MEMORANDUM

To: Republican Members and Staff, Subcommittee on Oversight and Investigations

From: Majority Committee Staff

Re: Oversight and Investigations Subcommittee Hearing, "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies."

Please note that this memo is for internal use only and should not be shared with anyone outside of Energy and Commerce Republican Member offices.

On Tuesday, May 16, 2023, at 2:00 p.m. (ET) in 2123 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled, "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies."

I. WITNESSES

- *Puesh Kumar*, Director, Office of Cybersecurity, Energy Security, and Emergency Response, Department of Energy
    - According to the Department of Energy (DOE), Director Kumar has over 15 years of experience in grid modernization, cybersecurity, and emergency response in both government and the private sector.[1]
    - His testimony is expected to address evolving cyber threats, the DOE's cybersecurity roles and responsibilities, partnerships and initiatives including other agencies and industry, new research and development activities, and the DOE's implementation of the Infrastructure Investment and Jobs Act (IIJA).[2]

- *David Travers*, Director, Water Infrastructure and Cyber Resilience Division, Office of Groundwater and Drinking Water, Office of Water, Environmental Protection Agency
    - Director Travers is expected to discuss the Environmental Protection Agency's (EPA) plans for IIJA funds, technical assistance and grants for water systems and other partners, and its recent interpretive rule, *Evaluating Cybersecurity During Public Water Sanitary Surveys*.[3]

---

[1] DEP'T OF ENERGY, *Puesch Kumar*, https://www.energy.gov/ceser/person/puesh-kumar (last visited May 11, 2023).
[2] *See Full Committee Hearing to Examine Cybersecurity Vulnerabilities to the United States' Energy Infrastructure: Hearing Before the S. Comm. on Energy and Natural Res.*, 118th Cong. (2023) (statement of Puesh Kumar, Director, Office of Cybersecurity, Energy Security, and Emergency Response), *available at* https://www.energy.senate.gov/services/files/7C2EC274-467C-4444-BD14-D4F11E474492.
[3] ENVTL. PROT. AGENCY, *Addressing PSW Cybersecurity in Sanitary Surveys or an Alternate Process*, Mar. 3, 2023, *available at* https://www.epa.gov/system/files/documents/2023-

- *Brian Mazanec*, PhD, Deputy Director, Office of Preparedness, Administration for Strategic Preparedness and Response, Department of Health and Human Services.
    - Prior to joining the Department of Health and Human Services (HHS), Deputy Director Mazanec served as the Director of the Defense Capabilities and Management team at the Government Accountability Office (GAO).[4]
    - His testimony is expected to discuss emerging threats to healthcare infrastructure, the HHS's coordination with private sector entities, and its recently released cybersecurity resources.[5]

II. HEARING GOALS

Both Republican and Democratic Members will likely share concerns about the increasingly complex risk of cyberattacks on critical infrastructure. There will likely be bipartisan support for the represented agencies coordinating with relevant stakeholders and critical infrastructure owners and operators. This hearing provides Members an opportunity to do the following:

- Reinforce the importance of Sector Risk Management Agencies (SRMA) such as the DOE, EPA, and HHS to federal efforts to secure critical infrastructure against cyberattacks.

- Gather information on the roles of the three Sector Risk Management Agencies (SRMA) and how they fit into the federal cybersecurity scheme.

- Inquire about coordination between the SRMAs, given the interconnected nature of critical infrastructure.

- Explore how these SRMAs collaborate with critical infrastructure owners and operators and other stakeholders and identify opportunities for them to be more effective and helpful partners.

- Examine federal cybersecurity support programs and initiatives, such as financial awards and technical assistance, including the DOE and EPA's use of related IIJA funding.

03/Addressing%20PWS%20Cybersecurity%20in%20Sanitary%20Surveys%20Memo_March%202023.pdf [hereinafter EPA Memo]; Envtl. Prot. Agency, EPA 817-B-23-001, Evaluating Cybersecurity During Public Water System Sanitary Surveys (Mar. 2023), *available at* https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf [hereinafter EPA Guidance].

[4] GEORGE MASON UNIV., *Brian M. Mazanec*, https://schar.gmu.edu/profiles/brianmazanec (last visited May 12, 2023).

[5] DEP'T OF HEALTH AND HUMAN SERVS., *HHS Cybersecurity Task Force Provides New Resources to Help Address Rising Threat to Cyberattacks in Health and Public Health Sector*, Apr. 17, 2023, https://www.hhs.gov/about/news/2023/04/17/hhs-cybersecurity-task-force-provides-new-resources-help-address-rising-threat-cyberattacks-health-public-health-sector.html.

III. ADDITIONAL BACKGROUND AND RECENT DEVELOPMENTS

1. Recent Administration Activities

- On March 2, 2023, the Biden Administration released its National Cybersecurity Strategy.[6] It contains four "pillars," including "Pillar One: Defend Critical Infrastructure." Within this pillar, the strategy includes five objectives.[7]

- The Biden Administration stated it is reviewing and planning to revise Presidential Policy Directive-21.[8]

2. Government Accountability Office Review

- High-Risk List: The Government Accountability Office (GAO) lists "Ensuring the Cybersecurity of the Nation" as one of its "High-Risk Areas Needing Significant Attention."[9] The GAO has issued many reports and recommendations in this area.[10]

- Review of National Strategy: Additionally, the GAO found that the national strategy discussed above does not contain all of the ideal components of a national strategy, lacking milestones, performance measures, resources needed to accomplish goals, and fully defined roles and responsibilities.[11] The GAO found that, "Until the implementation plan is developed and contains the missing characteristics of a robust national strategy, overall progress in strengthening cybersecurity will remain limited."[12]

3. Department of Energy

- Other relevant entities**:** Members should be aware that several additional entities play roles in securing energy infrastructure. For example, the Federal Energy Regulatory Commission (FERC) has jurisdiction over reliability standards for the bulk-power system, the facilities and control systems part of the interconnected electric transmission

---

[6] EXEC. OFFICE OF THE PRESIDENT, *Fact Sheet: Biden-Harris Administration Announces National Cybersecurity Strategy*, Mar. 2, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.
[7] EXEC. OFFICE OF THE PRESIDENT, NATIONAL CYBERSECURITY STRATEGY 7-13 (2023), *available at* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[8] Tim Starks, *A Presidential Critical Infrastructure Protection Order is Getting a Badly Needed Update, Officials Say*, WASH. POST, May 11, 2023, https://www.washingtonpost.com/politics/2023/05/11/presidential-critical-infrastructure-protection-order-is-getting-badly-needed-update-officials-say/; EXEC. OFFICE OF THE PRESIDENT, *Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure*, Nov. 7, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure/.
[9] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-23-106686, HIGH RISK SERIES: EFFORTS MADE TO ACHIEVE PROGRESS NEED TO BE MAINTAINED AND EXPANDED TO FULLY ADDRESS ALL AREAS 10 (2023).
[10] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, *Cybersecurity*, https://www.gao.gov/cybersecurity (last visited May 11, 2023).
[11] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 9, at 11-12.
[12] *Id.*

network.[13] FERC has certified the North American Electric Reliability Corporation as the organization responsible for developing these standards.[14] Additionally, while DOE operates some pipeline security programs, the Department of Homeland Security's (DHS) Transportation Security Administration possesses regulatory authority over pipeline cybersecurity.[15]

- Infrastructure Investment and Jobs Act Implementation:[16] According to the DOE, the IIJA provided to it $27 billion to upgrade and modernize the electric grid, including its resistance to cyberattacks.[17] Its Office of Cybersecurity, Energy Security, and Emergency Response states it will lead the implementation of the following provisions: State Energy Security Plans (sec. 40108); Enhancing Grid Security Through Public-Private Partnerships (sec. 40121(c)); Energy Cyber Sense (sec. 40122); Rural and Municipal Utility Advanced Cybersecurity Grants and Technical Assistance (sec. 40124); Cybersecurity for the Energy Sector Research, Development, and Demonstration (sec. 40125(b)); Energy Sector Operational Support for Cyberresilience (sec. 40125(c)); and Modeling and Assessing Energy Infrastructure Risk (sec. 40125(d)).[18]

- Electric Grid Distribution Systems: The GAO has flagged that the country's grid distribution systems, which are primarily regulated by states, increasingly face a risk of cyberattacks.[19] In a 2021 report, the GAO found that while DOE developed plans to help combat these threat, it should more fully coordinate with the DHS, states, and industry to more address the risk of cyberattacks for the grid's distribution system.[20]

2. Environmental Protection Agency

- Office of the Inspector General Concerns: The America's Water Infrastructure Act (AWIA) amended section 1433 of the Safe Drinking Water Act to require water systems serving more than 3,300 people to assess the risk of malevolent acts and natural hazards to that system and develop an emergency response plan.[21] The EPA bears responsibility for overseeing and enforcing water systems' AWIA compliance.[22] Water systems must

[13] Federal Power Act § 215.
[14] *See id*.; RICHARD J. CAMPBELL, CONG. RESEARCH SERV., R45312, ELECTRIC GRID CYBERSECURITY 2-3 (2018).
[15] PAUL W. PARFORMAK & CHRIS JAIKARAN, R46903, CONG. RESEARCH SERV., PIPELINE CYBERSECURITY: FEDERAL PROGRAMS 6-7 (2018).
[16] Pub. L. No. 117-58.
[17] DEP'T OF ENERGY, *Office of Cybersecurity, Energy Sec., and Emergency Response, Bipartisan Infrastructure Law Implementation*, https://www.energy.gov/ceser/bipartisan-infrastructure-law-implementation (last visited May 11, 2023).
[18] *Id.*
[19] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-23-106441, CYBERSECURITY HIGH-RISK SERIES: CHALLENGES IN PROTECTING CYBER CRITICAL INFRASTRUCTURE 1 (2023).
[20] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-21-81, ELECTRIC GRID CYBERSECURITY: DOE NEEDS TO ENSURE ITS PLANS FULLY ADDRESS RISKS TO DISTRIBUTION SYSTEMS (2021).
[21] OFFICE OF THE INSPECTOR GEN, ENVTL. PROT. AGENCY, REPORT NO. 23-P-0003, THE EPA MET 2018 WATER SECURITY REQUIREMENTS BUT NEEDS TO IMPROVE OVERSIGHT TO SUPPORT WATER SYSTEMS COMPLIANCE 2 (2022).
[22] *See id.* at 2-3.

also review their risk and resilience assessments at least once every five years. The Office of the Inspector General (OIG) found that the EPA needs to improve its oversight of water system compliance and noted several oversight weaknesses that contributed to noncompliance by water systems, including the EPA's lack of: (1.) accurate water system contact information; (2.) needed resources; and (3.) transparent communication and formal guidance. The OIG issued four recommendations to the EPA: (1.) update and implement a plan supporting AIWA compliance; (2.) update its process to track accurate water system contact information and AIWA noncompliance; (3.) review risk assessments and emergency response plans to pinpoint areas for improvement; and (4.) develop guidance on AIWA compliance.[23] As of May 5, 2023, the OIG considers these recommendations unresolved.[24]

- Recent Interpretive Rule: On March 3, 2023, EPA issued an interpretive rule consisting of a memorandum and guidance, indicating that EPA maintains that states must assess cybersecurity resilience when conducting sanitary surveys, or periodic audits of water systems.[25] However, some stakeholders have expressed concerns that EPA did not comply with federal laws and regulations governing the burden of information requests on the public, and that EPA did not follow proper rulemaking procedures.[26] Additionally, this interpretive rule applies the sanitary survey requirements for cybersecurity to *all* public water systems, rather that only those subject to the requirements to conduct risk and resilience assessments and prepare an emergency response plan under the America's Water Infrastructure Act of 2018 (community water systems serving over 3,300 people).[27]

3. Department of Health and Human Services

- Additional Resources: On April 17, 2023, the Department of Health and Human Services issued three resources to address cybersecurity risks in the Health and Public Health Sector:[28]
    - Knowledge on Demand:[29] online educational platform containing free cybersecurity trainings for health and public health organizations.
    - Health Industry Cybersecurity Practices:[30] publication developed for stakeholders that contains best practices.

[23] *Id.* at 10-11.
[24] Memorandum from Sean O'Donnell, Inspector Gen., Envtl. Prot. Agency, to Radhika Fox, Assistant Administration, Office of Water, Envtl. Prot. Agency, May 5, 2023.
[25] *See* EPA Guidance, *supra* note 3; EPA Memo *supra* note 3.
[26] *See, e.g.*, Letter from Am. Water Works Assoc., and U.S. Conference of Mayors, to, Michael Reagon, Administrator, Envtl. Prot. Agency, and Richard Revesz, Admin., Office of Info. and Reg. Affairs, Apr. 24, 2023; Am. Water Works Assoc., States Directed to Assess Cybersecurity in Sanitary Surveys, Mar. 3, 2023, https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance.
[27] *See* EPA Memo, *supra* note 3 (emphasis added).
[28] DEP'T OF HEALTH AND HUMAN SERVS., *supra* note 5.
[29] DEP'T OF HEALTH AND HUMAN SERVS., *Knowledge on Demand*, https://405d.hhs.gov/knowledgeondemand (last visited May 12, 2023).

- Hospital Cyber Resiliency Initiative Landscape Analysis:[31] report on domestic hospitals' current cybersecurity preparedness, including a review of certain hospitals against standard guidelines.

III. STAFF CONTACT

For questions regarding this hearing, or if you would like assistance drafting questions on a particular topic within the scope of the hearing, please contact Christen Harsha of the Committee staff at (202) 225-3641.

---

[30] HEALTHCARE & PUBLIC HEALTH SECTOR COORDINATING COUNCIL, HEALTH INDUSTRY CYBERSECURITY PRACTICES: MANAGING THREAT AND PROTECTING PATIENTS 2023 (2023), *available at* https://405d.hhs.gov/Documents/HICP-Main-508.pdf.

[31] DEP'T OF HEALTH AND HUMAN SERVS., HOSPITAL CYBER RESILIENCY INITIATIVE LANDSCAPE ANALYSIS (2023), *available at* https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf.