Opening Statement
Ranking Member Elijah E. Cummings

Hearing on "Social Security Administration: Information Systems Review"
May 26, 2016

The Social Security Administration is located in my district in Baltimore and manages our nation's Social Security program. It ensures that more than 50 million seniors receive the benefits they have earned through their lifetime of work. That is about 89% of the U.S. population over the age of 65.

To administer the Social Security program, as well as the Disability Insurance program and the Supplemental Security Income program, the Social Security Administration collects sensitive data on nearly every American.

The data breach at the Office of Personnel Management affected more than 25 million people. A breach at the Social Security Administration could affect nearly every single person in this country.

The good news is that Social Security has never had a known data exfiltration. However, threats are constantly evolving, and today's hearing will enable us to examine what more must be done to meet these threats and ensure that Social Security data remain safe and secure.

In many ways, Social Security's information technology systems are models for the f~~F~~ederal government.

The agency has saved about $370 million in its IT budget over three years.

This sounds technical, but Social Security achieved the highest individual metric grade for IT project savings on the FITARA Implementation Scorecard metric that our Committee commissioned. In other words, it was the benchmark against which the other 23 agencies were measured.

However, Social Security is confronted by tens of millions of scans and probes every week trying to find vulnerabilities in the agency's defenses. Every second of every day, determined hackers, here in the United States and around the world, are trying to breach Social Security's firewalls.

Audits of Social Security's IT systems and practices have found weaknesses that need to be corrected. In 2012, a FISMA audit reported that these shortcomings constituted a material weakness.

The agency has worked to address these shortcomings, and more recent audits have found improvements in the agency's IT security. But there is still a "significant deficiency in internal controls," according to the most recent audit.

Additional measures must be implemented to close remaining gaps. Unfortunately, Social Security's IT budget has been underfunded for years.

According to the FISMA audit, one of the factors that contributed to the agency's significant deficiency was that "SSA focused its limited resources on higher risk weaknesses and therefore was unable to implement corrective action for all aspects of the prior year deficiencies."

Social Security benefits are funded through the Social Security tax paid by employers and employees. Funding for benefits is considered mandatory spending and is not subject to the appropriations process. However, the agency's administrative expenses are paid from an account that is funded by discretionary appropriations subject to the annual appropriations process.

Congress' failure to adequately fund Social Security's administrative expenses has resulted in extended wait times for seniors calling the 800 number, reduced operating hours at field offices, and delays for adjudicative hearings that now average more than 500 days.

Underfunding the Social Security Administration has also affected its efforts to modernize its 40-year-old IT infrastructure and address evolving cyber risks.

The President's Fiscal Year 2017 budget seeks the first installment of what is expected to be a $300 million request over the coming years to upgrade Social Security's IT systems.

Congress must act on this request and provide the agency the resources it needs to protect the data entrusted to it. Shortchanging data security at Social Security in the senseless pursuit of austerity could put the privacy of every American at risk—and that is a risk we simply cannot afford to take.

Thank you, Mr. Chairman.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.