



October 23, 2020

Contact: Matt Skinner, Public Information Manager

405-521-4180

matt.skinner@occ.ok.gov

What Can Go Wrong...

State agencies, private sector join to prepare for cyber-attack

Officials are reviewing the lessons learned from the first of what is anticipated to be an annual cyber and energy security exercise involving government agencies and the private sector in Oklahoma.

Focusing on response to a cyber-attack that impacts utility and other energy services as well as local and state government services, the exercise involved the Oklahoma Office of Emergency Management (OEM), the Office of Management and Enterprise Services (OMES), and the Oklahoma Corporation Commission as participants, with state utilities, various state agencies and the offices of the Oklahoma Secretary of Energy and Environment and Oklahoma Secretary of Digital Transformation and Administration as observers.

Oklahoma Corporation Commissioner Dana Murphy said the exercise adds critical items to the list of potential disasters for which Oklahoma must be prepared.

"Oklahoma's expertise in dealing with natural disasters is well proven and has been praised by other states," Murphy noted. "Now we must apply that expertise to the new possibility of a man-made disaster impacting the fairly new nexus of cyber security, energy security and government services. I am pleased that the introductory exercise showed that while we must never stop learning, the vast experience of those involved in the state's emergency response effort served as a great foundation for effective responses to new threats."

(more)

(Exercise – pg. 2)

Oklahoma Secretary of Energy and Environment Kenneth Wagner said such exercises are crucial.

“In today’s ever-changing technological landscape, it is absolutely essential that Oklahoma is prepared and ready to respond to a cyber-attack that would impact our state’s critical infrastructure,” Wagner said. “Our office strongly supports the efforts of our various state agencies and industry partners in being prepared to work collaboratively to respond to any cyber event. Exercises such as this teach us valuable lessons on where we can strengthen our levels of expertise and communication during times of crisis. We look forward to participating in additional exercises in the future.”

Oklahoma Secretary of Digital Transformation and Administration David Ostrowe said the exercise addressed a top priority.

“There is no free lunch. Every advancement in technology not only brings with it great advantages, but also new risks that must be addressed,” Ostrowe said. “We must be on the cutting edge when it comes to preparing for and responding to those risks, particularly when it comes to the interplay between cybersecurity and energy.”

The exercise, conducted virtually October 15, was planned by state officials and former Oklahoma Energy and Environment Secretary Michael Teague, who worked with the Norwich University Applied Research Institutes (NUARI). NUARI has been conducting cyber-security exercises nationwide for 15 years. This is the first time NUARI has worked with Oklahoma and the first time it has included energy security as part of a cyber exercise. The Oklahoma exercise was funded through a federal Department of Homeland Security grant.