COMMITTEE ON EDUCATION AND THE WORKFORCE

COMMITTEE STATEMENT

Opening Statement of Rep. Brett Guthrie (R-KY)
Chairman, Subcommittee on Higher Education and Workforce Development Joint Hearing on "Public-Private Solutions to Educating a Cyber Workforce"

When Americans think of data breaches and cyber-attacks, names like Equifax come to mind. This and other recent high profile data breaches have made private and sensitive information vulnerable to identity theft as well as other cyber-crimes.

Cyber-crimes are constantly appearing in the news, and Americans want to know what is being done to protect their data, as well as other vulnerable targets that comprise our national infrastructure.

Organizations in the public and private sectors are actively seeking skilled professionals to fill the numerous jobs available in the growing cybersecurity field, and are coming up short in the number of Americans able to fill these essential positions that ensure our American cyber-infrastructure is safe.

A recent study by Intel Security and the Center for Strategic and International Studies (CSIS) examined the global cybersecurity workforce shortage and confirmed that the talent shortage was real and widespread. Eighty-two percent of participants report a shortage of cybersecurity skills.

The same report found that more than 209,000 cybersecurity jobs in the U.S. are unfilled, and job postings are up 74 percent over the past five years. Additionally, the demand for cybersecurity professionals is expected to continue to grow to over 1.8 million by 2022.

This skills gap is not unique to the cybersecurity sector. Many other industries such as manufacturing and transportation are facing a shortage of skilled workers to fill good-paying jobs. However, when dealing with cybersecurity, the stakes are even higher because we are dealing with national security.

Fortunately, the discussions we have today will not be the beginning of the conversation in Congress on closing the skills gap.

The House unanimously passed the *Strengthening Career and Technical Education for the 21st Century Act*, which allows states to dedicate additional resources towards high-demand fields such as cybersecurity based on changing economic, educational, or national security needs.

Additionally, the Committee on Education and the Workforce has been carefully observing the implementation of the *Workforce Innovation and Opportunity Act* that was signed into law in 2014.

This law streamlined the confusing maze of workforce development programs, and increased the amount of funding available to the states to meet specific workforce demands based on conversations with public and private stakeholders in each state.

Today's hearing will examine solutions to filling the skills gap that currently exists in the cybersecurity field, and how coalitions across government, academic institutions, and private industries can pave the way to successfully close this skills gap and keep our country's cybersecurity infrastructure safe.

# # #