Opening Statement of Ranking Member Susan Davis (CA-53)
Subcommittee on Higher Education and Workforce Development
Joint Hearing on "Public-Private Solutions to Educating a Cyber Workforce"
Tuesday, October 24, 2017 – 2:00pm
HVC-210, House Capitol Visitor Center

Thank You Mr. Chairman.

This is a timely and important hearing. I am excited to be working with our colleagues from the Cybersecurity and Infrastructure Subcommittee.

We are holding this joint hearing today to explore the critical issue of the cybersecurity workforce pipeline. It is an urgent problem that has serious ramifications for our national security. As my colleagues have pointed out today, cybersecurity attacks are on the rise resulting in massive data breaches and the loss of critical private data.

And we know that cybersecurity vulnerabilities extend to critical infrastructure and our elections. The need for a more secure cyberinfrastructure is only going to grow as technology continues to move into even more aspects of our daily lives. By tackling this problem we can secure critical information and create many more high-paying jobs.

The fundamental building block of a strong and durable cyberinfrastructure is highly skilled cybersecurity workers. But there's a consensus that we face a critical shortage of cybersecurity professionals, leaving the nation especially vulnerable. In today's hearing we will hear from businesses as well as higher education institutions on what is being done, and what remains to be done in order to fill our cybersecurity workforce needs.

In order to address these problems we must ensure that we are actively recruiting women, African Americans, Hispanics, and Native Americans into the field. These groups are woefully underrepresented in the cybersecurity workforce. According to a recent survey, women account for only 14 % of North America's cybersecurity professionals. We must do better than this. We must not only deepen but also broaden the pool of highly trained individuals in the field.

I look forward to hearing from Dr. Ralls on the many innovative programs that the Northern Virginia Community College has developed to build a robust cybersecurity workforce. In response to burgeoning demand, the Northern Virginia Community College has grown from 50 to 1,500 students in one of its associates programs in just four years – that's a remarkable thirty-fold increase. They are using successful, proven career development methods like apprenticeships and career and technical education to bridge the gap.

This is the type of innovation we should promote and support. However I am concerned that the administration is pointing us in the wrong direction. The administration's budget request proposed to cut funding for the CyberCorps Scholarship for Service program by a whopping 27% from its FY17 levels. We should be looking to expand, not contract, our efforts to fill cybersecurity workforce shortages.

Government, educational institutions, and industry leaders must come together to address the shortage. Government should be adequately investing in the educational and workforce development infrastructure to grow the talent pool and raise awareness for cybersecurity careers. I know that there are innovative ways that the workforce system can use federal investment to build a strong cybersecurity workforce. In my district, the San Diego Workforce Partnership is using funding from the Obama Administration's Tech-Hire grants to build cybersecurity training programs.

I also believe that educational institutions must be more responsive to the shortages by creating and expanding cybersecurity programs and I know we have great examples here today.

Businesses and industry leaders must also do their part and I look forward to hearing today from IBM. Industry leaders should be expanding apprenticeship programs, investing in retraining and upskilling their current workforce as well as recruiting from a more diverse talent pool. And it goes without saying, I hope, that our industry leaders must work collaboratively with educational and training institutions. Businesses must also take a critical look at their hiring practices and really look at their credentialing requirements to ensure that they are not over-specifying credentials that might create a barrier.

I would like to thank Chairs Ratcliffe, McCaul, and Guthrie for holding this hearing.

I look forward to hearing from the witnesses on how we can create attractive career pathways in cybersecurity for both the civilian and military workforce.