**Opening Statement**

**Ranking Member Robin Kelly**

**Field Briefing on “Federal Efforts to Improve Cybersecurity”**

**Subcommittee on Information Technology**

**June 20, 2016**

Thank you Chairman Hurd, and welcome to the beautiful city of Chicago. And thank you to our witnesses for taking the time to testify here this morning.

In the past two years alone, the public and private sectors have faced serious challenges to keeping their networks and systems secure from cyber thieves. In that timeframe, sophisticated companies like Anthem, Sony Pictures, Target, and Home Depot, all reported being victims of cyber-attacks. Last year’s data breach at the Office of Personnel Management similarly highlighted the challenges the federal government faces in securing its systems from cyber spies. And just last week, we learned that hackers had gained access to the Democratic National Committee networks.

These attacks make clear that no business or sector of the economy is immune from sophisticated adversaries.

In response to the rising frequency of large-scale cyber-attacks, both Congress and the Administration have taken a number of steps to address this issue.

This past December, Congress passed, and President Obama signed into law, the Cybersecurity Information Sharing Act of 2015. With this landmark legislation, the private sector and federal government will now have a more effective framework for sharing cybersecurity information to better respond to cyber threats.

More recently, the President released his Cybersecurity National Action Plan – more commonly known as CNAP (SEE-NAP) – for the country. A critical component of CNAP is the establishment of a new commission that is tasked with providing the President with recommendations on actions the country should take over the next decade to strengthen cybersecurity in both the public and private sectors.

These federal efforts all have great potential for improving the state of this nation’s cybersecurity, but only if the federal government and private sector work together. And that’s why we’re here today.

We’re holding today’s Congressional field briefing in Chicago to hear your views on how our cyber laws and regulations have been working.

Professor Santos, from Illinois Tech, works on groundbreaking innovations in numerous fields, and you are widely viewed as a leading academic expert in the field of computer science and cybersecurity.

Mr. Horn is from Advocate Healthcare, the largest health care provider in Illinois.

Ms. Hatter is from Intel, one of the largest semiconductor chip makers in the world.

Mr. Carano is from ChicagoFIRST, which protects the infrastructure of the financial institutions in the second largest financial hub in the country.

We’re interested in hearing about the challenges to cyber security and what you believe the federal government can do to help you keep sensitive data and networks safe.

I want to thank our witnesses again for their testimony today. Government and the private sector need to work together on cyber security. I look forward to heading back to Washington with a better picture of what works, what doesn’t work, and where we need to improve.

Thank you, Mr. Chairman.

Contacts: Aryele Bradford, Deputy Communications Director, (202) 226-5181.