Testimony of Renee P. Wynn

Former Chief Information Officer of the National Aeronautics and Space Administration

FOR A HEARING ON

Controlling Federal Legacy IT Costs and

Crafting 21st Century IT Management Solutions

BEFORE THE

United States Senate

Homeland Security and Governmental Affairs Committee Subcommittee on Emerging Threats and Spending Oversight

April 27, 2021

Washington, D.C.

Good morning Chairwoman Hassan, Ranking Member Paul, and distinguished members of the Subcommittee. I am honored to testify today on the importance of Information Technology (IT) modernization, highlighting barriers and challenges in the IT modernization process and how Congress and agencies can work together to address them.

Now is an ideal time for departments and agencies to begin or continue large, complex IT modernization projects. Much has been learned about remote working and delivering federal government services during the COVID pandemic. This learning can be used to accelerate modernization efforts. To do this, the departments and agencies must have the right personnel, processes, and budgets in place to significantly increase the probability that such IT modernization projects will be successful.

As the former Chief Information Officer (CIO) of NASA and the Acting CIO and Deputy CIO of the Environmental Protection Agency (EPA), I have had ample opportunity to understand the dynamics inherent in modernizing federal government IT. My experience as NASA's (CIO) gave me the best view of the biggest challenge a CIO faces when modernizing IT in the federal government - an agency's culture, which is sometimes referred to as the "people challenge." A CIO must have sustained support and funding for IT modernization from the Agency heads to her executive management team, she must have the right people with the right skills, including the contractor workforce, and build and maintain relationships across the Agency and with the contractor community. Without this support, complex IT projects will fail.

NASA's Business Service Assessment

Prior to my arrival, NASA had initiated and completed a Business Services Assessment (BSA). The BSA was undertaken to identify organizational and management improvement areas for NASA's mission support services. This included, but was not limited to, procurement, facilities, and human resources. IT was the first mission support function assessed, and the findings resulted in a list of recommendations. Some key recommendations covered revising the governance process to include mission executives and non-IT executives from the different NASA centers, establishing more enterprise-wide IT services, better software management practices and the need for an improved cybersecurity program.

The CIO office developed and executed an implementation plan based on the BSA recommendations. While implementing the plan, my team and I learned many valuable lessons. We adjusted our approach based on our experiences and highlighted an issue that was preventing us from gaining the full benefit of the BSA recommendations and future IT modernization efforts: too much of NASA's IT budget and staff (civil servants plus contractors) were not managed by the NASA CIO. This made it difficult for NASA to control IT spending because many of the geographically dispersed Centers were independently establishing IT service contracts or buying software, even though the CIO office provided the service or had existing software licenses available. Misalignment of budget and organization plagued the other mission support areas already implementing their BSA recommendations, too.

NASA used insights from the BSA to create a Mission Support Future Architecture Plan (MAP) to make holistic improvements across the entire mission support operations spectrum. MAP took

the bold and politically charged step of having all the people and budget associated with a mission support function report to the head of the mission support function, such as the Chief Human Capital Officer (CHCO), the Chief Procurement Officer (CPO), or the CIO. The two largest mission support functions, IT and Facilities, were scheduled to be the two final organizations to go through the MAP process. This allowed the agency to learn from implementing MAP before starting on the largest, most complex organizations.

As I led the transformation resulting from the BSA and MAP, I found the most significant challenge was addressing culture, again this is sometimes referred to as the "people challenges." As I saw it, people challenges can be divided into three categories – those that worked for me (including contractors); those that worked for the other mission support functions; and those that I served, the civil servants and contractors delivering NASA's complex mission.

The people, civil servants, and contractors, that worked for me were extremely talented, but concerned that the BSA meant they were not valued by NASA and were seen as doing a poor job. To this end, I and the Center CIOs spent a lot of time reassuring them that NASA did value them, and the BSA was a gift that elevated the importance of their work and increased their value to NASA.

The other mission support areas were frequently critical of the CIO and IT modernization projects. While the Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO) and Chief Procurement Officer (CPO) understood the need for MAP for their area, there was resistance from some of them because they faced losing their IT staffs to the CIO. This resistance affected our collaboration efforts. I and my Deputy had to work to regain the trust we needed for mutual success and future IT modernization projects.

NASA's top executives provided steadfast support of the NASA CIO throughout the mission support transformational efforts. However, the executives and staff below them were resistant and at times, difficult. Nothing rattles a civil servant more than having portions of their budgets and staff reallocated. When difficulties would arise, either I, my Deputy or a Center CIO would have to work with them to address their concerns. We were not always successful at soothing hurt feelings, but many a painful conversation would at least result in better mutual understanding, and improved working relationships. To say the least, my team and I spent a lot of time working culture change or the "people challenges."

Congressional Support

Congress has taken appropriate steps to address IT management and cybersecurity risks through legislation. From the Clinger-Cohen Act of 1996 to the Federal Information Security Modernization Act of 2014 (FISMA) and to the Federal Information Technology Acquisition and Reform Act of 2015 (FITARA), all were designed to advance government services to the public and provide improved information security for the U.S. government. The legislation gave the CIO the authorities to lead the way for more modern and secure IT so the public would be better served.

With the passage of the Modernizing Government Technology (MGT) Act, Congress continued its support to improve Federal technology by providing financial resources to agencies through the

creation of a central modernization fund housed by the General Services Administration (GSA). These funds are allocated through the Technology Modernization Fund (TMF) board. The board's primary objectives lie in evaluating project proposals submitted by agencies wishing to use some portion of the TMF as well as monitoring the progress of the funded IT modernization projects.

The oversight of Congress has also been a driving factor in making the intended improvements. This needs to continue as a bipartisan, unified approach, as it has had a positive impact on how seriously past administrations have focused on IT modernization and cybersecurity. These legislative actions plus sustained oversight, have provided the foundation to improve IT management and cybersecurity for the federal government.

Congressional action taken over the years has given the federal government a solid foundation for pursuing IT modernization so the government can better serve the public.

Going Forward

I have learned during my tenure as the NASA CIO that successful IT modernization projects require sustained and predictable budgets, the right people, and unwavering internal leadership support to deliver their expected benefits.

Congress should remain focused on IT modernization and cybersecurity through oversight hearings, providing predictable appropriated budgets and funding for the TMF. Oversight hearings with the CIO should also include other Department or Agency leadership such as, but not limited to, the Chief Procurement Officer, Chief Financial Officer and even the Chief Human Capital Officer. Together, they should provide the update on large, complex IT modernization projects. Finally, Congress should also be prepared to act should gaps emerge in the federal government's ability to deliver more modern and effective public services.

The CIO must also have the right workforce, an appropriate blend of civil servants and contractors invested in the mission of the federal government. Yet, the federal government continues to struggle with recruiting and retaining experienced IT professionals, especially those with the skills to run large IT projects. Contractors help fill the gap, but there needs to be a blend of civil servants and contractors working on every IT project. There is no specific ratio, just an effective balance. It is an art and depends upon the complexity of the IT project. Current civil servants must have time to keep up to date on technology advances, as well participate in re-skilling opportunities. Early efforts to re-skill existing federal employees have been successful. This should continue. Whether a civil servant or a contractor, all involved must have the knowledge, skills, and expertise to meet the growing demands of IT modernization and cybersecurity.

Internal to agencies, department and agency heads should provide unwavering support for IT modernization and cybersecurity projects so the CIO can address the culture, IT workforce and budget challenges.

IT modernization and improved cybersecurity practices are fundamental requirements for delivering improved and secure federal services to the American public.

Thank you for the opportunity to appear before the Subcommittee today and testify on this critical topic. I stand ready to answer your questions.