COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

The Cyber Talent Pipeline: Educating a Workforce to Match Today's Threats

July 29, 2021

A recent report by the cybersecurity firm Sonicwall found that ransomware attacks in North America increased 158 percent between 2019 and 2020. Another report by Comparitech found that cyber attacks against U.S. government organizations affected 71 million Americans and cost over $18 billion in downtime and recovery. The surge in cyberattacks against State and local governments, hospitals, and school districts, coupled with recent headlines about SolarWinds, Colonial Pipeline, and Kaseya have galvanized new calls to action to better defend the internet ecosystem.

I am encouraged by the momentum, and I am committed to putting more resources in the hands of State and local governments and improving CISA's awareness of malicious cyber activity through cyber incident reporting. But without a capable cyber workforce, all of our investments in tools and data will be in vain. The number of high-profile cyber incidents over the past year has emphasized just how essential cybersecurity has become. And the truth is the number of trained cybersecurity professionals has not increased to the levels necessary to meet the demand from industry and government. In fact, recent data show a deficit of over 460,000 trained cybersecurity professionals in the United States, relative to our current needs.

While the federal government has undertaken several initiatives in recent years to expand and better train our nation's cybersecurity workforce, we must do more. This hearing will give us an opportunity to hear from experts in the field who are working to educate the next generation of cybersecurity workers, so we can learn more about the programs that are currently in place and where greater investment is needed.

There is no silver bullet. We will need a multi-pronged approach that focuses on training the cybersecurity workforce of the future in schools and universities, re-skilling existing workers for the jobs that are currently available, and making sure we have the right training in place to address the disparate cybersecurity challenges in Information Technology and Operational Technology.

During my 15 years in Congress working on cybersecurity issues, I have heard consistently about the importance of prioritizing K-12 cyber education to grow and diversify the talent pipeline. Over that time, an entire generation of students has graduated high school and entered higher education or the workforce, and we still are behind where we need to be in including cyber education at the elementary and secondary level. However, CISA's Cybersecurity Education and Training Assistance Program, or CETAP has begun to show meaningful results.

I am glad Congress demonstrated support for CETAP by formally authorizing the program in last year's National Defense Authorization Act, and it is essential that Congress continues to provide it with the resources necessary to carry out its mission. I look forward to hearing today from the CETAP grant recipient, CYBER.ORG, to learn more about their progress in developing curriculums for K-12 educators

and what more can be done to both expand resources to teachers and build awareness of existing programs. Reaching children in the K-12 environment is an important step in making sure we don't leave talent untapped.

Just as important, however, is that we reach students in college, contemplating college, or mid-career who may not have considered a career in cybersecurity to be a viable option. That's is where bringing cybersecurity workforce programs to overlooked communities and reskilling programs come in, and I look forward to hearing from California State University, San Bernardino on its important work in this space.

Finally, as we look for new opportunities to redouble our efforts to grow our nation's cyber talent, I want to be mindful that cybersecurity training is not one-size-fits-all. The recent Colonial Pipeline ransomware attack highlighted the significant impact any incident involving critical infrastructure can have. While the attack only affected the information technology systems of the pipeline company, the precautionary decision to shut off operational technology systems reflected the vulnerability of our industrial control systems. As we work to address our cyber workforce shortage, we must remain cognizant of the different skills and positions involved in securing industrial control systems and ensure that our training programs fully reflect the broad range of cybersecurity threats we face.

Before I close, I want to commend Secretary Mayorkas for making enhancing the cyber workforce the second of DHS's 60-day cyber sprints. By prioritizing this aggressive approach, Secretary Mayorkas has made meaningful progress in reducing the significant number of cyber vacancies at the Department while taking additional steps to address the shortage of cyber professionals nationally. A diverse and skilled workforce has always been a competitive advantage for our nation against our adversaries, but with constantly evolving cyber threats, we must continuously be looking to enhance our cyber education to stay ahead.

# # #

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