COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity, Infrastructure Protection, and Innovation Subcommittee Chairman Cedric Richmond (D-LA)

Growing and Diversifying The Cyber Talent Pipeline

May 21, 2019

When I became the Ranking Member of this Subcommittee in 2015, researchers were projecting that the shortage of cybersecurity professionals would reach 1.5 million by 2020. In 2018, that research showed a current-day shortage of nearly 3 million unfilled positions around the world – and over 300,000 in the United States alone. That means that nearly a third of the U.S. cybersecurity workforce is, at this point, an empty desk. Nevertheless, every day, we introduce newer, smarter, more connected devices and infrastructure to make our lives easier, our businesses more profitable, and countless other goals. And, every day, we learn new ways these devices can be hacked, disrupted, or manipulated to cause everything from minor inconveniences to major global havoc.

We have seen ransomware attacks take out entire branches of local government. We have had our personal data, intellectual property, and military secrets stolen by hostile foreign governments. It has never been more clear: we need more people at the table who know cybersecurity. And we must do more than admire the problem. This Subcommittee held three cyber workforce hearings last Congress, and learned something in all of them. Now that I have the gavel, I want to use it to drive home an important point: diversity is essential for national security, and for cybersecurity. We need to bring people to the table who have different perspectives, different experiences, and different ways of looking at a problem.

Right now, the vast majority of the cybersecurity workforce is white and male – only 9% are African American, 4% are Hispanic, and 11% are women. My concern is that having such a homogenous workforce could lead to blind spots and, potentially, intelligence failures – particularly for Federal agencies like the Department of Homeland Security. I know we have some panelists here today that can speak to these issues directly, and I look forward to their perspectives. Despite the good work being done in the public and private sector on cyber workforce, here's what I know for sure – we still are not tapping into diverse talent streams. If we are serious about fixing this problem, we need to put our money where our mouth is.

We have to stop starving the Federal programs that support cyber talent, such as the National Science Foundation's Cyber Corps Scholarship for Service, who's budget is on the chopping block every year. We also need to stop bleeding talent at the very agencies who need cyber experts to carry out their missions, like DHS, the FBI, and the National Security Council at the White House. And finally, we have to move the conversation around diversity out of the background and put it front-and-center. We cannot continue to make diversity an afterthought and expect that it will spring forth naturally.

A few weeks ago, the White House issued an Executive Order on America's Cybersecurity Workforce. It introduced a President's Cup cyber competition, and some workforce rotation opportunities – which are good – but was mostly silent on diversity. Officials reportedly explained that they "hoped diversity would be a natural byproduct" of the Order. This is exactly the type of thinking we cannot afford to have if we are serious about reversing trends. I look forward to hearing from our witnesses today about opportunities to address this important national security issue.

# # #

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