Opening Statement of Ranking Member Cedric L. Richmond (D-LA)

Subcommittee on Cybersecurity and Infrastructure Protection Joint Hearing

"Public-Private Solutions to Educating a Cyber Workforce"

Tuesday, October 24, 2017

Last month, we held a hearing to discuss the challenge public and private sector groups encounter as they try to *recruit* and *retain* skilled cybersecurity professionals – including Federal agencies like DHS.

Every expert on the panel seemed to agree that the real problem is demand: the need for cybersecurity talent is accelerating at an impossible rate. We cannot rely on 4-year academic institutions and traditional educational frameworks to produce a stream of professionals commensurate with the number of connected devices we now use.

What we learned is that, before we can recruit and retain, we have to start with a more fundamental question – how can we educate, train, and certify today's students and job applicants to be tomorrow's cybersecurity experts? How do we inject more professionals into the job market?

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 reports suggest that deficit is *growing* instead of shrinking, and may reach 1.8 million by 2022. To overcome this shortage, we need a "no stone left unturned" mentality that allows us to tap into every segment of the applicant pool.

Unfortunately, that is not the case today. At our hearing last month, we heard from the International Consortium of Minority Cybersecurity Professionals, or ICMCP, that women and minorities are still vastly under-represented in cybersecurity – with women making up around 11 percent, and African Americans and Hispanics making up less than 12 percent of the global cyber workforce *combined*. What those numbers say to me is that we are still leaving talent on the table.

ICMCP's testimony went even further, arguing that in the realm of national security, having a diverse cyber workforce is mission critical. To support this, ICMCP pointed to the 2014 CIA Diversity in Leadership Study which found that a lack of diversity in CIA's leadership may have contributed to past intelligence failures. We need to be leveraging non-traditional training models like apprenticeships or vocational programs, community colleges, and career development tools.

We also need to grow partnerships at the K-12 level to make sure children are being introduced to computers at an earlier age – even the ones who go to schools that can't afford a specialized tech program.

Some of the skills we need to leverage can't be taught in a classroom, and we need to think creatively about how we identify and cultivate traits that lend themselves to cybersecurity – for example, a natural affinity for problem solving or an analytical approach to risk.

With the right access and support, these candidates can easily learn the technical skills through on-the-job training, industry certifications, community college courses, and modern vocational programs. As our world grows more and more connected, we also need a multidisciplinary approach to cyber education – one that reaches professionals in fields like construction, nursing, and electrical engineering.

I look forward to hearing ideas from our esteemed panel of witnesses today about how we, as Federal policymakers, should be thinking about growing and diversifying our cyber talent pipeline. But ultimately, if we're going to make a dent in the cyber workforce challenge, we need to do more than talk about it.

We cannot pretend to be serious about right-sizing the cyber workforce while at the same time entertaining the Administration's request for massive cuts to programs like the National Science Foundation's Scholarship for Service.

Similarly, I cannot fathom what kind of message is being sent to DACA recipients working to earn tech degrees in fields like cybersecurity – nor can I understand the logic behind needlessly sending this homegrown talent abroad.

I'll conclude by saying that defending our networks from cyber attack requires strong leadership, sustained funding from Congress, and action. 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.