COMMITTEE ON HOMELAND SECURITY
Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrustructure Protection Subcommittee Ranking Member Eric Swalwell (D-CA)

Securing Operational Technology: A Deep Dive into the Water Sector

February 6, 2024

Everyday our adversaries grow bolder and more capable of exploiting vulnerabilities across operational technology (OT) networks. Just last week, Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly testified before another committee that CISA has observed a "deeply concerning evolution in Chinese targeting of US infrastructure" and that Chinese intrusions have already been eradicated across multiple sectors, including water.

Director Easterly's comments build on an advisory issued last year by the United States and its Five Eyes partners, which described the increasingly sophisticated and difficult to detect tactics of Chinese threat actor Volt Typhoon. The FBI announced last week that it had disrupted Volt Typhoon, and I commend them. But it doesn't change that fact the President Xi has been clear about his ambitions regarding Taiwan, and Director Wray has said that China will leverage its significant cyber arsenal to undermine the efforts of the U.S. and others who are interested in helping Taiwan preserve its democracy. China's hackers will continue to be a menace to U.S. critical infrastructure for years to come. But it isn't just China.

Late last year, Iranian hackers targeted and compromised water utilities across the country. And since at least 2018, CISA has been warning about Russian hackers targeting U.S. critical infrastructure, including the water, energy, nuclear, and aviation sectors. But China, Russia, and Iran are just the tip of the iceberg. Other nations are rapidly developing their capabilities, and that is to say nothing of cyber criminals looking to make a buck.

For too long, the Federal government has left critical infrastructure owners and operators on their own to defend against these sophisticated threat actors and failed to integrate the unique security concerns of OT in its guidance and programs. Even efforts to improve cyber workforce training overlooked the skills required to develop the OT security experts we will need as technology deployed across critical infrastructure networks continues to evolve.

I commend the Biden Administration for accelerating efforts to improve OT security across critical infrastructure networks. From expanding the CyberSentry program to signing into law legislation I drafted, the *Industrial Control Systems Cybersecurity Training Act,* President Biden and CISA are raising the bar on OT security. Despite this progress, our critical infrastructure networks are not as prepared or resilient as they need to be. Target-rich, resource-poor sectors - like the water sector - remain particularly vulnerable to cyberattack.

In my view, there are three things we can do that would have a meaningful impact on OT cybersecurity, particularly in target-rich, resource-poor sectors.

First, many critical infrastructure owners and operators lack the resources necessary to modernize and secure the technology they use. For the past two budget cycles, CISA has proposed a Critical Infrastructure Cybersecurity Grant Program, but it has never provided authorization language and Congress has never funded it. Moving forward we should explore opportunities to provide resources for critical infrastructure to improve cybersecurity – whether it is through grants or through a revolving fund program.

Second, we need to ensure that the programs, tools, and guidance CISA and its Federal partners are offering are accessible, usable, and provide security value to their full spectrum of stakeholders – from target-rich, resource-poor sectors to those who have been building cybersecurity capacity for decades. Too often, I have heard the Federal government's tools and services are too difficult to navigate and that it is too difficult to understand which are appropriate for a particular entity's needs.

Finally, we need to formalize CISA's approach to collaborating with the private sector to defend against threats to OT, including by authorizing the Joint Cyber Defense Collaborative. When it was first established, JCDC galvanized the public-private response to Log4j and Russia's invasion of Ukraine. Although JCDC continues to provide an important forum for public-private collaboration, there have been complaints that activity has slowed absent a momentum-driving – or formal authorization legislation - event to drive activity.

For over a year, I have been working on legislation to authorize JCDC, collecting and incorporating multiple rounds of feedback from both private sector and government partners. My legislation recognizes the potential of JCDC, and puts it on a path of realizing it.

Before I close, I would be remiss if I did not acknowledge an article I read in *Politico* yesterday regarding growing concerns about the value of JCDC. Many of the concerns raised in the story can and should be resolved by Congress stepping in to provide direction and accountability to JCDC through authorization – and that work is underway.

More concerning, however, is the apparently growing sentiment among some in the private sector that collaborating with CISA – and JCDC in particular – could put them in the "crosshairs" of conservative critics who buy the former President's election fraud claims and are therefore rethinking whether they should collaborate with government on cybersecurity issues. Given the pressing cyber threats facing the United States, we cannot allow for CISA's cybersecurity work to become politicized and the trusted partnerships the it has spent multiple Administrations cultivating to erode.

I look forward to working with my colleagues on legislative solutions to improve OT security, particularly in target-rich, resource poor sectors.

# # #

Media contact: Adam Comis at 202-225-9978