Diversified Reporting Services, Inc.

RPTS TARDIEU

HIF136020

PROTECTING CRITICAL INFRASTRUCTURE FROM CYBERATTACKS: EXAMINING EXPERTISE OF SECTOR SPECIFIC AGENCIES

TUESDAY, MAY 16, 2023

House of Representatives,

Subcommittee on Oversight and Investigations,

Committee on Energy and Commerce,

Washington, D.C.

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

Present: Representatives Griffith, Guthrie, Duncan, Palmer, Lesko, Crenshaw, Cammack, Rodgers (ex officio); Castor, DeGette, Schakowsky, Tonko, Ruiz, Peters, and Pallone (ex officio).

Also present: Representative Kelly.

Staff present: Sean Brebbia, Chief Counsel; Sarah Burke, Deputy Staff Director; Jerry Couri, Deputy Chief Counsel; Lauren Eriksen, Clerk; Christen Harsha, Senior Counsel; Tara Hupman, Chief Counsel; Peter Kielty, General Counsel; Emily King, Member Services Director; Chris Krepich, Press Secretary; John Strom, Counsel; Joanne Thomas, Counsel; 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 Monfort, 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 five minutes for an opening statement.

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 cyberattacks 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 cyberattack 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 cyberattacks.

For example, the Director of National Intelligence reported that China is almost certainly capable of launching cyberattacks 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 cyberthreat 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 cyberthreats. 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:]

**********COMMITTEE INSERT**********

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

*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 cyberattacks 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 cyberattacks. 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 neighbor's 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 cyberattacks 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 cyberthreats and the risks that they pose.

Many critical infrastructure organizations can take steps to prepare for and prevent cyberattacks. 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 cyberthreats and can use their existing regulatory authorities to make sure that counter measures reach the organizations that need them the most. And 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 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 cyberthreats, 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 cyberthreats, 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 INSERT**********

*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 five minutes.

*The Chair. Thank you, Chair Griffith. Today we are here to learn more about cyberattacks 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 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 percent of electricity, oil and gas, and manufacturing firms experienced cyberattacks affecting population and energy supply over the previous 12 months.

Securing our critical infrastructure from cyberthreats 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 cyberthreats 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 cyberattacks 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 foraging 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.

Cyberthreats 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 The Chair follows:]

**********COMMITTEE INSERT**********

*The Chair. 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 five-minute opening statement.

*Mr. Pallone. Thank you, Mr. Chairman. 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 patient's Social Security numbers, test results, and diagnosis, and prescription history. And then earlier this year, the personal healthcare information of members and staff was stolen when D.C. Health Link was breached.

Cyberthreats to critical energy, water, and health infrastructure are unfortunately becoming more common and attacks are more costly. In 2022, hundreds of cyberattacks 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 cyberattacks every year~~,~~. W~~but~~hile many of these attacks are unsuccessful thanks to the cyber defenses these companies have established~~, .~~

~~S~~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 cyberattacks. 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 Republican's Default of America Act threatens indiscriminate cuts to federal agencies overseeing infrastructure. I'm concerned that it could seriously hamstrung cybersecurity efforts at a time when we must be

ramping up our defenses against cyberthreats 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 INSERT**********

*Mr. Pallone. So with that, Mr. Chairman, thank you, and I yield back.

*Mr. Griffith. Thank the gentleman for yielding back. That concludes member's 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 five 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 five-minute opening statement.

TESTIMONY 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, OFFICE OF GROUNDWATER AND DRINKING WATER, OFFICE OF WATER, ENVIRONMENTAL PROTECTION AGENCY

TESTIMONY 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 cyberthreats 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 five 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 cyberthreats 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 testimony of Mr. Kumar follows:]

**********COMMITTEE INSERT**********

*Mr. Griffith. Thank you so much. I now recognize Dr. Mazanec for his five minutes of opening statement.

TESTIMONY OF BRIAN MAZAENC, 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 cyberattacks. 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 cyberattacks that exploit complex hospital infrastructures, underfunded cybersecurity functions, and numerous vulnerable legacy metal -- medical devices. These cyberattacks against the sector are growing both in number and severity.

The frequency of cyberattacks 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 cyberattacks against hospitals not only affect the targeted institution but have a blast radius-like 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 cyberthreats and strengthens the Healthcare and Public Health Sector's cyber security posture. Doing so is critical as cyberattacks 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 department, 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 cyberthreats 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 cyberattacks 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 testimony of Dr. Mazanec follows:]

**********COMMITTEE INSERT**********

*Mr. Griffith. Thank you so much. Now I recognize Mr. -- Dr. Travers for his five-minute opening statement.

TESTIMONY 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 cyberattacks. This mission is among EPA's highest Homeland Security priorities.

Water systems are frequently targeted for cyberattacks 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, cyberattacks 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 cyberattacks. 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 eight 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 systems which have exploited the failure to implement cybersecurity best practices.

Due to this continued vulnerability, the increasing frequency of cyberattacks on critical infrastructure facilities as reported by the FBI and DHS, and the public health risk of a cyberattack 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 cyberthreats. 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:]

**********COMMITTEE INSERT**********

*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 five minutes.

Dr. Mazanec, as you discussed in your testimony, hospital's 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 cyberattack 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 under-resourced 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 cyberattack 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 pre-existing 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 cyberattack 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 five 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 cyberattack 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 cyberattacks 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 cyberthreats, 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 cyberattack? 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 cyberattack?

*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. Its 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 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 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 company -- 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. Yeah, get Energy next. First it's going to be Health.

*Mr. Guthrie. First it will be Health.

*Mr. Griffith. Mr. Guthrie of Kentucky, five 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. Okay, 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. Okay. 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 quarterback-like 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. Okay, 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 cyberthreats. Water -- small water systems generally lack capacity of larger water systems, for example. You can expect a larger water system, for example, to have a 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 five 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 cyberthreats, and how is that -- 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 cyberthreats on their individual networks, we're seeing cyberthreats 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 cyberthreats, 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 cyberthreats 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 five 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 1 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 cyberthreats 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. Yeah, 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 cyberattacks. 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. Yeah. 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 five 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, cyberattacks 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 -- 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 cyberattacks?

*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 cyberattacks?

*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 five 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 co-lead 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. Yeah, 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 Blackberries' most recent

Global Threat Intelligence Report, which I have right here, the U.S. electric and gas industries have been targeted by cyberattacks in the last six 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 cyberthreats to the U.S. Energy Sector?

*Mr. Kumar. Representative, as you alluded to, the cyberthreat 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 cyberthreats 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 cyberattacks 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 cyberthreats 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 five 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. Cyberattacks are on the rise and on pace to shatter record setting numbers. In the last five 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 cyberattacks. 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 ~~L~~living in the desert with 116 degrees, the lack of water or undrinkable water is an emergency, okay. Unfortunately, smaller water systems ~~have~~ that serve~~d~~ 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 cyberattacks.

So, Dr. Travers, can you provide examples how the EPA has helped smaller and under-resourced 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, those 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. Yeah, thank you.

*Dr. Travers. Yeah.

*Mr. Ruiz. Thank you. A robust well-trained workforce is essential to preparing for and responding to cyberattacks 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 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. -- 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. Yeah, 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.

*The Chair. 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 cyberthreats, 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.

*The Chair. Thank you.

*Dr. Mazanec. Thank you very much for the question. So HHS, similar to the Department of Energy, participated in the interagency 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.

*The Chair. 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.

*The Chair. Okay, 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.

*The Chair. Thank you.

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

*The Chair. 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 five 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 expertise 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 cyberattacks.

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 eight 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 a ~~tax~~ttacks before they impact public safety. Cyberthreats 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 stilled 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 bipartisanship 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 five 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. Manzanec, did I get it right?

*Dr. Mazanec. Almost. Mazanec.

*Mrs. Cammack. Mazanec, okay. 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 cyberthreat 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 dollars 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 cyberthreats, 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 five minutes of questions.

*Mr. Peters. Thank you, Mr. Chairman.

I~~'ll~~ follow-up somewhat on Ms. 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, ~~the~~ 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 cyberattack 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 cyberattack 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 Scripts 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. -- 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 a -- in a 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 it not static here --

*Mr. Peters. Right.

*Dr. Mazanec. -- 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 five 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 cyberattack 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 cyberattacks, 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 American's 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, yeah, 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. Yeah, 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 five 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 cyberattack?

*Dr. Mazanec. Thank you, Congressman. So HHS brings a lot to the table in our SRMA responsibilities here working with the sector, 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-Cyberattack 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. Yeah.

*Dr. Mazanec. -- 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, 911, 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 cyberattacks. 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. Yeah.

*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. Yeah, but --

*Dr. Mazanec. -- 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 cyberattacks 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. Okay, so two problems that need to be fixed.

Mr. Kumar, the deal you announced last year that they're putting 45 million dollars 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. -- for cyber defense companies to create the tools -- okay.

*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 five 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~~ In 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 cyberattacks 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. Yeah, ~~M~~my district is urban, suburban, and rural. I start in Chicago and go three 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 context, 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 4:19 p.m., the subcommittee was adjourned.]