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

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

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

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

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

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

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

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

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

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

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

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

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

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

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