Statement of Ranking Member Cedric L. Richmond

Cybersecurity and Infrastructure Protection Subcommittee Hearing:

CHALLENGES OF RECRUITING AND RETAINING A QUALIFIED CYBERSECURITY WORKFORCE

September 7, 2017

For some time now, experts have predicted that the demand for cybersecurity professionals was quickly outpacing supply. In 2012, the Bureau of Labor Statistics projected that by 2020, there would be 400,000 computer scientists available to fill 1.4 million computer science jobs. Recent estimates suggest the deficit is growing instead of shrinking, and may reach 1.8 million by 2022.

Let's be clear – this is nothing short of a threat to national security. These are the professionals we rely on to help us prepare for and respond to the next WannaCry, Marai or Fancy Bear. These are the people who will prevent state-sponsored hackers from taking down our electrical grid or infiltrating our state election systems.

And these are the experts we need to stand on the front lines during a major cyber attack and make sure we have functioning hospitals, banks, transportation systems, and lines of communication.

We need cybersecurity professionals in the private sector protecting our intellectual property and personal data, and we need them in the public sector protecting our Nation's most sensitive intelligence. Yet, we know that the Federal government – and DHS in particular – is struggling to compete with the private sector for cyber talent.

What's more, this Administration has failed to fill even the most critical, senior-level cybersecurity posts – asking agencies like DHS' National Programs and Protection Directorate to carry out broad, complex cybersecurity missions without a permanent Under Secretary. This lack of leadership makes us vulnerable. We should be doing everything we can to 'right-size' our cybersecurity labor force – and there's a lot more we can do.

We need to introduce students to computers before they get to college – even the ones who go to schools that can't afford expensive tech programs and specialist instructors. I also believe there may be untapped potential in vocational schools, 2-year programs, and minority-serving institutions.

And once we've figured out how to get more people to choose cybersecurity as a career, we need to convince them to turn down a higher paying job and spend some time in Federal service. Within the Federal government, we need to promote recruitment and retention programs, particularly at DHS, which has lagged behind other cyber-focused Federal agencies like the NSA or FBI in attracting cyber talent.

For its part, DHS needs to be more forward-thinking and learn to anticipate the needs of an evolving workforce that values professional development, a flexible work culture, and the ability to transition in and out of positions or even fields.

In closing, there is no question that the cyber workforce challenge is a daunting one – but the stakes are too high to ignore it. Last year, the global economy lost over $450 billion to cybercriminals – and over 2 billion personal records were stolen in the U.S. alone. Meanwhile, studies show that less than half of U.S. businesses would say they are prepared for a cyber attack, and small 'Main Street' businesses are struggling the most.

I look forward to hearing the testimony of our witnesses today, and hope we can identify innovative ways to work together to address cybersecurity workforce challenges.