Ranking Member Cedric Richmond Opening Statement

Subcommittee on Cybersecurity & Infrastructure Protection Hearing

"The Current State of DHS' Efforts to Secure Federal Networks"

March 28, 2017

Americans rely on Federal agencies to safeguard some of our most sensitive national data – from health records and Social Security Numbers to intelligence and information on troop movements.

This information may be exposed or exploited by something as simple as a careless employee or a failure to patch a known vulnerability.

This information can just as easily be taken or altered by criminal networks and - as we discussed last week in this Committee - state-sponsored hackers.

The Russian attacks this past year on our democratic processes and political institutions are a salient reminder of the damage state adversaries like Russia can inflict.

Just last year, GAO surveyed agencies with 'high impact' systems – those that hold information so sensitive that a breach could cause catastrophic harm to individuals, the government, or the nation. The survey showed that cyber attacks from state actors represented the most serious and frequent threat these agencies faced.

This same team of GAO analysts, one of whom we have with us today, revealed that from 2006 to 2015, the number of cyber attacks on Federal agencies went from about 5,500 per year to over 77,000 – a 1,300% increase.

We also know that our government networks have not only been targeted, -- they have also infiltrated.

Successful cyber attacks have been carried out against the Office of Personnel Management, the Internal Revenue Service, and the Departments of State, Defense, Veterans Affairs, and Health and Human Services, to name just a few.

To be clear, there is no one-size-fits-all, "silver bullet" for securing Federal networks.

That said, there are some positive signs that current efforts may be having an impact.
A recent report from the Office of Management and Budget shows that, over the last year, the number of cyber attacks on U.S. government networks has gone down -- not up -- for the first time in a decade.

I am also interested to hear from DHS and GAO on the extent to which this downward trend may be attributable, at least in part, to greater adoption of the EINSTEIN program by Federal agencies.

I look forward to hearing from this panel about how DHS is working with its Federal partners to deliver cybersecurity services that are valuable, affordable, and effective.