July 28, 2021

Testimony of Federal Chief Information Officer Clare Martorana

House Committee on Oversight and Reform
Subcommittee on Government Operations

Hearing on
Federal Information Technology Acquisition Reform Act: Scorecard 12.0

Introduction

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee, thank you for the invitation to testify about the 12th FITARA scorecard. Technology powers each agency in being able to deliver on its mission for the American people. It's FITARA that gives every Chief Information Officer (CIO) a seat at the table to make the best enterprise IT decisions to deliver for their workforce and our citizens.

It is a privilege to speak to you about the current state of federal information technology (IT), and share the Biden Administration's vision for delivering modern and secure IT solutions across the federal enterprise. I'd also like to thank the Committee for your leadership in promoting IT modernization. While this work is challenging, it's a challenge I firmly believe in taking on to secure federal IT and place agencies on a path to deliver transformational services to the American people. I'd also like to acknowledge Sean, Keith, their fellow CIOs, and the IT workforce across our government for their hard work to achieve the grades on this scorecard.

Federal IT: What's Possible

Imagine a day when a citizen can use their mobile phone to sign in and see everything they have in flight with our government – a small business loan application, the status of their tax refund, or the estimated social security retirement benefits they'll receive one day. Imagine the process is easy, understandable, convenient, secure, and fast—just like the consumer experiences we have every day, from online banking to ordering food delivery. With the amount of information we collect across the federal government and the enormous investment of taxpayer dollars in federal IT, it's not only possible for our government to deliver this type of high-quality customer experience -- it's an expectation in the 21st century.

For over 20 years in private sector, I used innovative technology and human-centered design to create products, services, and experiences that improve people's lives, from my time as President of Everyday Health to my roles as Senior Vice President and General Manager of WebMD. Over the past five years, I've been part of government teams using the same technology and design principles to improve the lives of our veterans, our federal employees, and our retirees. In my role as Federal CIO, I intend to use my past experience to scale these successes across the federal enterprise. In order to get there, however, we must first focus on the most pressing circumstances we find ourselves in today.

Cybersecurity is the Immediate Priority in Federal IT

Having come to the Federal CIO position directly from OPM, I can tell you firsthand that CIOs across government are faced with an enormously challenging environment – managing agency technology portfolios at different levels of funding and maturity, working to retire legacy IT while trying to launch modern platforms, and most importantly, identifying vulnerabilities and ensuring the cybersecurity of their networks. The increasing number of sophisticated cyber events in recent months has highlighted our need to rethink how we approach cybersecurity.

Organizations across the world are shifting to a new security paradigm that assumes the integrity of the networks on which they operate cannot be trusted. These new organizing principles are called Zero Trust. It means assuming everyone and everything is possibly untrustworthy, limiting access intelligently, and validating every user and device. The goal is to establish confidence levels in the people and devices attempting to access resources and achieve more granular visibility and control over granting them access. It also means getting better at detecting anomalous activity faster to prevent harm.

Federal agencies have been busy building out a strong foundation of Zero Trust capabilities for years, to include identity, credential, and access management, and shifting to continuous monitoring and dynamic management approaches. My goal is to help agencies tie all of these efforts together into a Zero Trust roadmap, which we can use to inform multi-year implementation and investment plans.

President Biden's *Executive Order 14028 on Improving the Nation's Cybersecurity,* released in May of this year, set us on this path. First, we asked agencies to assess their Zero Trust maturity in 60 days and share that information with OMB. Second, our partners at the Cybersecurity and Infrastructure Security Agency (CISA) are developing a capability maturity model to standardize the approach across the Federal government. And, finally, OMB will issue guidance to define successful roadmaps for agencies.

To ensure that every agency is where they need to be, it's going to take an enterprise approach – and we must move rapidly. It will take CIOs in agencies that are farther along in their Zero Trust journeys to partner with those in the earlier stages, sharing best practices, wisdom, and playbooks to expedite this process. It will take working with our Chief Financial Officers, Chief Acquisition Officers, and agency leadership to build the operational model for investment, deployment, and sustainment of these capabilities. As Federal CIO, I am committed to getting every agency to the same level of readiness. We will work rapidly and seamlessly. We must -- our adversaries are on the offensive.

Operating as an Enterprise to Deliver for the American People

1. Investing in the Present

We are fortunate that this Congress, and in particular members of this Committee, recognize the challenges ahead and have worked to provide us with the flexibility and funding to get the job done.

The $1 billion appropriation to the Technology Modernization Fund, or TMF, is an important commitment to improving the government's foundational infrastructure. But this appropriation is just a down-payment on the multi-year technology modernization projects federal agencies have identified. Since the passage of the American Rescue Plan Act of 2021, and our expedited review process, OMB has received more than 100 proposals for projects totaling over $2 billion and we continue to receive proposals on a rolling basis.

As the chair of the TMF Board, I am reviewing, prioritizing, and overseeing agency IT projects according to four objectives.

- Modernizing high priority systems. All federal agencies - in addition to the American public - benefit from the continued modernization of technology. Modernization can improve the efficiency and effectiveness of internal government operations, enabling agencies to better fulfill their missions and streamline service delivery to the public. The TMF supports the modernization of priority agency assets and services, including systems already designated as High Value Assets (HVAs) that have significant impact, or longstanding security issues.

- Cybersecurity. The gaps uncovered in the recent SolarWinds incident and other cybersecurity incidents underscore the need for attention and resources dedicated to our information security. TMF funding will help agencies take critical steps towards a "zero trust" architecture. Ultimately, building safety and security into every aspect of federal IT and services will increase the trust in government by our most important users – the American people.

- Public-facing digital services. Every interaction with the public is an opportunity to demonstrate competence and deliver effectively. In today's world, the majority of these interactions will happen digitally – for example, through a mobile-friendly website or a government benefit provided online. The COVID-19 pandemic exposed the gaps in the government's ability to deliver services digitally, and TMF funding supports the creation or modernization of digital services with dramatic benefits to increasing access and equity, reducing fraud, and improving service delivery.

- Cross-government collaboration and scalable services. Across government, many of us are working hard to solve the same problems. We must think about strategies to accelerate digital modernization across the government, and having an enterprise mindset will help expedite this transformation. The TMF Board seeks projects that can replicate success of one agency throughout the government and improve how the entire government collaborates.

With such a significant investment, I understand the importance of oversight to the entirety of the TMF process – from the initial award of a project and throughout the project lifecycle to maintain its success. I will ensure that TMF project owners are held accountable to achieving results and that we are transparent with the public and Congress about the use of TMF resources.

2. Investing in our People

Every modernization plan, every new cybersecurity upgrade, every contract to bring in best-in-class industry capabilities depends on having a technically skilled federal workforce. To achieve this, we must attract the best minds from the broadest array of backgrounds to join us. The Administration believes our country and our government is at its best when it draws from the full diversity of our nation and everyone has a chance to fulfill a call to public service. Building our IT workforce is a necessary step if we want to achieve anything else, and we have a three-pronged strategy to do so:

- First, we must attract new talent. We have an impressive federal workforce, but the number of jobs that require IT competencies keep increasing, and we're not hiring fast enough to fill them. That's why teams built from the ground up to support innovative technical work and service

design, like the United States Digital Service or GSA's Technology Transformation Service team, are so important. These programs are critical to creating spaces that can recruit our nation's digital talent and bring them to bear on some of our government's toughest digital service challenges. Thank you for supporting their expansion in the American Rescue Plan Act.

- Second, we have to build the talent pipeline early. We know that growing our talent pool can't happen if we're only looking at the traditional pool of "cybersecurity or IT talent." We need to recruit diverse talent that is underrepresented in the federal workforce today, create more opportunities for graduates and junior professionals, and invest in K-12 programs that can support students who are interested in pursuing work in the technology field. For example, we are working with OPM and GSA to establish programs to bring in early career talent, train them not only in technology, but also inspire them to serve the American people throughout their careers. Another great example is the CyberCorps Scholarship for Service program at the National Science Foundation, which provides scholarships to college and graduate students pursuing cybersecurity-related degrees in exchange for subsequent government service.

- Finally, we will invest in retaining and revitalizing our current workforce through professional development programs like reskilling and upskilling. Just a few months ago, we concluded our first Data Science Training Program, in which 61 federal employees developed skills in managing large datasets, data visualization, and machine learning. As part of this program, they all completed capstone projects that addressed real business problems at their agencies. We look forward to building on this success as we look for ways to invest in other in-demand, technical skills.

3. Transitioning to Enterprise Collaboration & A Product Mindset

The federal government is fundamentally in the service business. Most of what we do directly with the American public—such as counseling small businesses, providing our veterans with health care, issuing passports, or delivering the mail—depends on our ability to understand what the public needs from us, to learn from them how we are or are not meeting their expectations, and to adjust our delivery methods to improve the way we deliver benefits and services to them.

When we have a product mindset, designing with users and not for them, we focus on delivering high-quality user experiences. Products continuously improve based on user feedback and metrics, and enable us to always make enhancements to customer delivery. This continuous improvement is necessary to advance product performance and keep our systems and infrastructure safe and secure. When we operate in this way, it results in exceptional customer experience -- making our government work better for everyone. I wake up energized at the possibilities to use technology to improve everyday interactions that our families, friends, and neighbors have with the government.

To get there, CIOs must be empowered to work across the enterprise. It's not our citizens' job to figure out how to navigate across department and agency silos to get better service delivery – it's ours. By working together and giving our colleagues the tools, resources, and workforce needed to transition their agencies to a "product mindset" – not one organized around information systems, but around users and services -- we can make significant progress. Retiring legacy systems and eliminating duplicative technology is a means to an end. By delivering modern, efficient tools and technology to our federal

workforce, we can reduce administrative burdens and enable our colleagues to focus on service delivery -- the main reason many chose to become public servants.

4. Embracing Innovation in Policy Development

We also need to think creatively in order to meet the moment. One change that I am championing is to begin developing new or refreshed IT policies by pairing our policy experts with technologists at the beginning of the policy-making process. This will allow us to lean in to the most innovative technology solutions that already exist in the private and public sectors while ensuring that we comply with applicable laws, rules, and regulations. By integrating delivery experts with policy experts and working together at the beginning of this process, we can test new ideas and help propel IT modernization across the government. We must raise government technology standards and practices to those of the private sector, and rely on open-source technologies, modern security practices, and pressure-tested solutions already in place. By embracing innovation and translating it into modern and secure policies and experiences, agencies will be best positioned to deliver best-in-class services for the American people.

Conclusion

Stepping into the role of Federal CIO brings challenges and great opportunities at a critical moment in history. Just as the COVID-19 pandemic forced us over the last year to reimagine how we accomplish our mission at every federal agency, this year will be about transitioning to a "new normal" state of operations. As we focus on the transition out of the COVID-19 pandemic and rebuilding the American economy, modern technology is essential to our long-term success – and it will enable our government to draw from the full diversity of our nation in recruiting the next generation to fulfill a call to public service.

My priorities shared today outline the investments, the people, and the focus that are critical to the end goal: delivering secure information technology across government and high-quality services to the American people. Technology is the underpinning of everything the government accomplishes. Your constituents who are relying on this level of service delivery – and our federal employees who need secure, modern tools and processes to deliver it to them – deserve nothing less.

Thankfully, as we begin this new chapter of federal IT modernization, we have a strong foundation on which to build. I am excited for the opportunity to enable the government's diverse missions as Federal CIO, and I look forward to partnering with Congress throughout my public service. Thank you for the opportunity to testify today, and I look forward to taking your questions.