COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity, Infrastructure Protection, & Innovation Subcommittee Chairwoman Yvette Clarke (D-NY)

Building on our Baseline: Securing Industrial Control Systems Against Cyberattacks

September 15, 2022

I would like to thank the witnesses for participating in today's hearing on securing the industrial control systems at the heart of our nation's critical infrastructure. This is a topic that we, as lawmakers and Federal officials, don't spend nearly enough time talking about, working on, or funding. We rely on industrial control systems and other operational technology, or OT, to make sure we have power in our houses, clean water to drink, and countless other functions and services essential to our health, safety, and livelihoods. Still, questions about how we secure these critical OT systems tend to take a backseat to traditional IT security.

That is simply not an option in today's threat landscape – as OT grows increasingly connected to the internet, is more integrated with IT systems, and becomes a far more attractive target for cyber criminals and our adversaries. In an industrial environment, the risk of a cyber compromise is not limited to stolen customer data or reputational harm to a company. The consequences can be deadly. An OT disruption could hurt our communities, our economy, and even our national security. And yet, in a recent report, the National Telecommunications Security Advisory Committee, or NSTAC, found that our "biggest gap" in industrial cybersecurity is our "lack of urgency." The NSTAC's diagnosis was simple: "the U.S. has the technology and the knowledge to secure these systems but has not prioritized the resources" to do so.

In a hearing earlier this year, I said that the U.S. desperately needs to revamp its playbook for critical infrastructure cybersecurity. That is particularly true for OT security. Fortunately, I believe we are starting to see a shift in attitudes – and the Biden Administration is helping to lead that charge. In his first few months in office, President Biden launched a new ICS Cybersecurity Initiative – envisioned as a series of cybersecurity sprints – starting with the Electricity Subsector and then expanding to other sectors like pipelines and water. Last July, President Biden formalized this Initiative in a National Security Memorandum on Improving Control System Security.

The Memorandum also directed CISA to work with NIST on a set of cybersecurity performance goals to serve as clear guidance to operators about the level of security "the American people can trust and should expect for such essential services." This statement reflects a commitment to three principles that should underpin the Federal approach to OT security. First, the American people are entitled to trust that the services they have grown to rely on meet a reasonable, baseline standard of security and resilience. Second, critical infrastructure operators have a responsibility to earn and maintain the trust of the American people. And finally, the Federal government has a responsibility to bring its expertise, convening power, and resources to bear in support of this effort.

I am pleased to have the Federal government's lead 'convener' for critical infrastructure, and the principal architect of those baseline standards, CISA, on our panel today. I know CISA has been working

to complete the Common Baseline performance goals required by NSM-5, and I understand they will soon be finalized. I see these baseline standards as having real promise to reshape the OT security landscape – but they will only be as effective as CISA's ability to engage and incorporate the feedback they are hearing from stakeholders.

I am also pleased to have another leader in Federal OT cybersecurity here today – Idaho National Laboratory – to talk about how they're working to secure OT systems and support some of CISA's most critical OT programs, like CyberSentry, which I worked to codify last year. I would like to see this program grow and expand to new stakeholders, and I look forward to hearing how Congress can support that growth. I would also like to hear how CISA is targeting its efforts toward OT operators with the greatest need, and the fewest resources – for instance, small utilities or State and local governments.

In this Subcommittee, we often talk about the need to meet sectors where they are – recognizing their different security postures, resources, and expertise. That applies here as well. We need to do everything we can to make sure that efforts like the ICS sprints and the performance goals are designed to benefit all stakeholders – not just the most sophisticated. That will require the Administration to identify lessons learned, and apply them – for instance, to the upcoming chemical sector sprint. Finally, as we're shoring up these programs and ICS investments, I also want to hear how we're investing in our ICS security workforce – and doing so in a way that fosters diversity.

# # #

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