COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Subcommittee Hearing Statement of Chairman Bennie G. Thompson (D-MS)

Building on our Baseline: Securing Industrial Control Systems Against Cyberattacks

September 15, 2022

Operational technology underpins almost every aspect of how we live and work. From generating and distributing the electricity lighting this room, to ensuring that the water coming from the faucets is clean enough to drink, operational technology is the backbone of the national critical functions essential to public health, public safety, and national security. In the late summer, two "national critical functions" in Mississippi failed.

Jackson, Mississippi is in the midst of a water crisis, leaving over 100,000 of my constituents without a clean water supply or appropriately managed wastewater. They cannot use the water coming out of the faucets in their homes to brush their teeth, bathe, or wash the dishes. Tens of millions of gallons of untreated wastewater has flowed into Jackson-area waterways. Jackson schools had to revert to remote learning earlier this month because the toilets would not flush. Although the water crisis was not caused by a cyberattack, its horrific impacts and cascading consequences underscore the urgency of ensuring the safety, reliability, and functionality of the industrial control systems that support national critical functions. For me, the Jackson water crisis frames the way I think about today's hearing.

Since I became Chairman of the Committee again in 2019, I have expressed my concerns about the cybersecurity posture of the water sector, and I am pleased that we now have a President who has made improving it a priority. Earlier this year, the Full Committee received testimony from the American Water Works Association about the challenges facing municipal water authorities as they work to improve their cybersecurity and about the ICS Cybersecurity Initiative water "sprint." We learned that water authorities struggle to stretch their budgets to invest in cybersecurity, and that Federal support needs to be tailored to the existing maturity and resources of the sector.

A draft report on the convergence of operational and information technology by the National Security Telecommunications Advisory Committee released in August confirmed these findings. As the Committee continues its oversight of the Federal government's ICS security efforts, we are learning that stakeholders are eager to partner -provided that the government is collaborative and transparent. Toward that end, I have three goals for this hearing.

First, I am interested in knowing what support CISA has provided to the City of Jackson during the water crisis - including in helping the City understand the cascading effects of being without water. Second, I want to understand what CISA learned about the cybersecurity posture of the water sector through the ICS cybersecurity sprint, and what resources CISA brought to bear as it collaborated with the Environmental Protection Agency. Finally, I am interested in learning how CISA is encouraging ICS owners and operators to prioritize cybersecurity and resilience and invest in it accordingly.

I support the development of voluntary security guidelines, but they will only make us more secure if the private sector agrees to implement them. There are certain things the public should be able to rely on. Being able to drink the water coming out of the faucet is one of those things. If we are going to rely on voluntary security goals to protect ICS from cyberattacks, we must ensure that stakeholders are incentivized and able to implement them

# # #

Media contact: Adam Comis at (202) 225-9978