CHAIRMAN DANE MAXWELL
MISSISSIPPI PUBLIC SERVICE COMMISSION
SOUTHERN DISTRICT

CONTACT:
Caroline Nettles
Communications Director
Caroline.nettles@psc.ms.gov
(601) 540-5938

March 1, 2022

PSC Chairman Dane Maxwell Statement on Cybersecurity for Critical Infrastructure in MS

As many of you know, I am a former Marine and as a Marine, it was my job to protect against physical attacks. That was my former job, but as you know, I will always be a Marine. In my current job, it is my business to protect against attacks not only physical in nature, but also silent and covert assaults, such as cyber-attacks.

It is no secret to anyone in this room that Russia preceded the attack on Ukraine, with cyber-attacks. Now, the cybersecurity and infrastructure security agency (a federal agency that seeks to improve cyber security readiness) has issues a "shields-up" warning, urging organizations to reduce their chances of a cyberattack and ensure they are prepared for a breach in our homeland. The threat for cyber intrusions from Russia is becoming more of a possibility for local organizations and businesses. This is not the only source calling out for caution.

North Carolina State cyberwarfare expert Jack Shanahan said the attacks could be as minimal as "denial of service" attacks but could grow significant enough to impact our country's most critical infrastructure like financial networks, transportation networks, energy systems, and energy networks.

According to U.S. Department of Energy Secretary Jennifer Granholm, enemies of the United States have the capability to shut down the U.S. power grid, and "there are very malign actors trying, even as we speak." As grid modernization progresses, opportunities for malicious conduct increase. But the energy grid is not the only vulnerable asset related to utility infrastructure. Last year, hackers took down the largest fuel pipeline in the United States, owned by Colonial Pipeline Company, causing fuel shortages across the East Coast. Experts also have concerns about the vulnerability of water and wastewater systems.

In October of 2020, Governor Tate Reeves signed his first Executive Order, Executive Order 1456, which created a task force of state cybersecurity. The task force is led by Attorney General Lynn Fitch, and its members were appointed by the Governor. The task force is directed and empowered to primarily focus on the needs and protections of state agencies. Both Governor Reeves and Attorney General Fitch are to be commended for their efforts to protect Mississippians from cyber events.

CHAIRMAN DANE MAXWELL
MISSISSIPPI PUBLIC SERVICE COMMISSION
SOUTHERN DISTRICT

At the Mississippi Public Service Commission, we are charged to do more. We must focus our efforts on mitigation of risks and vulnerabilities as they apply to the electric grid, natural gas pipelines, and regulated critical infrastructure. We must do all we can to ensure reliability for Mississippians.

While state commissioners have not historically regulated or established rules or procedures in this area, many now are focusing their attention on vulnerabilities in public utility infrastructure and are working to identify cybersecurity measures that would most effectively mitigate such vulnerabilities and risks. Urgent priorities include strengthening existing protections- for the generation and distribution system as well as the overall power system, natural gas systems, and other regulated infrastructure; enhancing coordination at all levels; and accelerating the development of robust protocols for response and recovery in the event of a successful attack.

It is for these reasons, that in the coming weeks, I will be sitting down with the colleagues to discuss how best to proceed, to adequately protect Mississippians from outside cyberattacks on our critical infrastructure. We do not know when an event might occur, but we do know is that there are bad actors out there, and the result of an attack can be catastrophic.

###