COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

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

July 29, 2021

Today's hearing builds on a longstanding priority for the Homeland Security Committee—addressing the shortage of skilled cybersecurity professionals. This problem is not new, but the urgency is greater than ever in light of the increasing number of ransomware attacks and other significant cyber incidents. Fortunately, the Biden Administration has made addressing cybersecurity workforce issues a priority, with Secretary Mayorkas launching a 60-day sprint on strengthening the cyber workforce earlier this year. This decision reflects an understanding that investments in technology are not sufficient on their own—we must also have a well-trained workforce.

In today's digital age, a basic cybersecurity education is essential for everyone, not just cybersecurity professionals. Individuals are vulnerable to cyber criminals, and an employee clicking on a link in a phishing email can expose a company's networks to intruders.

By investing in K-12 cyber education, we improve cyber literacy across the board, while developing a pipeline of young people who can move into more advanced training and join the cybersecurity workforce. Unfortunately, many students currently receive limited cybersecurity education in school today, and the evidence suggests rural and low-income schools with fewer resources are less likely to offer this important training.

The federal government can help address this gap by providing resources to schools across the country, offering trainings to teachers, and developing cybersecurity curriculum that can be used nationally. Additionally, by starting education early, we can help address a longstanding concern of mine regarding the cybersecurity workforce—the low number of women and minorities in the field, particularly in senior roles.

I am glad DHS is taking steps to address this through a partnership with the Girl Scouts that will help to educated school-aged girls in cybersecurity and that CYBER.ORG is partnering with HBCUs to help develop a pipeline of Black high school students into cybersecurity programs. These actions demonstrate the important role DHS can and should play in encouraging cyber education. These are important programs, but we'll need a lot more of them to make up for the current gaps. Many cybersecurity jobs are high-paying, and they required a variety of education levels, but many young people may not know about them or may not believe they are attainable.

Federal investment in K-12 cyber education can raise awareness of these career opportunities to more students, increase the diversity of our workforce, and strengthen our national security. Additionally, programs supporting cyber education must continue at higher education institutions and in trainings that can provide cyber skills education to those already in the workforce. DHS's support for the National

Centers for Academic Excellence in Cybersecurity and partnerships with other entities like the national labs are important examples of how government, researchers, and teachers can work collaboratively to address our cyber workforce shortage. DHS must continue to strengthen these partnerships – particularly in collaboration with HBCUs and MSIs – in order to develop the workforce we need to address the varied cyber threats we face today.

I thank Chairwoman Clarke for her leadership in holding this hearing and for prioritizing this critical issue. The excellent witnesses here today have a broad range of expertise in the field of cybersecurity education and their insights will be valuable as we continue our work in defending the homeland from cyber threats.

# # #

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