Opening Statement
Rep. Elijah E. Cummings, Ranking Member
Hearing on "GAO's High Risk Report: 25 Years of Problematic Practices"

February 11, 2015

Mr. Chairman, thank you for holding this important hearing. And thank you, Mr. Dodaro, for the in-depth work that you and your team at GAO put into updating this High Risk report, which found "[s]olid, steady progress has been made in the vast majority of high-risk areas."

I know this has been a long day for you. We had a press conference with you this morning, then you testified over in the Senate, and now you are testifying here before our Committee. So a lot has already been said about this year's report.

But in my opinion—and based on my work over the past several years—I believe that if there is one thing we must take away from this new report today, it is that we need to focus much greater attention and effort on combating cyber attacks and preventing data breaches, which pose a clear and present danger to our national and economic security.

The number of cyber attacks is increasing rapidly, and they affect hundreds of millions of Americans. They often originate overseas, and they are very difficult to combat effectively.

This year, the nonpartisan experts at GAO have determined, for the first time, to elevate to the High Risk list the objective of protecting personally identifiable information, or PII. In its report, GAO found that a steady and alarming increase in the frequency of devastating cyber-attacks has compromised the sensitive personal information of tens of millions of Americans.

In its report today, GAO noted the obvious fact that cyber attacks affect both government and private sector entities.

With respect to the federal agencies, GAO found that the government "continues to face challenges in effectively implementing cybersecurity policies."

GAO also took into account the significant challenges faced by the private sector. Recent attacks against companies like Sony show the difficulties private corporations have with safeguarding individual personal information.

And just last week, Anthem, one of the nation's largest health insurers, was hit by a devastating cyber attack in which hackers were able to break into the company's computer networks and steal up to 80 million records of customers and employees, including their social security numbers.

Congress and the Executive Branch must do all we can to implement GAO's recommendations to mitigate the risks at federal agencies. We must also ensure that

American consumers are protected when they provide their personal information to private companies.

Over the past several years, I have been pressing for this Committee to conduct more vigorous oversight of cyber security measures in both the private and public sector, but I have had very little success. I have requested information and hearings on data breaches at retail companies, financial institutions, healthcare corporations, government contractors, and federal agencies. But there was little interest on the other side.

I am very encouraged to report that this is now changing. Earlier today, the Committee adopted—on a bipartisan basis—our new oversight plan for the 114th Congress. And we voted unanimously to include in our oversight plan a commitment to conducting robust oversight of this very critical issue.

Mr. Chairman, thank you for agreeing to our proposals to the oversight plan and for calling today's important hearing. I stand ready to work with you and all Members of the Committee in a bipartisan manner.