**Opening Statement**

**Ranking Member Elijah E. Cummings**

**Hearing on “Enhancing Cybersecurity of Third-Party Contractors and Vendors”**

**April 22, 2015**

 Thank you, Mr. Chairman. And thank you for agreeing to my request to hold today’s hearing on the cybersecurity challenges posed by contractors and third-party vendors.

 Over the past several years, we have seen an alarming increase in the number of major data breaches that originated with contractors and vendors.

Just last year, Target and Home Depot were breached by hackers who gained access to the retailers’ networks by using credentials stolen from the computer systems of vendors that did business with these companies.

Federal agencies are not immune. The breach of the Postal Service last year originated from a spear-phishing attack on a contractor for the agency.

Last year, contractors with the Office of Personnel Management (OPM) were subjected to a sophisticated cyber-attack, and tens of thousands of sensitive personnel records were compromised.

One of those contractors was a company called USIS. At the time, it was the largest provider of background investigation services to the federal government.

USIS is currently at the center of a billion dollar civil fraud suit brought by the Justice Department for allegedly “dumping” incomplete background investigation reports to OPM over a 4½-year time period. According to the Justice Department, USIS deliberately took this action to increase its revenues and profits.

Apparently, the company’s desire to increase profits also may have been to blame for its failure to make the cyber investments necessary to secure the large amounts of sensitive personal information it should have been protecting on its networks.

On September 3, 2014, Committee staff received a briefing from security experts at the Department of Homeland Security, the Office of the Director of National Intelligence, and OPM, all of whom analyzed the cyber attack against USIS.

While much of that briefing was sensitive, one point may be discussed publicly. Press accounts had initially reported that the attack may have compromised the personal information of up to 27,000 federal employees, however, government cyber security experts believe this number is a floor—not a ceiling.

The actual number of individuals affected by the USIS data breach is still not yet known, but these experts believe that the personal information of many more federal employees may have been compromised.

Unfortunately, investigating the USIS data breach has been particularly challenging because neither USIS nor its parent company, Altegrity, have fully complied with this Committee’s requests for answers.

Today’s hearing is a recognition that the federal government faces increased cyber risks from contractors. But as I mentioned earlier, this is a challenge the private sector faces as well.

I have repeatedly pressed for more rigorous oversight of cyber security in both the private and public sectors. Although we had little success in the previous Congress, I am encouraged by the bipartisan approach we have taken on this very critical issue, and I hope it continues.

So Mr. Chairman, thank you again for agreeing to hold today’s hearing. In addition, I understand that our staffs are meeting tomorrow to discuss a possible follow-on hearing with some of these private sector entities, and I thank you for continuing to work with us on this issue.