Opening Statement as Prepared for Delivery by Chair Maggie Hassan
Emerging Threats and Spending Oversight Subcommittee Hearing:
Controlling Federal Legacy IT Costs and Crafting 21st Century IT Management Solutions
April 27, 2021

Good morning, and thank you to our panel of witnesses for appearing today to discuss controlling federal legacy IT costs and crafting 21st century IT management solutions.

I also want to thank Ranking Member Paul and his staff for working with us on this hearing, and for our continued partnership to address wasteful spending and government inefficiencies. Even though Ranking Member Paul is unable to join us this morning, I look forward to working with him and other members of the Subcommittee to address the threats posed by the federal government's failure to maintain a modern and agile information technology infrastructure.

Today is the first of multiple hearings on federal legacy IT systems. By shining a light on this important issue, I hope that agencies will work to reduce their reliance on costly legacy IT systems in partnership with Congress, the Biden Administration, and industry stakeholders. Today's hearing will focus on identifying the costs and consequences of legacy IT, as well as the institutional barriers to modernization.

According to the Office of Management and Budget and Government Accountability Office, in fiscal year 2020, the federal government spent roughly $90 billion on IT investments and operations. Based on analysis of agency expenditures, legacy IT maintenance costs accounted for one-third – about $29 billion – of total spending. However, the actual cost is estimated to be much greater when we consider legacy IT's negative effects on security, delivery of services, and customer experience.

To frame our discussion, we should have a common definition of legacy IT. Legacy IT describes the federal government's use of old technology or custom systems designed to support insular agency operations. That is, legacy IT includes technology and systems that are no longer supported by industry vendors, as well as those that require additional maintenance or specialized knowledge to operate.

We have seen the consequences of relying on legacy IT systems. For example, in 2014, hackers stole the personal information of more than 20 million people from the Office of Personnel Management, because they were able to breach OPM's vulnerable legacy IT systems that lacked encryption. Despite this breach that was clearly linked to a failure to modernize, OPM still relies on a 34-year old legacy IT system that costs $45 million annually - roughly one-third of OPM's annual IT budget - even though a modern system would only cost $10 million and produce $16 million in cost savings.

At the Internal Revenue Service, the system used to annually process millions of tax documents is more than 50 years old and relies on a programming language called the "common business-oriented language," or COBOL, which was invented in 1959. In 2018, implementation of the 2017 tax law hit a major roadblock due to a shortage of staff with the specialized knowledge needed to update COBOL-based tax-processing systems. IRS estimates that it costs $15.9 million

annually to operate this system and 60 percent of those costs are for labor alone. During the COVID-19 pandemic, IRS faced additional challenges, because many of its aging systems rely on paper rather than digital records, which were inaccessible to IRS employees working remotely. And as a result, the American people felt the burden of delayed tax-returns and economic stimulus payments.

Similarly, in 2016, the Social Security Administration was forced to rehire retirees to maintain the COBOL system used for making payments to beneficiaries and their dependents. These systems cost the Social Security Administration almost $146 million annually to operate. However, the Social Security Administration estimates that it would only cost $25 million over five years to modernize the system, and would significantly improve functionality and security, as well as eliminate the need for specialized programmers.

This begs the question: what are agencies waiting for? What is holding them back from realizing significant cost savings, increasing security, and providing greater customer service delivery through reducing their reliance on legacy IT?

In addition to the costs and consequences of relying on legacy IT systems, today's hearing will also discuss the institutional barriers that prevent agencies from moving forward with their modernization efforts.

Our distinguished panel includes the director of the Government Accountability Office's information technology and cybersecurity team, as well as three former federal agency chief information officers who navigated the challenging IT modernization landscape and successfully moved their agencies away from legacy IT systems. I look forward to hearing from all of our witnesses about how they achieved success by leveraging available resources and being innovative.