS. So we were pleased to see that reflected in the document as well.

Mrs. RODGERS. Thank you. Good. I'm pleased to hear that too. Thank you all for being here.

I yield back.

Mrs. LESKO. Thank you. I'd like to recognize Representative Tonko from New York for 5 minutes of questioning.

Mr. TONKO. Thank you, Madam Chair, and thank you to our panelists and to—for being here and for your leadership.

As past chair and now ranking member of the Environment Subcommittee, ensuring that all Americans have easy access to safe drinking water has been a long-time priority. Our community drinking water and wastewater systems provide a critical service for the American public. The resilience of these systems in the face of cybersecurity threats is key to ensuring that everyone has clean water.

As the Sector Risk Management Agency for water systems, EPA is able to draw on extensive relationships and water system exper-

tise to support cybersecurity efforts. That's why this committee has a long history of working together on a bipartisan basis to support EPA's cybersecurity efforts. In 2018, this committee further enhanced EPA's ability to work with water systems to improve their resiliency. The bipartisan America's Water Infrastructure Act, or AWIA, gives EPA important authorities and tools that can help water systems identify risks and plan for emergencies, including those cyber attacks.

So, Dr. Travers, how is EPA using the tools provided by Congress in the bipartisan AWIA effort to enhance EPA cybersecurity efforts and better partner with water systems?

Dr. TRAVERS. Thank you for the question, Congressman. AWIA, as you rightly cited, represents certainly a statute of foundational importance to the Water Sector. It required community water systems serving more than 300 people—3,300 people, excuse me, to prepare risk assessments and emergency response plans, which is a critical first step in enhancing the resilience and security of these water systems.

So in response to that congressional mandate, EPA developed a suite of tools and training and technical assistance, all of which I will note we completed within about 8 months, given the very aggressive timeframe within the statute. As a result of our efforts, as a result of the partnership that we enjoy with our sector, we have seen excellent compliance rates with AWIA. That was, of course, the important policy outcome we wanted to see. About a hundred percent of large and medium systems have complied with the provisions of AWIA, and about 96 percent of small systems have complied with the provisions. So I think it is an excellent use story, and I think AWIA, as I said, imparted a critical impetus and policy directive to the water sector that the sector took seriously.

Mr. TONKO. Thank you, I appreciate that. And while cybersecurity threats won't go away, there are steps water systems can take to improve their chances of deterring and detecting attacks before they impact public safety. Cyber threats are constantly evolving and require vigilance and forward-looking plans. This is especially true for the cybersecurity of critical water systems that we depend upon for drinking water.

So, Dr. Travers, again, how does EPA work with other Federal agencies to develop best practices for cybersecurity infrastructure, and what sector-specific adaptations are needed when translating and communicating these strategies to apply to water systems?

Dr. TRAVERS. Thank you for the question, Congressman. EPA has worked extensively with our interagency partners in developing best cybersecurity practices for the water sector. What we have noted is that many water systems within the sector have neglected to adopt basic cybersecurity strategies, and so our efforts have focused on underscoring that the adoption of very kind of rudimentary practices can be astonishingly effective in mitigating the risk of cybersecurity.

So, for example, you asked about how we adapt cybersecurity practices for the water sector. We have provided a checklist, again, as a result of the AWIA requirements for water systems, so—which is readily accessible to water systems which may have limited technical capacity in dealing with cybersecurity, so we present it in a

form that is a distilled version of a much larger standard developed by NIST, and we conducted extensive training and exercises based on those practices. We have also actually conducted assessments at utilities themselves leveraging those standard.

And I will say on a final note that we have leveraged CISA's cross-sector performance goals in developing our basic checklist of cybersecurity practices, again, to ensure consistency across the Federal Government.

Mr. TONKO. Well, thank you. I would say that, based on the bipartisanism of AWIA, I hope we can continue to effectively respond to those cybersecurity threats.

And with that, Madam Chair, I yield back. Thank you.

Mrs. LESKO. Thank you. And now I call on Representative Cammack from Florida for 5 minutes of questions.

Mrs. CAMMACK. Thank you, Madam Chair, and thank you to our witnesses. You're in the home stretch, so hang in there.

Dr. "Man-za-nec," did I get it right?

Dr. MAZANEC. Almost. "Maz-a-nec."

Mrs. CAMMACK. Mazanec, OK. Thank you. You noted in your testimony that ransomware is currently the largest threat to the healthcare and public health sector. Specifically, what can you give me in terms of examples, and I'm looking for three, that the department of Health and Human Services has planned and enacted to address the growing ransomware threat, and what you are doing to help health systems and hospitals address that growing threat.

Dr. MAZANEC. Thank you, Congresswoman, that's an excellent question. I'll highlight a couple things a little more that I already touched on, but I think one of the key ways to address the ransomware threat or any sort of malign cyber threat is through deterrence by denial, hardening the sector so it's less appealing to adversaries. There's a lot of financial incentives, other incentives that I think make it an easy target, the healthcare public health sector—making it an appealing target, I should say.

So some of the resources we have recently developed or updated and put out there are essentially resources that help harden the target and deter, hopefully, some of the ransomware actors. This is—the resources that I'm referencing are things like the HICP, the Health Industry Cybersecurity Practices Guide, which we updated not that long ago, that has 10 mitigating strategies in it. Again, not incredibly complicated, they're basic things, tools and steps that a diverse array of entities within the sector can take to harden their target, things like implementing better data protection, IT asset management, those kind of cyber hygiene practices.

We've also facilitated a lot of sector coordination, as I mentioned, through the Health Sector Coordinating Council Joint Cyber Working Group working with our industry partners and other venues. That leads to a lot of information sharing where we're working to enhance threat and intelligence sharing. That, again, I think helps combat the threat.

And then ultimately helping ensure from an incident response planning perspective that the sector and the entities have incident response plans in place. We have our plan that we recently updated within the department and that we're ready to exercise it

should an attack occur to minimize the impact on patients and patient's safety.

Mrs. CAMMACK. Thank you. Now kind of digging into some of the Internet of Things within the hospital systems. Data shows that 53 percent of connected medical devices and other Internet of Things devices in hospitals have a known critical vulnerability. Many of these devices do not have patches or compensating controls that are provided by the manufacturers.

So what is HHS doing to ensure that these vulnerabilities are remedied with validated patches and other mitigations from the manufacturers and that these solutions are made available in a timely manner—and I would like you to define what a timely manner is—by the manufacturers, but also how can this also be made available to other servicers and technicians outside of the manufacturers?

Dr. MAZANEC. Thank you for that question. And indeed, the—part of what makes the sector so complicated are the diverse array of connected, interconnected legacy devices. We—I mentioned earlier we recently completed a hospital cyber resiliency initiative landscape analysis to really dig in to an aspect of the sector and understand the threats they face. One of the things that came of that assessment was along the lines of your question, a finding that a significant number of hospitals—I think it was nearly a hundred percent within the population we looked at—had at least some devices that were not patched, were at sort of legacy end of life.

So that's something that we're aware of, we're working to address, that we provide, again, these resources that put in place a framework for each entity to use to identify where they need to update and implement patches, and we're hopeful that that will be helpful. And, of course, our colleagues within the Food and Drug Administration recently got additional authorities—enforcement authorities in the omnibus legislation for medical devices, which is not all internet-connected devices in the sector, it's a subset of it, but they are currently working through how to implement those and address that from a medical device perspective.

Mrs. CAMMACK. Well, and when you say resources and providing resources, is that more technical guidance, or is there actually a funding mechanism that goes along with that?

Dr. MAZANEC. So we do not currently directly provide funding to address this issue. We provide guidance, we provide knowledge-on-demand web-based resources in that sense that can help the expertise in the sector more efficiently and effectively address this issue. But, as I mentioned, you know, the threat is not static, it's growing. As we move forward and consider various policy options and part in collaboration working with you and your staff, one of the things, of course, we will explore is are there more things we can do along the lines of funding to address this issue.

Mrs. CAMMACK. Well, and I've got one question left, so I'm going to get to it as quickly as possible. Last 11 years, healthcare has had the highest average cost of \$10 million per breach with a record number of data breaches in 2021. What is HHS doing in order to ensure the timely reporting by manufacturers of known cybersecurity vulnerabilities on their devices? And again, define timely.

Dr. MAZANEC. So I would—if it's possible, I would like to get back to you with—and we can work with our colleagues in FDA to get a little more information from a medical device perspective, but I do want to highlight the sector as much more than just medical devices. There's a lot of additional connected devices as part of the Internet of Things.

Mrs. CAMMACK. Right.

Dr. MAZANEC. Operational technology. So I think we take a holistic approach to the risks facing the sector as the SRMA and ASPR. The cyber threats, the other threats, and certainly those connected devices exacerbate it. But we can get back to you and your staff with additional information on what FDA is doing specific to the medical devices that they have authorities over.

Mrs. CAMMACK. Perfect. I appreciate it. Thank you so much.

My time is expired, Mr. Chairman. I yield.

Mr. GRIFFITH [presiding]. The gentlelady yields back. I now recognize the gentleman from California, Mr. Peters, for his 5 minutes of questions.

Mr. PETERS. Thank you, Mr. Chairman.

I'll follow up somewhat on Mrs. Cammack's questions about healthcare. The number of ransomware attacks on health organizations more than doubled from 2016 to 2021, exposing that personal health information of nearly 42 million patients. In May 2021, a health system in my district, Scripps Health, was attacked with malware, and when—while Scripps immediately launched an investigation and took steps to contain the damage, the cyber attack still disrupted care at Scripps and resulted in a surge of patients at other healthcare facilities across the San Diego area.

Dr. Mazanec, when a cyber attack happens, how does HHS work with hospitals and State public health agencies to respond and recover?

Dr. MAZANEC. Thank you, Congressman, that's a great question. And I would note from the 2021 Scripps Health incident, that was actually the specific attack, and I referenced in my opening remarks, the JAMA, the Journal of American Medical Association study that came out just last week that look—dug into that incident and reported on what they call the blast effect to—in terms of creating significant detrimental outcomes in the surrounding area too. So it wasn't just the affected entity—

Mr. PETERS. Right.

Dr. MAZANEC [continuing]. That had adverse effects. In terms of how we respond in general, in that instance and in general to an incident, we work, first of all, very closely with our interagency partners and our other partners, ASPR within the Department of Health and Human Services, so it's a team effort in responding. We first observe—get information on the incident, and then we convene a healthcare public health risk management cyber incident response team, or an HPH cert, which is a formal entity within the Department that—with interagency participation that will determine the—how to classify the incident, how severe it is.

We're really interested in—from an SRMA perspective on impacts to patient health and safety, that's our primary focus, our—if there's a data breach, that's significant and concerning, but if it doesn't have an adverse effect on patient health and safety, that

will result in a lower sort of incident classification. But depending on how we classify the incident, that will inform our response from there in terms of do we monitor it or is there assistance we can provide.

And again, our interagency partners are key. Often it is not HHS who has direct contact with the entity, it may be the FBI, from a criminal perspective, or our colleagues at CISA.

Mr. PETERS. In terms of your—of the expertise you might provide, what is the knowledge and expertise that HHS can bring to the healthcare sector in an instance like this?

Dr. MAZANEC. So one of the great strengths of how—and I know my colleagues on the panel have noted this for their respective sectors as well, but as an SRMA, we do have, I think, a unique position and understanding of the patient impacts, health and safety. We understand the sector better than anyone else. And then we partner with law enforcement, FBI, with CISA, who bring other skills to the table to support the affected entity however, you know, we best can.

But we bring that unique vantage point from a healthcare public health perspective that I think the others don't necessarily have.

Mr. PETERS. I understand also you have promulgated or offered voluntary guidelines for organizations. Can you tell me about those, and what are you hearing from healthcare systems that have implemented the guidelines about their impact on cybersecurity?

Dr. MAZANEC. Absolutely. So we just recently provided two key resources to the sector that essentially contain voluntary best practices. The first is a resource—and both of these I should note, too, were developed in close partnership with the sector; these are not things that we developed in isolation.

The first key tool is that the Healthcare Public Health Sector Cybersecurity Framework Implementation Guide. This essentially takes the NIST best practices for cybersecurity and tailors them to the sector. It—both of these just came out a few weeks or months ago, so they're still, I think, receiving feedback, but it's been very positive.

The other key tool, and I know I've mentioned it a few times already, is the HICP, the Health Industry Cybersecurity Practices, that was developed, again, with industry and led by our HHS 405(d) Program. That contains the top 10 mitigating strategies, has sort of off-the-shelf tools that are tailored to small, medium, large hospital systems, so it's a really flexible tool with best practices.

And as we go forward, we'll be collecting data through a number of different ways as to how the sector is use—are using these, how we can revise them as appropriate going forward, again, because the threat is not static here—

Mr. PETERS. Right.

Dr. MAZANEC [continuing]. It is continuing to grow and evolve.

Mr. PETERS. Well, I mean, the health systems will always be an attractive target for cyber criminals because of the value of the data that they hold and the security and health of the nation that's behind them. I would say congratulations on an acronym like HICP, but it's more than a hiccup in this case, so I appreciate your good work, and thank you again for being with us today.

And, Mr. Chairman, I yield back.

Mr. GRIFFITH. The gentleman yields back. I now recognize the gentleman from Alabama, Mr. Palmer, for 5 minutes of questioning.

Mr. PALMER. Thank you, Mr. Chairman. Thank you for holding the hearing, and thank you to the witnesses for appearing.

I might be wrong, but I think the first time that most Americans experienced a cyber attack against our energy infrastructure was the attack on the Colonial Pipelines, and they might not have realized it as they were sitting in long gas lines trying to put gas in their cars.

What I want to ask you is when—Mr. Kumar, when the Department engages in efforts to facilitate coordination between the electric and gas subsectors, or I guess any part of our energy infrastructure, to guard against and respond to cyber attacks, is there a thorough evaluation of the adequacy of the firewalls that these companies and other entities are using to protect our critical energy infrastructure?

Mr. KUMAR. Representative, thank you for the question. And the Colonial Pipeline incident, you're absolutely right, was a wakeup call for a lot of Americans and a lot of critical infrastructure owners and operators themselves that, you know, we need to do more, we need to really ensure that we have certain cyber baselines in place.

Mr. PALMER. I've got several questions, but what I'm really asking is, some of the energy infrastructure is obviously privately held, very—some of it is—like TBAs, Federal. When you're looking at trying to protect against these, are you evaluating across the board, whether it's privately on company or a government company, their firewalls, they're building to harden in their systems?

Mr. KUMAR. Representative, when it's a privately owned company, they usually have to invite us in to be able to do that type of assessment. We do offer assessments of those companies should they choose to take us up on those, so we definitely offer them. But again, it does determine if the private sector—

Now on the electricity side, there are—there's a regulatory regime where there is enforcement, and they do have to validate that they are meeting certain cyber requirements.

Mr. PALMER. Along the same line, you note in your written testimony that CESER facilitates both the Electric Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council, and I just wonder if these two entities ever interact to examine shared threats, and it's all on the same lines of what I led into this with, the shared threats with opportunities to collaborate to address them.

And one of the things that I'm particularly interested in is modeling, or what some people would call war gaming, to prepare in advance for these. And this happened—in my district we have the National Computer Forensics Institute, and they've done some of this, particularly in regard to responding to ransomware attacks. And I just wonder if the Department of Energy is doing anything to facilitate that type of activity to model these potential attacks.

Mr. KUMAR. Representative, thank you for that question. And absolutely. And we have to make sure we're looking at the entire energy sector. So we conduct cyber exercises, and when we conduct

them we include both electricity and oil and natural gas companies, and our scenarios include the interdependencies between the sectors but also what kind of modeling capabilities can we leverage from national laboratories and other resources to understand how a specific cyber threat could actually impact Americans across the country. And so that's absolutely a core component of what we are doing.

Mr. PALMER. Now this actually applies across the board to the other agencies involved in this hearing, whether it's a school system, hospital, or what have you. And I think it's very important that we do that and we emphasize that.

The other thing is, in the role of the national labs in trying to identify threats to the electric grid—and not just the electric grid but the critical infrastructure across the board—is there any evaluation of the risk of—in terms of the interconnectivity of everything, interfacing with systems that utilize technology that was designed, installed and manufactured and maintained by China? I mean, we tend to think that we have these boundaries that protect us, but when it comes to interconnectivity, I mean, even right down to fiber, we're connected.

And that—all three of you, if you'd like, can respond to that. But I think it's one of the critical questions that we need to answer.

Mr. KUMAR. Representative, what we're looking at is taking a threat-informed picture, and the reality is, one of the biggest threats we have is the threat from China, particularly when it comes to cyber capabilities. And so, as we do some of our testing—for example, we will test critical components for cyber vulnerabilities. When we do some of that work, we will—that is informed by the threat we are seeing, and that informs all of our work in our office.

Mr. PALMER. Mr. Mazanec?

Dr. MAZANEC. And, yes, I would from the HHS perspective and for the healthcare public health sector, the supply chain and the interdependencies are very significant. We focus on it holistically as well. And they're going to only increase as there are more and more connected and network devices in the medical system.

Mr. PALMER. Mr. Travers, do you have anything to add to that?

Dr. TRAVERS. Yes, thank you, Congressman. Supply chain and third-party availability of cyber tools form a critical part of our checklist that we provide to both drinking water and wastewater systems, so it is a core part of the messaging and training that we provide to the water sector.

Mr. PALMER. Well, I thank the witnesses.

I thank the chairman, and I yield back.

Mr. GRIFFITH. The gentleman yields back. I now recognize the gentleman from Texas, Mr. Crenshaw, for his 5 minutes of questioning.

Mr. CRENSHAW. Thank you, Mr. Chairman, and thank you all for being here.

I want to focus on our hospitals. So for you, Mr. Mazanec, you know, one simple question I have is, who at HHS is our private sector supposed to work with in the event of a cyber attack?

Dr. MAZANEC. Thank you, Congressman. So HHS brings a lot to the table in our SRMA responsibilities here working with the sec-

tor, but in terms of the lead coordinating entity, it is ASPR, the Administration for Strategic Preparedness and Response, that is sort of the central quarterbacking function within the Department.

That being said, though, if anyone reaches out, as I mentioned in my opening statement, we have a weekly meeting with all the key entities across the Department. If anyone is unsure of who to contact, if—and that's something we're looking to, you know, simplify and clarify for the sector, but if they reach out to any part of HHS, we are coordinating closely and will make sure we get them connected to who they need to be connected with to address the issue.

Mr. CRENSHAW. All right. I didn't even have that on my list, I mean, because we got Chief Information Officer—if we go to your website—staff trying to research this before I asked it, and that wasn't even on my list. We got a Health Sector Cybersecurity Coordination Center. What is that?

Dr. MAZANEC. So the Health Sector Cybersecurity Coordination Center, which we call HC3, is within the Office of the Chief Information Officer. It is a key repository of technical expertise and coordinates on—and puts out information to the sector tailored to it from a threat perspective. Again, there are key participants and partners with us with ASPR playing that coordinating—

Mr. CRENSHAW. But a hospital needs a 1-800 ber attack number. Do they have that number?

Dr. MAZANEC. So if they reached out to HC3, they would get—

Mr. CRENSHAW. How would they reach out to HC3, like do they go to your website, like how do they know?

Dr. MAZANEC. They have a web presence. We have the 405(d) Program, which is another program established by Congress that engages a lot with the sector, has a very, I think, comprehensive web presence that is faced into the sector.

But your question also indicates the importance of clarifying these—who they need to reach out to and engaging the sector. That's why some of these venues that I've mentioned previously, the Health Sector Coordinating Council Joint Cybersecurity Working Group—

Mr. CRENSHAW. Yes.

Dr. MAZANEC [continuing]. Is so important that we're engaging and touching the sector proactively so that we're not just waiting for them to reach out.

Mr. CRENSHAW. It's extremely important, that's why—and, you know, for emergencies we have a very simple number to call, 9-1-1, right? It should be the same for this if your job is to help them.

Another issue that they—that concern—that hospitals report is that regulators that they report to also have the ability to penalize them for reporting cyber attacks. You know, they can get—they can turn around and get fined after they ask for help because of the possibility that private data was released, et cetera. So how do you resolve that?

Dr. MAZANEC. So I think—I mean, that is a concern. We're—we've heard and one of the—I think what they're referencing is the HIPAA security rule.

Mr. CRENSHAW. Yes.

Dr. MAZANEC. Which is actually an incentive for the adoption of some of the best practices and resources we put out there. A covered entity under HIPAA—which, I should note, is not the entire sector, it's a subset of the sector that are covered by HIPAA—if they have a data breach and they can demonstrate that over the preceding 12 months they had implemented and taken due diligence to implement voluntarily some cyber hygiene best practices like the HICP that we put out or the cybersecurity framework, then that will have a mitigating effect on whatever penalty they might be subject to. So, in fact,——

Mr. CRENSHAW. Yes, but——

Dr. MAZANEC [continuing]. That regulatory role actually incentivizes the adoption of some of the best practices.

Mr. CRENSHAW. Ideally, but in another—but it's also easy to imagine a different scenario wherein they didn't get around to it yet because they're busy, I don't know, doing hospital stuff, and so now they won't report these cyber attacks to you, and you can't add that to your database. You can't add these new attacks to your best practices, you can't help the people who were designed—you're designed to help because they're like, "Well, I'm not going to report anything to you, I'll get fined." That's a problem that should be fixed.

OK, so two problems that need to be fixed.

Mr. Kumar, the deal you announced last year, that they're putting \$45 million into improving the security of American energy, in particular tools to protect the power grid, if you could just provide a quick update on what solutions have come out of this. It's—again, it's very vague statements on the website. We can't find much information on what the plan is.

Mr. KUMAR. Representative, when we put out these funding announcements, what we do is we target them to threats. So what we do is we take intel to say, "Here are the priority areas for the research that we would like folks to actually submit their applications to." So we're looking at things like how do new communications pathways create cyber risks, how do new emerging technologies such as AI and quantum could potentially impact the sector and therefore we need to develop tools and technologies to defend against them?

So, again, all of our focus areas are mentioned in our funding announcements so that when someone submits it—and it could be an industry company, it could be academia, it could be a national laboratory, it could be universities as well to say that they are going to submit for funding requests for that. And that's where the 45 million is focused on, and we're——

Mr. CRENSHAW. It's a grant program——

Mr. KUMAR. It's a grant program, yes, sir.

Mr. CRENSHAW [continuing]. For cyber defense companies to create the tools—OK.

Mr. KUMAR. Absolutely, sir.

Mr. CRENSHAW. Got it. And I'm out of time. Thank you.

I yield back.

Mr. GRIFFITH. The gentleman yields back. We now recognize Ms. Kelly of Illinois for her 5 minutes of questioning.

Ms. KELLY. Thank you, Chair Griffith and Ranking Member Castor, for holding this important hearing this afternoon, and I want to thank our witnesses for their testimony.

Mr. Mazanec, thank you for your testimony today. In your written testimony, you discuss how growing attacks from more aggressive adversaries are growing well beyond data breaches, now affecting timely access to patient care. For years, the health disparities for Black Americans and other minorities have been well documented, and a study by Pew Research Center revealed that a major reason attributing to these health inequities stems from less access to quality care.

So how do these cyber attacks directed at healthcare and public health critical infrastructure exacerbate health inequities among minority populations and among rural populations?

Dr. MAZANEC. Thank you, Congresswoman, that's an excellent question. I think one of the challenges, again, facing us and facing the healthcare public health sector is the incredible diversity of the sector. There are some very, very large hospital systems, and there are some very small hospitals and elements of the sector that really aren't nearly as well resourced from a cyber perspective. So one of the things we do in trying to make sure everyone is hardened across the sector is develop tailored resources that will help and make it more efficient and easy for those smaller, less resourced hospitals to bolster and harden their infrastructure.

So the HICP that I've mentioned a few times is definitely one of them. It has tailored resources that are designed for smaller hospitals that they can pick up and use. We also provide—and this is through our 405(d) Program—a knowledge-on-demand series of courses that, again, can help the sector where they maybe don't have as much resident cyber expertise to get the basics that they need and implement kind of the key mitigating strategies and basic cyber hygiene that should harden them as well.

Ms. KELLY. Yes, my district is urban, suburban, and rural. I start in Chicago and go 3 hours south, and there's less hospitals as you even go further south, and they're not the, you know, University of Chicago or Northwestern and things like that. Much smaller hospitals.

Also, I'm encouraged by HHS's recently published edition of the Health Industry Cybersecurity Practices, HICP, the Hospital Resiliency Landscape Analysis, and the Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide. How would a basic set of cybersecurity standards for all American hospitals help keep patients safe?

Dr. MAZANEC. So the—again, those resources you just mentioned, ma'am, are designed to provide the basic information needed to the smaller entities in particular, but they're applicable to the sector writ large to ensure that they can adopt best practices and harden their infrastructure.

I would note, too, from a—the diversity of the sector and our focus, again, on patient safety and health impacts, smaller, rural hospitals and in areas where there aren't multiple hospitals have less ability to divert when there is an issue. So in some respects, that can make them—the incidents even more severe when they occur in those contexts, in addition to the fact that they may have

less resources to harden their target. But this is why, again, we engage closely with the sector. We coordinate with them, we're developing tailored tools, and we'll continue to do that.

This is also why we think we need to elevate our activity given that the threat is growing as well. Why the—in the Fiscal Year 2024 President's Budget Request, we're requesting an increase for our activities in this space, and within ASPR, we are standing up a dedicated cyber division to focus on these issues. And we appreciate your support as we do that.

Ms. KELLY. Thank you so much, and thank the witnesses.

And I yield back.

Mr. GRIFFITH. Thank you, gentlelady, for yielding back.

Seeing no further Members wishing to ask questions this afternoon, I would like to thank all of our witnesses again for being here today.

And pursuant to committee rules, I remind Members they have 10 business days to submit additional questions for the record, and I ask the witnesses to submit their responses within 10 business days upon receipt of those questions.

Without objection, committee is adjourned.

[Whereupon, at 4:20 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Documents for the Record

E&C Oversight Hearing 5.16.23

**“Protecting Critical Infrastructure from Cyberattacks: Examining
Expertise of Sector Specific Agencies”**

1. Letter from the American Water Works Association and United States Conference of Mayors to EPA Administrator Michael Regan and Richard Revesz, Administrator, Office of Information and Regulatory Affairs, OMB
2. Letter from the American Water Works Association, et al., to EPA Administrator Michael Regan and Richard Revesz, Administrator, Office of Information and Regulatory Affairs, OMB re: ICR No. 2040-0090
3. Letter from the American Water Works Association, et al., to EPA Administrator Michael Regan re: Pending EO 12866 Regulatory Review
4. Letter from the American Water Works Association, et al., to Radhika Fox, Assistant Administrator for Water, Environmental Protection Agency
5. Letter from American Public Power Association to Mr. Griffith and Ms. Castor



THE UNITED STATES
CONFERENCE OF MAYORS

April 24, 2023

Mr. Michael Regan
Administrator
Environmental Protection Agency
Mail Code 28221T
1200 Pennsylvania Ave. NW
Washington, DC 20460

Mr. Richard Revesz
Administrator
Office of Information and Regulatory Affairs
1650 Pennsylvania Avenue, NW
Washington, DC 20503

VIA ELECTRONIC SUBMISSION

RE: Agency Information Collection Activities; Submission to the Office of Management and Budget for Review and Approval; Comment Request; Public Water System Supervision Program (Renewal), EPA-HQ-OW-2011-0443

Dear Administrator Regan and Administrator Revesz,

The American Water Works Association ("AWWA") and the US Conference of Mayors ("US Mayors") are filing comments on the U.S. Environmental Protection Agency ("EPA") request for comments on the proposed renewal of the Information Collection Request ("ICR") for the Public Water System Supervision Program ("PWSS"). These comments reflect the lack of coverage for the Cyber Rule issued by EPA on March 3, 2023,¹ and assumptions associated with existing and future burden assessment.

The ICR for the PWSS Program (ICR No. 2040-0090) covers information collections for "General State Primacy Activities" to implement compliance oversight and enforcement responsibilities under the Safe Drinking Water Act ("SDWA") which includes obligations for the primacy agency to maintain records on the results of sanitary surveys per 40 CFR 142.14.

¹ USEPA, March 3, 2023, [Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process](#) ("Cyber Rule")

As highlighted previously,² EPA has a statutory obligation under the Paperwork Reduction Act (“PRA”) to assess the burdens associated with the mandatory information collection and recordkeeping requirements created by the Cyber Rule. An ICR extension does not allow for the addition or inclusion of new information collection and recordkeeping requirements. Further the information collection requirements associated with the new Cyber Rule do not exist within the current sanitary survey program.

If cybersecurity was indeed part of the current sanitary survey program, there would be no need for EPA to issue the Cyber Rule and supporting guidance. As a point of reference, the terms “cyber” and “internet” do not even appear in EPA’s current sanitary survey guidance.³ Since it is not included, EPA is required by the PRA and regulations controlling paperwork burdens on the public to publish an ICR for public review and comment. In the absence of an approved ICR, state primacy agencies are not authorized to collect this information and public water systems are not required to respond to requests for information.

AWWA and the US Mayors recognize that the burden associated with a public water system responding to a sanitary survey is covered in multiple ICRs that have been approved individual SDWA regulations and not the PWSS Program. Typically, EPA states that the “PWS burden also includes the burden associated with sanitary surveys” but the expected burden of responding to the new sanitary survey requirements in the Cyber Rule, including minimum expected hours, have not been assessed by the agency. In addition, none of the following ICRs that include sanitary survey obligations address the new information collection and recordkeeping requirements created by the Cyber Rule:

- Microbial Rules (ICR No. 2040-0205)
- Lead and Copper Rule Revisions (ICR No. 2040-0297)
- Disinfectants/Disinfection Byproducts, Chemical and Radionuclides (ICR No. 2040-0204)

The only substantive analysis of the burdens associated with performing and responding to sanitary surveys by states and public water systems is the 2006 *Economic Analysis for the Final Ground Water Rule*,⁴ which estimated labor cost and hours for the following sanitary survey activities:

- Review/Inspect Wells (State & PWS)
- Review/Inspect Treatment (State & PWS)
- Review/Inspect Distribution System (State & PWS)
- Report Review and Discussion (State & PWS)
- Report Documentation/File Review (State)
- Report Development (State)
- Date Entry (State)
- Travel (State)

² Letter dated March 17, 2023 to EPA Administrator Regan and OIRA Administrator Revesz from the American Water Works Association, Association of Metropolitan Water Agencies, National Association of Water Companies and The United States Conference of Mayors (attached)

³ USEPA 2019, Sanitary Survey Field Reference for Use When Conducting a Sanitary Survey of a Small Water System, EPA 816-R-17-002

⁴ USEPA 2006, Economic Analysis for the Final Ground Water Rule, EPA 815-R-06-014

The burden obligations in the following tables represent some of the new information collection and recordkeeping obligations for states and public water system based on the Cyber Rule. The 2006 sanitary survey analysis should be used as a template for an ICR to capture the new burden obligations.

States

Information & Recordkeeping Activity	Changes in Burden Obligation
<i>Familiarization with the new Cyber Rule</i>	EPA has developed a 6-hour training for states to support this need
<i>Assessing cybersecurity during sanitary survey</i>	EPA has estimated the additional time required for states to assess cybersecurity based on population served by the system ⁵ • 2 hours (less than 50,000) • 4 hours (50,000 – 100,000) • 6 hours (greater than 100,000)
<i>Recordkeeping</i> • Track cyber assessment status • Document deficiencies, including significant deficiencies requiring corrective action • Track corrective actions	Currently state databases used to track and record results of sanitary survey do not include data fields designed to track compliance with cybersecurity provisions detailed in EPA guidance, which include 33 controls that may be assessed.

Public Water Systems

Information & Recordkeeping Activity	Changes in Burden Obligation
<i>Familiarization with the new Cyber Rule</i>	EPA has provided 6-hour training for PWS to support this need ⁶
<i>Assessing cybersecurity during sanitary survey</i>	The time EPA estimated the state will be on site for the cyber assessment will also be incurred by the PWS. In addition, the PWS will expend time to prepare the documentation necessary to demonstrate compliance with specific cyber controls. This may also require capitol investments to address controls that EPA has identified as potential “significant deficiencies”. EPA’s checklist includes 33 controls that they assert are “technically feasible for most PWS to address without significant capital expenditures”, however EPA has not provided any documentation that characterizes how this determination was made.

⁵ USEPA, March 16, 2023, Cybersecurity Assessment Training for Primacy Agencies: Part One and Part Two

⁶ USEPA, March 9, 2023, Cybersecurity Assessment Training for Public Water Systems: Part One and Part Two

	Using EPA's checklist and related training as a baseline, the Rule requires assembling an often-complex set of information sources to document compliance and in some cases may be difficult for the state to authenticate.
<i>Recordkeeping</i> • Document conformity, including significant deficiencies requiring corrective action • Track corrective actions • Report deficiencies on annual Consumer Confidence Report • Copies of any written reports, summaries, or communications relating to sanitary surveys must be retained for 10 years.	Results of the sanitary survey requiring corrective action in many instances may require capital expenditures to mitigate. A deficiency may also require public notice as part of the Consumer Confidence Report.

We again respectfully ask that EPA withdraw the Cyber Rule until such time that it has fulfilled the statutory obligations defined by the PRA and regulations controlling paperwork burdens on the public. In addition, OMB should provide a statement clarifying that any information collected to support compliance with the Rule would constitute a violation of the PRA and regulations controlling paperwork burdens on the public. We have further concerns with the lack of legally-required procedures followed before issuing the Cyber Rule which we look forward to addressing with both the agency and OMB.

Sincerely,

American Water Works Association
The US Conference of Mayors

cc: Janet McCabe – EPA/OA
Radika Fox – EPA/OW
Tim DelMonico – EPA/OCIR
Vicki Arroyo – EPA/OP
Jeffrey Prieto – EPA/OGC
Sean O'Donnell – EPA/OIG
Jennifer McLain – EPA/OW/OGWDW
David Travers – EPA/OGWDW/WICRD



THE UNITED STATES
CONFERENCE OF MAYORS

March 17, 2023

Mr. Michael Regan
Administrator
U.S. Environmental Protection Agency
1200 Pennsylvania Ave, NW
Washington, DC 20460

Mr. Richard Revesz
Administrator
Office of Information and Regulatory Affairs
1650 Pennsylvania Avenue, NW
Washington, DC 20503

RE: Public Water System Supervision Program (ICR No. 2040-0090)

Dear Administrator Regan and Administrator Revesz,

The undersigned associations write to you regarding the March 3, 2023 agency action issued by the U.S. Environmental Protection Agency (“EPA”) to State Drinking Water Administrators entitled “[*Addressing PWS Cybersecurity in Sanitary Surveys or an Alternate Process*](#)” (the “Rule”), which requires states to examine cybersecurity practices and controls at public water systems (“PWS”) while conducting sanitary surveys and collect data from PWS regarding the same. This is one of several new substantive requirements imposed by EPA’s new final Rule. According to EPA, this Rule is effective immediately. However, the information collection and record keeping requirements associated with this new Rule violate the Paperwork Reduction Act (“PRA”) and are not covered by EPA’s current Information Collection Request (“ICR”) for the Public Water System Supervision Program (“ICR No. 2040-0090”). This ICR covers information collections for “General State Primacy Activities” to implement compliance oversight and enforcement responsibilities under the SDWA. This includes requirements for the primacy agency to maintain records such as the results of sanitary surveys per 40 CFR 142.14. ICR No. 2040-0090 expires on March 31, 2023.¹

¹ Notice of Office of Management and Budget Action, Public Water System Supervision Program (EPA ICR No. 0270.47), Issued 3/09/2020, https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201903-2040-005#

Given the absence of an OMB approved ICR for the information required under the new Rule, state primacy agencies are not authorized to collect this information and public water systems are not required to respond to requests for information.

More specifically, Congress made it very clear in the PRA² that an agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information, the agency has completed all requirements provided in OMB regulations for data collection.³ This includes publishing a notice in the Federal Register that provides the following:

- a title for the collection of information;
- a summary of the collection of information;
- a brief description of the need for the information and the proposed use of the information;
- a description of the likely respondents and proposed frequency of response to the collection of information;
- an estimate of the burden that shall result from the collection of information;
- notice that comments may be submitted to the agency and OMB; and
- the time period within which the agency is requesting OMB to approve or disapprove the collection of information.

The agency has not fulfilled its obligation to assess burdens the Rule will impose on primacy authorities or PWSs. The Rule requires the collection and review of substantively new and different information than what is currently approved in the current ICR. While the agency's Rule did undergo E.O. 12866 review, no new supporting statement or revised ICR has been prepared or issued for public review and comment.

We are not aware that EPA has given public notice to support renewal of this ICR, that would include providing revised burden estimates, and published a justification of the practical utility of the ICR requirements, especially those contained in the new Rule. Examples of new requirements for primacy agency and PWSs that result in burdens due to the Rule include, but are not limited to, the following:

Training⁴

- EPA has released 6 hours of training for states to review the Rule, implementation options and available resources. The training includes a table provided by EPA

² Paperwork Reduction Act, Public Law 104-13, <https://www.reginfo.gov/public/reginfo/pra.pdf>

³ 5 CFR 1320 - Controlling Paperwork Burdens on the Public, <https://www.govinfo.gov/content/pkg/CFR-2010-title5-vol3/xml/CFR-2010-title5-vol3-part1320.xml>

⁴ EPA Cybersecurity for the Water Sector – Training, <https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector#rule>

estimating “the additional time required for states to assess cybersecurity will be reflective of the population served by the system.”

- EPA has released 6 hours of training for PWSs demonstrating how to use EPA’s cybersecurity checklist to assess their program, information on how to address vulnerabilities, and available resources. EPA’s checklist includes 33 questions related to various cybersecurity controls for which no estimated time burden is provided, but a majority are classified in the training materials as potential “significant deficiencies” if not implemented.

Recordkeeping

- States must maintain records of significant deficiencies and confirmation that the deficiency has been corrected. This requires a modification of existing compliance data systems to add necessary data fields to document cybersecurity related items as part of the sanitary survey.
- States must develop and maintain list of “approved agents” if it allows agents other than the state to conduct the cybersecurity component of the sanitary survey.
- States must add cybersecurity to their annual evaluation of the state’s program for conducting sanitary surveys in the report transmitted to EPA.

Expanded Scope of Coverage

- EPA records⁵ indicate that there are 151,606 PWSs for which this Rule may apply. According to EPA compliance records there are 10,003 community water systems that serve 3,300 or more persons that must comply with AWIA §2013.⁶ These systems are mandated by Congress to include an assessment of cybersecurity threats as part of a risk and resilience assessment and an emergency response plan. Therefore, the scope of the Rule captures an additional 141,603 PWSs that would at minimum be required to assess the applicability of the new Rule and associated requirements.

We do not believe that the expiration of the current ICR satisfies any of the criteria that may justify emergency processing by OMB. There is no reasonable explanation for why the agency would be unable to comply with the normal clearance procedures for the existing ICR. The addition of new information collection obligations created by the Rule do not justify emergency processing either since this action has been under consideration by the agency since 2021.⁷ Finally, there has been no consultation or collaboration with the organizations

⁵ EPA, Safe Drinking Water Information System (SDWIS), 2022Q4 Summary Data

⁶ EPA, America’s Water Infrastructure Act Section 2013 Compliance Data, <https://www.epa.gov/waterresilience/americas-water-infrastructure-act-section-2013-compliance-data>

⁷ Unified Agenda of Regulatory and Deregulatory Actions, Fall 2021, <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=2040-AG20>

representing PWSs regarding considerations that might “minimize the burden” per 5 C.F.R. 1320.13.

Respectfully, we ask that EPA withdraw the Rule until such time that it has fulfilled the statutory obligations defined by the PRA and regulations controlling paperwork burdens on the public. In addition, OMB should provide a statement clarifying that any information collected to support compliance with the Rule would constitute a violation of the PRA and regulations controlling paperwork burdens on the public. We have further concerns with the lack of legally-required procedures followed before issuing the Rule which we look forward to addressing with both the agency and OMB.

Sincerely,

American Water Works Association
 Association of Metropolitan Water Agencies
 National Association of Water Companies
 US Conference of Mayors

cc: Radika Fox – EPA/OW
 Tim Del Monico – EPA/OCIR
 Vicki Arroyo – EPA/OP
 Jeffrey Prieto – EPA/OGC
 Sean O'Donnell – EPA/OIG
 Jennifer McLain – EPA/OW/OGWDW
 David Travers – EPA/OGWDW/WICRD



January 25, 2023

Mr. Michael Regan
 Administrator
 Environmental Protection Agency
 1200 Pennsylvania Ave, NW
 Washington, DC 20460

Re: Pending EO 12866 Regulatory Review: Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity

Dear Administrator Regan,

The undersigned associations write you regarding EPA's Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity, which OMB is currently reviewing.

Collectively we are dedicated to protecting public health and the environment by providing safe drinking water and excellent wastewater services. The infrastructure our members maintain is the foundation on which U.S. communities are built.

Cybersecurity is mission-critical for all types of water utilities. As such, we support efforts to strengthen cybersecurity, and are eager to collaborate with the agency to develop and implement effective approaches. However, EPA's planned efforts to add cybersecurity requirements to the Sanitary Survey Program for drinking water utilities are ill-advised, impractical, and are not designed to meaningfully improve system resiliency. EPA's approach is also legally flawed as described in the addendum to this letter.

We write to raise the significant legal, procedural, and policy concerns drinking water utilities have regarding the imposition of cybersecurity requirements through the Sanitary Survey

Program and offer a process to examine alternatives. Ultimately, we fear the Sanitary Survey approach could do more harm than good for drinking water utilities.

To that end, we are committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based. We recognize the necessity to act, and we are committed to working expediently to develop and implement cybersecurity solutions for the water sector that are developed by consensus with critical input and support from water utilities, an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector.

Thus, to best serve our shared goal of cybersecurity solutions for the water sector, we urge you to recall the RIN 2040-ZA41 Memorandum under review at the Office of Management and Budget for reconsideration with stakeholders and to ensure compliance with all applicable laws.

Sincerely,

American Water Works Association
 Association of Metropolitan Water Agencies
 National Association of Clean Water Agencies
 National Association of Counties
 National Association of Water Companies
 National League of Cities
 National Rural Water Association
 US Conference of Mayors
 Water Environment Federation

cc: Christopher Inglis – EOP/ONCD
 Elizabeth Sherwood-Randall – EOP/ONSA/OHSA
 Richard Revesz – EOP/OMB/OIRA
 Janet McCabe – EPA/AO
 Radhika Fox – EPA/OW
 Jeffrey Prieto – EPA/OGC
 Sean O'Donnell – EPA/OIG
 Tim Del Monico – EPA/AO/OCIR
 Victoria Arroyo – EPA/AO/OP

Addendum to Joint Association Letter regarding the Pending EO 12866 Regulatory Review: Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity

Statutory & Regulatory History

With increasingly severe cyber threats over the last decade, support has grown at all levels of government and within the sector to enhance water and wastewater system security and resilience. In recent years, the prevailing—and appropriate—trend was a collaborative approach to improving water and wastewater sector-specific cybersecurity through risk and resilience assessments and emergency response planning undertaken by utilities, which Congress has fully endorsed. But within that past eighteen months, EPA has made a significant shift by instead proposing regulation for drinking water utilities through the Sanitary Survey Program, an admittedly “creative”¹ approach, which we find neither practical nor legally supportable. A brief statutory and regulatory history follows:

America’s Water Infrastructure Act of 2018 (AWIA)

The AWIA (PL 115-270) was passed to improve drinking water and water quality, increase water and wastewater infrastructure investments and jobs, and enhance public health and quality of life. It included significant changes to the Safe Drinking Water Act (SDWA). Among those, AWIA Section 2013 references cybersecurity in addressing community water system risk and resilience. Particularly, this section amended SDWA Section 1433 to require each community water system serving a population of greater than 3,300 persons to conduct a system risk and resilience assessment at least every five years, including the risk from malevolent acts that could “substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water”, which encompasses cyber threats. SDWA § 1433(a). Further, Section 2013 requires such systems to incorporate the findings of their assessment into an emergency response plan, which includes “strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system.” SDWA § 1433(b). Thus, Congress specifically highlighted cybersecurity as an issue to address through risk and resilience assessments and emergency response planning.

We would also like to call attention to the provision pertaining to alternative preparedness and operational resilience programs. SDWA § 1433(f). Specifically, consistent with section 12(d) of the National Technology Transfer and Advancement Act of 1995, this provision requires EPA to recognize voluntary consensus standards and guidance developed by third-party organizations, like AWWA, that support and facilitate the implementation of the above requirements. For example, AWWA’s Cyber Security Assessment Tool and Guidance was developed in collaboration with the National Institute of Standards and Technology (NIST), the Cybersecurity

¹ Statement of Anne Neuberger, Transcript: Securing Cyberspace, The Washington Post (Oct. 13, 2022), <https://www.washingtonpost.com/washington-post-live/2022/10/13/transcript-securing-cyberspace/>.

and Infrastructure Security Agency (CISA), and EPA representatives in 2014 (and updated in 2019) to provide a consensus-based, sector-specific approach to the NIST cybersecurity framework. Yet, EPA has not leveraged this option to advance the agencies mission in support of AWIA §2013 and related cybersecurity objectives.

Infrastructure Investment & Jobs Act of 2021

A significant component of the Infrastructure Investment and Jobs Act (PL 117-58) was greater investment and support to rehabilitate and update water infrastructure, including through several authorizations that support cybersecurity improvements. For example, the Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program (sec. 50107) and the Clean Water Infrastructure Resilience and Sustainability Program (sec. 50205) provide grant funding from EPA to help reduce cybersecurity vulnerabilities, among other priorities, at drinking water and wastewater systems. Similarly, the Act (sec. 50113) required EPA and CISA to develop and report to Congress (1) a prioritization framework to identify public drinking water systems that, if degraded or rendered inoperable, would have significant public health and safety impacts, taking into consideration any identified cybersecurity vulnerabilities and independent capacity to address such vulnerabilities, and (2) a technical cybersecurity support plan for public drinking water systems with a methodology for identifying for which systems cybersecurity support should be priorities, timelines for making voluntary technical support available, and specific capabilities that could be utilized to provide such support. These were completed in May 2022² and August 2022³, respectively. Congress did not, however, authorize EPA to develop or otherwise impose cybersecurity requirements on water utilities.

EPA Unified Agenda – Fall 2021⁴

In the Fall 2021 Unified Agenda listed EPA/OW RIN 2040-AG20, Cybersecurity in Public Water Systems, as a rulemaking in the final rule stage. EPA indicated that it was evaluating regulatory approaches to improve cybersecurity at public drinking water systems. While EPA planned to offer separate guidance, training, and technical assistance to states and public drinking water systems on cybersecurity, EPA also announced its plan to issue this Final Interpretive Rule to “provide regulatory clarity and certainty and promote the adoption of cybersecurity measures by public water systems.” Particularly, EPA proposed to include cybersecurity assessments as part of the regular drinking water Sanitary Survey Program:

Sanitary surveys, which states, tribes, or the EPA typically conduct every 3 to 5 years on all public water systems, should include an evaluation of cybersecurity to identify significant deficiencies. EPA recognizes, however, that many states

² <https://www.epa.gov/system/files/documents/2022-08/Prioritization%20Framework%20RtC%20final.pdf>

³ https://www.epa.gov/system/files/documents/2022-08/9910_RtC-Technical%20Cybersecurity%20Support%20Plan_20220818_final.pdf

⁴ <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=2040-AG20>

currently do not assess cybersecurity practices during public water system sanitary surveys. This action is necessary to convey to states that EPA interprets existing regulations for public water system sanitary surveys as including the possible identification of significant deficiencies in cybersecurity practices.

EPA justified the interpretive rule under the Administrative Procedure Act (“APA”) as an “interpretation of existing responsibilities under current regulations” stating that “[i]t establishes no new regulatory requirements and, hence, has no regulatory costs or benefits.” Importantly, EPA explicitly acknowledged that there were alternatives to the interpretive rule approach, specifically that EPA could “[p]rovide guidance to states, tribes, and EPA on evaluating cybersecurity practices during public water system sanitary surveys without issuing an interpretive rule.”

EPA said it would issue a Final Interpretive Rule in April 2022. However, in response to this proposal, in December 2021, water system associations asked EPA to not pursue this regulatory strategy, citing various significant concerns with its legality under the APA, inadequate protection of sensitive information, lack of national consistency given that the Sanitary Survey Program is implemented by states, insufficient skill and training of state staff. (*e.g.*, AWWA 12/9/21 letter, Association of State Drinking Water Administrators 9/29/21, 2/9/22, 11/21/22 letters).

EPA Unified Agenda – Spring 2022⁵

Following these public comments, EPA recategorized EPA/OW RIN 2040-AG20, Cybersecurity in Public Water Systems, as a “Long-Term Action” in the Spring 2022 Unified Agenda. Additionally, in a May 2022 budget hearing before the House Committee on Energy and Commerce’s Subcommittee on Environment and Climate Change, EPA assured the subcommittee that the Agency would be transparent in its rulemaking processes to allow for proper public notice and comment. Further, when asked about water and wastewater cybersecurity, the Agency indicated that it is “laser focused on this cybersecurity issue” and “using all of our statutory authority to pursue cybersecurity in the water space that we can.” Stating further that EPA would not outsource its leadership responsibility in the water and wastewater cybersecurity space, engage regularly with the water sector and the Coordinating Council on Cybersecurity. The Agency committed to making each of these assurances in writing; however, to our knowledge, those written assurances have not been made. The Fiscal Year 2023 EPA Budget, Houston of Representatives, Subcommittee on Environment and Climate Change, Committee on Energy and Commerce, Washington, D.C. (May 17, 2022) at 1737-1837.

EPA Unified Agenda – Fall 2022⁶

The most recent Unified Agenda retitled the “Long Term Action” for EPA/OW RIN 2040-AG20 to “Public Water System Cybersecurity Requirements.” This action is summarized

⁵ <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=2040-AG20>

⁶ <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=2040-AG20>

as “evaluating regulatory approaches to improve cybersecurity at public water systems. EPA plans to offer separate guidance, training, and technical assistance to states and public water systems on cybersecurity. This action will provide regulatory clarity and promote the adoption of cybersecurity measures by public water systems.”

OMB/OIRA RIN 2040-ZA41 – Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity

On December 16, 2022, EPA submitted RIN: 2040-ZA41, *Memorandum to State Drinking Water Administrators on Public Water System Cybersecurity*, to OMB/OIRA for review. While EPA has not made the memo or its contents public, we suspect it is substantively the same as the prior proposed interpretive rule. Accordingly, AWWA, AMWA, NRWA, NAWC, WEF, and NACWA requested a meeting with OMB to discuss the memo and express our concerns with a Sanitary Survey Program-based approach.

We are also aware that the Association of State Drinking Water Administrators (ASDWA) had a meeting with OMB expressing similar concerns with the prospective imposition of regulatory burden resulting from this Memo. In addition, concerns were also expressed by AWWA about the Memo and EPA’s process during the public comment period of the January 13, 2023, meeting of EPA’s Local Government Advisory Committee.

Response and Recommendations

While we appreciate that EPA has moved from a Final Interpretive Rule to Long-Term Action, and while the contents of the RIN: 2040-ZA41 memorandum are not yet public, we have significant concerns that EPA has yet to address. Proceeding at this stage with any sort of regulatory requirement would be premature.

First, as explained in a December 9, 2021, letter from AWWA, AMWA, NAWC, and NRWA to Assistant Administrator of Water Radhika Fox: “We do not believe an agency action to establish cybersecurity requirements through an interpretive rule is legally justifiable, as interpretive rules must not set new legal standards or impose new requirements.” If the effect of EPA’s action is still to impose cybersecurity requirements on operators at public drinking water systems, EPA must satisfy the APA and other legal prerequisites, or may otherwise be subject to judicial review. 5 U.S.C. § 706(2)(A); *Mortg. Bankers Ass’n v. Harris*, 720 F.3d 966 (D.C. Cir. 2013) (quoting *F.C.C. v. Fox Television Stations*, 556 U.S. 502, 513 (2009) for the holding that the APA provides the full scope of “judicial authority to review executive agency action for procedural correctness.”).

An interpretive rule “simply indicates an agency’s reading of a statute or a rule. It does not intend to create new rights or duties, but only reminds affected parties of existing duties.” *Paralyzed Veterans of Am. V. West*, 138 F.3d 1434 (Fed. Cir. 1994) (quoting *Orengo Caraballo v. Reich*, 11 F.3d 186, 195 (D.C.Cir.1993)). “The critical feature of interpretive rules is that they are

issued by an agency to advise the public of the agency's construction of the statutes and rules which it administers." *Perez v. Mortgage Bankers Ass'n*, — U.S. —, 135 S.Ct. 1199, 1204, 191 L.Ed.2d 186 (2015) (citation omitted). "The most important factor in differentiating between binding and nonbinding actions is "the actual legal effect (or lack thereof) of the agency action in question. . . . Agency action that creates new rights or imposes new obligations on regulated parties or narrowly limits administrative discretion constitutes a legislative rule." *Ass'n of Flight Attendants-CWA, AFL-CIO v. Huerta*, 785 F.3d 710, 717 (D.C. Cir. 2015) (citing *Nat'l Mining Ass'n v. McCarthy*, 758 F.3d 243, 252 (D.C. Cir. 2014)). The hallmark of an interpretive rule is that such rules are exempt under the APA from public notice and comment requirements. 5 U.S.C. § 553(b)(A). However, when a rule goes beyond that advisory or confirmatory purpose, it is considered a legislative rule, to which public notice and comment requirements apply. 5 U.S.C. § 553(b).

EPA's Memo to add cybersecurity requirements to the Sanitary Survey Program goes well beyond merely providing the "regulatory clarity and certainty" it purports, and does, in fact, establish new regulatory requirements not otherwise imposed under the SDWA. The Sanitary Survey Program is a precondition of state primacy, which is a "systematic program for conducting sanitary surveys of public water systems in the State," which includes an "onsite review of the water source (identifying sources of contamination using results of source water assessments where available), facilities, equipment, operation, maintenance, and monitoring compliance of a public water system to evaluate the adequacy of the system, its sources and operations and the distribution of safe drinking water." SDWA § 1413; 40 C.F.R. §§ 142.10, 142.16. EPA's Memo would seek to add cybersecurity to the state primacy requirements. Although the Sanitary Survey Program requirements generally cover operations, they have never included cybersecurity nor was the Program drafted with cybersecurity in mind — yet EPA is now attempting to tenuously read it in. Such an action would constitute an entirely new requirement, going well beyond the purpose of an interpretive rule. Moreover, SDWA Section 1433 requires that certain drinking water systems conduct risk and resilience assessments that include cybersecurity considerations, then incorporate the assessment findings into an emergency response plan with particulars on how resilience can be improved and implementation of such procedures. It does not, however, require that cybersecurity be part of the state Sanitary Survey Program or be enforced as such. EPA's proposed actions therefore are also inconsistent with Congressional intent.

In addition to this noncompliance with the APA, EPA has not held any open stakeholder engagement on its Final Interpretive Rule or as part of development of the RIN 2040-ZA41 Memorandum, nor has it held a cooperative federalism or Unfunded Mandates Reform Act (2 U.S.C. § 1501 et seq.) consultation with representatives of local and state government. Essentially, EPA has proceeded despite ample opposition from multiple water and wastewater organizations, including state administrators, and without sufficiently engaging with those most affected despite offering assurances to Congressional leaders that such engagements would take place.

More importantly, EPA's proposal to include cybersecurity requirements within the drinking water Sanitary Survey Program administered by state sanitarians is a sub-optimal way to address cybersecurity challenges posed to critical water infrastructure systems. As repeatedly noted by the ASDWA (9/29/21, 2/9/22, 11/21/22 Letters), for example, state authorities that administer the Sanitary Survey Program lack the appropriate staffing, training and expertise to evaluate cybersecurity programs. Even with training, given the complexity of cybersecurity

measures and their relatively rapid evolution, agency staff could misunderstand best practices and their implementation, resulting in an unmerited deficiency or a redirection from a practice that is sufficiently securing the utility. Nothing in federal or state law protects information collected through state agencies' sanitary surveys from being shared publicly, and such disclosures could risk exposing system vulnerabilities to actors who pose cybersecurity threats.

To address these issues and concerns we are committed to working collaboratively with EPA and other stakeholders to develop an effective approach to cybersecurity that is risk- and performance-based. We recognize the necessity to act, and we are committed to working expediently to develop and implement cybersecurity solutions for the water sector that are developed by consensus with critical input and support from water utilities, an approach that is legally sound and will result in a far more effective approach to mitigate cyber threats facing the water sector.

Thus, to best serve our shared goal of cybersecurity solutions for the water sector, we urge you to recall the RIN 2040-ZA41 Memorandum under review at the Office of Management and Budget for reconsideration with stakeholders and to ensure compliance with all applicable laws.



December 9, 2021

The Honorable Radhika Fox
 Assistant Administrator for Water
 U.S. Environmental Protection Agency
 Washington, DC 20460

Dear Assistant Administrator Fox:

Representatives of the water and wastewater sector have repeatedly raised concerns about the agency's pursuit of issuing a direct final interpretive rule to add cybersecurity to the sanitary survey assessments, but our concerns have not been addressed. Therefore, we feel compelled to express our opposition to the proposed approach.

As you well know, water and wastewater systems are on the front lines of protecting public health and the environment and have exceptional track records doing so. Our members have many years of experience with both sanitary surveys and cybersecurity, and they believe the surveys will be ineffective at improving cybersecurity at water systems.

We believe a solution to securing cybersecurity for the water sector that is arrived at by consensus with and support from water utilities will be far more effective to protect against cyber compromises.

The most effective approach is one that is risk- and performance-based, rather than top-down, one-size-fits-all. This would allow for tailored solutions based each community's unique set of risks, threats, and vulnerabilities.

Among our concerns are:

- We do not believe an agency action to establish cybersecurity requirements through an interpretive rule is legally justifiable, as interpretive rules must not set new legal standards or impose new requirements.
- Nothing in federal or state law protects information collected through sanitary surveys by state agencies from being shared with the public. If, for instance, a state discloses that a utility has a particular vulnerability, the information would be very valuable to hackers looking for an easy target, opening the utility up to ransomware attacks or worse.
- State primacy agency staff are not qualified to assess the cyber readiness of a water system. We anticipate state staff could misunderstand either a best practice or a utility's implementation of said best practice and thus report an unmerited significant deficiency. This could lead to misinformation in the media, reputational harm, and fines. Worse, state primacy agency staff could unintentionally direct a utility toward a practice that is in fact inappropriate for securing the utility and perhaps open the door to a hacker.
- Should a state primacy agency give a utility a clean bill of health and the utility subsequently suffer a compromise, both the state and the utility could be put in legal jeopardy.

Assistant Administrator Fox
December 9, 2021
Page 2 of 2

- Each state agency may develop their own procedures and recommendations for utilities, leading to a patchwork of regulations across the country. Not only is this burdensome to water utilities that have subdivisions in multiple states, but it will complicate the development of guidance and training by the sector organizations, CISA, and even EPA. Related, many states could go farther than EPA intends in the agency's guidance documents and turn the sanitary survey program into an entirely different regulatory regime.

We are examining various options to effectively protect water systems from cyber threats. We are eager and committed to a collaborative solution that is protective of public health and cyber infrastructure in water utilities, and we would like to work with your office to do so. However, we caution against measures that could fail to have a decisive impact on water sector cybersecurity and that lack input by water sector subject matter experts.

As stewards of public health and the environment, the water sector is ready to accept requirements and accountability that does not do more harm than good or divert resources from water utilities' most effective cybersecurity measures. We look forward to collaborating with you on a better solution that will result in greater cybersecurity in the water sector. We are willing to commit the resources necessary to arrive at one in a reasonable amount of time.

If you would like to discuss our concerns, we would be more than happy to have the conversation.

Sincerely,



G. Tracy Mehan III
Executive Director, Government Affairs
American Water Works Association



Diane VanDe Hei
Chief Executive Officer
Association of Metropolitan Water Agencies



Robert F. Powelson
President and Chief Executive Officer
National Association of Water Companies



Matthew Holmes
Chief Executive Officer
National Rural Water Association



Walter T. Marlowe, P.E., CAE
Executive Director
Water Environment Federation

cc: Jennifer McLain/EPA OGWDW
David Travers/EPA WSD
Brian Scott/NSC



May 16, 2023

The Honorable Morgan Griffith
 Chairman, Subcommittee on Oversight & Investigations
 House Committee on Energy & Commerce
 2125 Rayburn House Office Building
 Washington, DC 20515

The Honorable Kathy Castor
 Ranking Member, Subcommittee on Oversight & Investigations
 House Committee on Energy & Commerce
 2322 Rayburn House Office Building
 Washington, DC 20515

Dear Chairman Griffith and Ranking Member Castor:

The American Public Power Association (APPA) appreciates the opportunity to submit a statement for the record for the House Energy & Commerce Committee's Subcommittee on Oversight & Investigation's hearing, "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies."

APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. APPA represents public power before the federal government to protect the interests of the more than 49 million people that public power utilities serve, and the 96,000 people they employ. APPA advocates and advises on electricity policy, technology, trends, training, and operations.

Key Points

- The model of shared responsibility for cybersecurity and resilience, assigning each critical infrastructure sector a Sector-Risk Management Agency (SRMA) to work closely with on a day-to-day basis, while broadly coordinating with the Department of Homeland Security (DHS), has and continues to be successful; DOE is the energy sector's SRMA.
- The electric sector has strong mandatory and enforceable cyber and physical security standards, including cyber incident reporting, in place.
- Cybersecurity standards and mandates must be risk-based; not all electric utilities have the same risk profile.
- The federal government should play a greater role in helping electric utilities in assessing vendor cybersecurity practices, such as establishing a federal vendor certification or accreditation program.
- Congress should pause from consideration of legislation to create additional cyber incident reporting mandates until the Cybersecurity Incident Reporting for Critical Infrastructure Act (CIRCA) is fully implemented.
- Threats are always evolving, and standards and reporting are only one part of ensuring security.
- Strong industry-government partnerships should be supported to prevent, prepare for, and respond to attacks are vital.

Sector-Risk Management Agencies

In 2013, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (PPD-21) established a national policy on critical infrastructure security and resilience. PPD-21 tasked DHS with coordinating the overall federal effort to promote the security and resilience of critical infrastructure. However, recognizing existing statutory and regulatory authorities of specific departments and agencies, as well as their unique knowledge and specialized expertise, PPD-21 wisely identified 16 critical infrastructure sectors and designated a Sector Risk Management Agency (SRMA) for each sector to “serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities,” among other tasks. The Department of Energy (DOE) is the SRMA for the energy sector; within DOE, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) leads DOE’s cybersecurity and energy security mission.

APPA strongly supports the partnership model established in PPD-21, with DOE as the energy sector’s SRMA. However, the partnership model is not without complications. This is especially true when it comes to cyber incident reporting. As detailed further below, APPA urges Congress to pause from consideration of legislation to create additional cyber incident reporting mandates on the electric sector until CIRCIA is fully implemented. That would allow for the evaluation of CIRCIA’s implementation and a determination of whether further changes are needed.

Mandatory and Enforceable Standards

Congress approved the mandatory and enforceable standards regulatory regime for the bulk power system in the Energy Policy Act of 2005 (EPA05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts and updates mandatory reliability standards that apply across the North American grid, including Canada. These standards include the critical infrastructure protection (CIP) standards addressing physical security and cybersecurity. Participation by industry experts and compliance personnel in the NERC CIP standards development process ensures that the standards are risk-based and technically sound. The Federal Energy Regulatory Commission (FERC) has the power to then approve or remand those standards as they apply in the United States. To ensure compliance, under FERC’s oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time. CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

APPA believes that the regulatory regime established in EPA05 has been very successful due to the deep involvement of technical experts from government and industry alike, as well its iterative nature that allows NERC to identify and respond to developing threats.

Information Sharing and Incident Reporting

The electric sector has long been subject to cyber incident reporting mandates to DOE via an Electricity Emergency Incident and Disturbance Report (OE-417) and through the NERC/FERC process. These requirements are in addition to obligations under individual state laws on data security and data breach reporting that cover many information technology (IT) cyber security incidents. The electric industry has historically had robust voluntary participation in information sharing organizations, including with the Electricity Information Sharing and Analysis Center (E-ISAC) and the Multi-State Information Sharing and Analysis Center for the public power community. Finally, the electric sector has seen increased

adoption of technologies that assist with the visibility and monitoring of its industrial control system and operational technology networks, which also allows some automated sharing of information with the federal government.

Another layer of mandatory cyber incident sharing requirements is expected to be added on top of these pre-existing requirements through CIRCIA implementation. Signed into law in March 2022, CIRCIA will require covered critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to DHS's Cybersecurity and Infrastructure Security Agency (CISA). APPA filed comments in November 2022 in response to a request for information kicking off the CIRCIA rulemaking asking CISA to take a careful and deliberative approach to implementation that accounts for existing reporting mandates and organizations, and to appropriately tailor reporting mandates commensurate with risk to national security.

As outlined above, the electric sector is unique among critical infrastructure sectors in the extent and maturity of existing information sharing regulations and programs. Public power utilities, as units of state and local governments and varying so widely in size and risk profiles, are still more unique. Given these complexities, and pursuant to CIRCIA's explicit intent, it is critical that CISA, DOE, FERC/NERC, and industry are given the time and space necessary to harmonize the new reporting envisioned by CIRCIA with those that already exist. Layering on additional reporting mandates prior to full implementation of CIRCIA would create significant confusion, as well as impose a significant burden on public power utilities with little, if any, security benefits.

Supply Chain Security Challenges

One area of energy sector cybersecurity that would benefit from more involvement from the federal government is supply chain. NERC first adopted supply chain standards in 2017, but a significant challenge for NERC-registered entities in complying with these standards is that vendors are not subject to FERC's jurisdiction under section 215 of the FPA. Supply chain cybersecurity would benefit from a greater federal government role in providing resources that would assist utilities in assessing vendor cybersecurity practices, such as a federal vendor certification or accreditation program. Encouraging domestic manufacturing of necessary products and components would also likely have both supply chain security and reliability benefits. APPA has not yet endorsed a particular approach to vendor accreditation or certification. However, APPA would be concerned with a program structure that places additional requirements on utilities in the expectation that utility vendors would conform to such requirements. Most – if not all – public power utilities would not have the leverage to demand certification from vendors on their own.¹

Public-Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and DHS, on matters of critical infrastructure protection. One important venue for this collaboration is the Electricity Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between the federal government 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. APPA and public power utilities play a leadership role on the ESCC, which includes utility CEOs and trade association leaders

¹ Post-Technical Conference Comments of the American Public Power Association, Joint FERC-DOE Supply Chain Risk Management Technical Conference, December 7, 2022, available at:

https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20230217-5199&optimized=false.

www.PublicPower.org #PublicPower 3

representing all segments of the industry. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

APPA works closely with DOE on a number of fronts. Notably, APPA has been awarded three grants since 2016 to help strengthen the cybersecurity posture of public power utilities. Most recently, in September 2022, DOE CESER awarded APPA a grant of \$15 million over a three-year period to facilitate the adoption and deployment of industrial control systems cybersecurity technologies for municipal utilities. This builds off an existing \$6 million, three-year cooperative agreement (awarded in 2020) to develop and deploy cyber and cyber-physical solutions for public power utilities, and a previous three-year cooperative agreement (awarded in 2016) to assist small- and medium-sized public power utilities with cyber risk assessment and cybersecurity training. APPA's implementation of these agreements is guided by its Cybersecurity Defense Community working group that includes representatives from public power utilities of varying sizes across the country.

A new program at DOE that is being stood up, the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC), which passed as part of the Infrastructure Investment and Jobs Act (P.L. 117-58), is based off the successes of these grant programs. The RMUC is authorized to appropriate a total of \$250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. APPA appreciates Congress' specific attention to the cybersecurity needs of municipal utilities in this program.

"Defense-in-Depth" and Sector-Wide Preparation Efforts

The goal of every utility and the entire industry is to manage risk prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize facilities and assets that, if damaged, would have the most severe impacts on their ability to keep the power on for their community. As such, the electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to "all hazard" threats to electric grid operations.

Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One of the biggest exercises, GridEx, takes place every two years. GridEx VI took place in November 2021 and involved hundreds of organizations and thousands of participants from industry, government agencies, and partners in Canada and Mexico. Managed by NERC and the E-ISAC, the event included a tabletop exercise where electric sector executives and senior government officials worked through incident response protocols in a scenario involving multiple operating challenges.

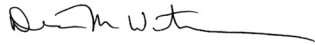
The three primary segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents exceeding an individual entity's capacity to respond. CMA participating entities serve approximately 80 percent of U.S. electric customers and 75 percent of U.S. natural gas customers.

Finally, electric utilities regularly share transformers and other equipment through long existing bilateral and multilateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program (STEP), SpareConnect, and Grid Assurance—to improve grid resiliency.

Conclusion

Public power utilities know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans. APPA supports the continued model of shared partnership for cybersecurity and resilience of the energy sector, with DOE as the sector's SRMA. It is critical that Congress and regulators take a risk-based, defense-in-depth approach to promoting cybersecurity of the electric sector, given the diversity of size, model and resources of individual entities. APPA appreciates the opportunity to provide a statement.

Sincerely,



Desmarie Waterhouse
Senior Vice President of Advocacy and Communications & General Counsel

**House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
May 16, 2023, Hearing**

Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies

Questions for the Record Submitted to Mr. Puesh Kumar

QUESTIONS FROM REPRESENTATIVE MORGAN GRIFFITH

- Q1. Cyberattacks to critical infrastructure present one of the most significant threats to the Nation and the interconnected nature of critical infrastructure systems exposes these systems to attacks from foreign adversaries and their allies. Last year, Congress placed a “high priority on ensuring the protection of the electric grid against cyberattacks and remains concerned about the rise in frequency and sophistication of large-scale, nation state-directed attacks,” in its report accompanying the House of Representatives’ Energy and Water Development and Related Agencies Appropriations Bill for Fiscal Year 2023. To better enhance secure systems to strengthen defense of grids, Congress provided funding to the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) specifically “to expedite development and testing of secure inputs, processing, and outputs of systems utilizing novel cybersecurity technology.” It is the Committee’s understanding that this directive has not been executed. How does CESER plan to carry out this direction from Congress in an expeditious manner to better secure systems and enhance national security in the face of growing threats?
- A1. The Department of Energy’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER)’s mission is to strengthen the security and resilience of the U.S. energy sector from cyber, physical, and climate-based risks and disruptions. To accomplish this mission, CESER develops tools and technologies to mitigate risks to the energy sector. CESER solicits applications to competitively select and award research and development (R&D) projects. CESER developed a Request for Information (RFI) to identify research gaps from the energy sector which includes the development and testing of secure inputs, processing, and outputs of systems utilizing novel cybersecurity technology. This RFI was released on September 5, 2023, and closed on October 11, 2023. CESER will then release a competitive solicitation, informed by the RFI, and award projects that best address the cybersecurity priorities included in the report accompanying the Energy and Water Development and Related Agencies Appropriations Bill for Fiscal Year (FY) 2023. These projects will be awarded in FY 2024.
- Q2. Late last year, the Cybersecurity Infrastructure & Security Agency (CISA) released its new Cross-Sector Cybersecurity Performance Goals (CPGs), a foundational set of information technology and operational technology practices and recommendations intended to help smaller, lesser-resourced organizations better prioritize cybersecurity efforts and reduce risk. It is the Committee’s understanding that CISA stated at the time

House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
May 16, 2023, Hearing
Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies
Questions for the Record Submitted to Mr. Puesh Kumar

that it was going to work with Sector Risk Management Agencies (SRMAs) to develop sector-specific CPGs.

- Q2a. Has CESER engaged CISA on developing these sector specific CPGs, and if so, how are those efforts progressing? When should we expect them to be done?
- A2a. CESER has engaged with the Department of Homeland Security's Cybersecurity Infrastructure and Security Agency (CISA) on developing sector-specific Cyber Performance Goals (CPGs). As the Sector Risk Management Agency (SRMA) for the energy sector, CESER, on behalf of the Department of Energy, is collaborating with CISA, industry trade associations, Sector Coordinating Councils, and energy private sector partners to identify specialized concerns the energy sector has with the application of sector-specific performance goals to energy devices and processes.

This is particularly important for both Industrial Control Systems (ICS) and operational technology devices, as well as new technologies like distributed energy resources (DER). Separately from the development of the CPGs, DOE funded an effort with the National Association of Regulatory Utility Commissioners (NARUC) to develop a set of cyber baselines for Distribution Systems and DER. CISA is a partner in this effort and this work will inform the energy sector specific CPGs. CESER anticipates completing these baselines in 2023. Additionally, CESER is using concepts from that effort to inform the development of performance goals for other parts of the sector, including oil and natural gas pipelines.

- Q2b. How is CESER using CISA's cross-sector CPGs to drive security improvements in the energy sector?
- A2b. The energy sector is highly regulated. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards for transmission and generation entities, the TSA Security Directives for critical natural gas pipelines at the federal level, and the growing number of state public utility commission requirements provide a high bar for security controls implemented throughout the energy

House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
May 16, 2023, Hearing
Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies
Questions for the Record Submitted to Mr. Puesh Kumar

sector. CESER is focusing efforts to use the CPGs as a resource for utility owner/operators who do not fall within the jurisdiction of one of the above-named frameworks. While the CPGs are performance goals, not implementable controls, CESER is focused on finding ways to use the CPGs to encourage sound cybersecurity practices and reduce risk throughout the energy sector.

- Q3. How do you measure and report on the impact and outcomes of your cybersecurity initiatives and investments on cyber-physical systems in critical infrastructure?
- A3. DOE has a comprehensive portfolio of activities to enhance the energy sector's cybersecurity and cyber-physical posture. The Department utilizes programmatic best practices from project identification / project selection to outcome management to secure cyber-physical systems from cybersecurity threats. Program and project progress (along with key highlights) within CESER, are tracked on a quarterly basis and reported through ongoing continuous review and improvement processes.

For example, CESER measures and reports the impact and outcomes of its supply chain cybersecurity testing efforts (CyTRICS program) quarterly under the DOE Annual Performance Goals. These metrics are available publicly on the federal government's performance management website: www.performance.gov.

In addition, CESER has measured and reported on impacts and outcomes in a 2018 report titled *From Innovation to Practice: Re-Designing Energy Delivery Systems to Survive Cyber Attacks*, which is posted on the Department of Energy's website: <https://www.energy.gov/ceser/articles/ceds-rd-innovation-practice-redesigning-energy-delivery-systems-survive-cyber>.

The report describes technologies that CESER developed and transitioned to the Energy Sector. Utilities nationwide have purchased risk-reducing technologies developed through this CESER-funded research.

**House Energy and Commerce Committee
Subcommittee on Oversight and Investigations
May 16, 2023, Hearing**

Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies

Questions for the Record Submitted to Mr. Puesh Kumar

- Q4. What are the main challenges and gaps that hinder effective collaboration and information sharing between SRMAs and private sector stakeholders on cyber-physical threats and incidents, and what are you doing to address them?
- A4. Consistent with Presidential Policy Directive 21 and the Homeland Security Act of 2002, the Secretary of Homeland Security, through the Cybersecurity and Infrastructure Security Agency, is tasked with coordinating a national effort to secure and protect against critical infrastructure risks. Sector Risk Management Agencies, such as the Department of Energy, coordinate with the Department of Homeland Security and critical infrastructure owners and operators to improve collaboration and information sharing. As the U.S. energy sector and our energy systems evolve, grow, and deploy new technologies, they face persistent cyber and physical threats from a variety of sources including nation-states, criminals, and other malicious actors — threats that the federal government and industry each have unique, critical, and complementary roles in addressing. Given that much of the Nation’s energy infrastructure is privately-owned, meeting the shared responsibility to address these issues requires government and industry to work hand-in-hand.

CESER leads DOE’s risk management coordination activities, including the Energy Threat Analysis Center (ETAC) Pilot which brings experts from the federal government and the energy sector together to address threats to the energy system. The ETAC Pilot addresses several long-standing challenges, including the need for intentional and ongoing integration of government and energy sector risk expertise, formalized/institutionalized collaboration on energy threat assessment at the operational level, two-way sharing of relevant and timely threat information, prioritization of energy sector risks informed by both government and private sector perspectives, and the development of collective mitigations for known risks to the energy sector.

House Committee on Energy and Commerce
Oversight & Investigations Subcommittee Hearing
“Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies” May 16, 2023

Questions for the Record submitted for **Brian Mazanec**, Ph.D., Deputy Director, Office of Preparedness, Administration for Strategic Preparedness and Response, Department of Health and Human Services

The Honorable H. Morgan Griffith

1. Late last year, the Cybersecurity Infrastructure & Security Agency (CISA) released its new Cross-Sector Cybersecurity Performance Goals (CPGs), a foundational set of information technology and operational technology practices and recommendations intended to help smaller, lesser-resourced organizations better prioritize cybersecurity efforts and reduce risk. It is the Committee’s understanding that CISA stated at the time that it was going to work with Sector Risk Management Agencies (SRMAs) to develop sector-specific CPGs.

a. Has the Department of Health and Human Services (HHS) engaged CISA on developing these sector specific CPGs, and if so, how are those efforts progressing? When should we expect them to be done?

Response: In 2017, HHS published the Health Industry Cybersecurity Practices (HICP) document that identified key threats and mitigation practices specific to the Healthcare and Public Health Sector. This document was refreshed and published in April 2023 with updated information acknowledging the changes in the sector and threats since 2017. As one of the cornerstone documents for health care cybersecurity, the HICP is becoming widely acknowledged and implemented by the HPH Sector as evidenced by the data outlined in the Hospital Resiliency Landscape Analysis.

Related to the development of CPGs, in March 2023, CISA published an update to the CPGs. The CPGs are intended to be a baseline set of cybersecurity practices broadly applicable across critical infrastructure. The CPGs provide a prioritized set of security practices for information technology (IT) and Operational Technology (OT) owners. The CPGs were a direct response to the challenge identified in National Security Memorandum (NSM)–5: *Improving Cybersecurity for Critical Infrastructure Control Systems* to develop baseline cybersecurity goals that are consistent across all critical infrastructure sectors. HHS is currently coordinating with CISA to ensure that all sector-specific CPGs are aligned in intent and messaged in a consistent manner with the HICP and other sector-specific resources to reduce confusion or fatigue within the HPH Sector. Coordination activities between CISA and HHS on this initiative is in the early stages.

b. How is HHS using CISA’s cross-sector CPGs to drive security improvements in the healthcare and public health sector?

Response: In 2017, HHS published the Health Industry Cybersecurity Practices (HICP) document that identified key threats and mitigation practices specific to the Healthcare and Public Health (HPH) Sector. This document was refreshed in 2023 with updated information acknowledging the changes in the sector and threats since 2017. As one of the cornerstone documents for health care cybersecurity, the HICP is widely acknowledged by the HPH Sector. Due to the existence of the HICP and the overall consistency between the HICP and the CPGs, the HPH Sector continues to rely primarily on the specialized HICP document to provide specific recommendations to the sector.

2. How do you measure and report on the impact and outcomes of your cybersecurity initiatives and investments on cyber-physical systems in critical infrastructure?

Response: To support development of a baseline of cyber capabilities across the sector, HHS recently released the Hospital Resiliency Landscape Analysis in April 2023. This document was developed in partnership with the Health Sector Coordinating Council (HSCC) and includes an identification of the biggest threats facing hospitals as well as an assessment of cybersecurity capabilities relative to commonly accepted cybersecurity practices. This document also offers a window into how the sector is adopting and implementing the cybersecurity best practices as outlined by HICP. While early and limited in scope, this iteration of the Landscape Analysis is a baseline and we are in early discussions on how to expand and build upon this effort. HHS sees this analysis as a fundamental way we can measure the impact and outcomes of our efforts.

In parallel, ASPR is developing version 2.0 of the Risk Identification and Site Criticality Toolkit (RISC Tool), which supports an all-hazards, objective, data-driven risk assessment for the HPH Sector. The RISC Tool includes an assessment on cybersecurity, closely aligning to the NIST Cybersecurity Framework. Version 2.0 is planned to launch in the fall of 2023 and will provide a source of data to HHS for measuring impact and outcome of activities through the analysis of voluntary self-reported risk assessment data.

Lastly, within the HPH Sector Joint Cybersecurity Working Group, there is Measurement Task Group focused on understanding current state and changes in cybersecurity posture within the HPH Sector. Though this Task Group's work is still in its nascent stage, it will help drive strategies and activities to measure progress across the sector with respect to cybersecurity.

3. What are the main challenges and gaps that hinder effective collaboration and information sharing between SRMAs and private sector stakeholders on cyber-physical threats and incidents, and what are you doing to address them?

Response: HHS is working diligently to strengthen cybersecurity and address the impacts of cyberattacks on the health care system. As we move forward, there are additional authorities and resources that would advance ASPR's ability to fully implement its plan to bolster HHS's cyber SRMA activities. For example, we are in the process of establishing a dedicated Cyber Division within ASPR's Office of Critical Infrastructure Protection. If ASPR is granted direct hire authority, as requested in the FY 2024 President's Budget, we would be able to bring critical staff with cyber expertise into the organization more quickly and move forward to directly support and aid preparedness, response, and recovery activities without delay. We would also be better positioned to immediately expand and enhance our efforts as the SRMA lead for the HPH sector. Additionally, we are looking to establish a new HHS cyber incident ticketing system to better track incidents and strengthen threat intelligence sharing through embedded liaisons within CISA and the FBI. Dedicated resources are needed to implement and operate supporting systems, as included in the FY 2024 President's Budget request. A key limitation on the ability for sector entities to share information with the government is the fear of litigation from customers, we have heard from sector stakeholders that this is a key reason for not sharing information. Additionally, sector stakeholders need additional reassurance that information shared with the department for security sharing purposes is not then used for regulatory reasons.