September 16, 2022

Testimony of Federal Chief Information Officer Clare Martorana

House Committee on Oversight and Reform
Subcommittee on Government Operations

Hearing on
Project Federal Information Technology: Make IT Work

Introduction

Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee – thank you for inviting me to appear before the Subcommittee today. I am eager to update you on the current state of Federal information technology (IT), share progress, and highlight where the Administration is heading.

Progress on Federal IT across Federal agencies would not be where it is today without the Subcommittee's consistent bipartisan support of IT modernization and oversight of Federal IT. Since the enactment of the Federal Information Technology Acquisition Reform Act (FITARA) in December 2014, your steady oversight and accountability of agency operations through the FITARA Scorecard has incentivized agencies to advance targeted IT and acquisition priorities, reduce wasteful spending, and improve project outcomes. FITARA enabled Federal agencies to close over 4,300 data centers resulting in approximately $4.7 billion in data center cost savings, and Chief Information Officers (CIOs) to have a seat at the table. While this has accelerated our stride forward, we have found that agency CIOs must also have *a voice* as strategic executive "C-suite" partners to ensure the cybersecurity posture of the agency is strong and the agency is on an accelerated path to IT modernization. We therefore recommend that the CIO Reporting Relationship metric be retained in the FITARA Scorecard.

President Biden believes our Government needs to deliver for all Americans. It is technology that will power our ability to deliver a 21st century government to the American people – your constituents. With the right strategy, investments, workforce, and partnerships, we can continue making progress toward our shared goal: delivering a simple, seamless, and secure customer experience to the American people.

21st Century Government Delivery Begins with Cybersecurity

Security is the foundation of *every* Federal agency and underpins an agency's ability to deliver a simple, seamless, and secure experience for the American people. Our friends, relatives, and neighbors have secure, modern experiences every day when interacting with their favorite consumer services. Over the past 2 years, the expectations have become even higher for our Government to deliver the same. When I look at an agency's ability to meet this standard, I start by looking at their foundation: cybersecurity.

President Biden took office in January 2021 amid an unprecedented series of large-scale cyber-attacks against software supply chains, key Federal systems, and critical infrastructure, including the SolarWinds incident, unprecedented Log4j vulnerability, a series of Microsoft Exchange Server attacks, and the Colonial Pipeline ransomware attack. Previous approaches, policies, and agency cyber measurements were not sufficiently protecting Federal systems and information.

In the face of rising cyber threats, the Administration has prioritized strengthening our Nation's cybersecurity. The President's Executive Order on *Improving the Nation's Cybersecurity* (EO 14028) makes a significant contribution toward modernizing cybersecurity defenses by protecting Federal systems, improving information-sharing between the U.S. Government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur.

The intent of EO 14028 is to aggressively change the strategy and culture of the Federal enterprise to center around leading practices in the cybersecurity community. OMB is committed to ensuring that agencies have the guidance they need to successfully execute EO 14028, and – to that end – has released five policy memoranda on protecting critical software, logging, endpoint detection and response (EDR), zero trust architecture (ZTA), and the software supply chain. These policies include:

- **M-21-30,** ***Protecting Critical Software Through Enhanced Security Measures,*** builds upon guidance and security criteria published by the National Institute of Standards and Technology (NIST) to help agencies identify and secure software used for security-critical functions.
- **M-21-31,** ***Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents,*** sets detailed requirements for log management, configuration, and enterprise-level centralization. It also provides a maturity model that prioritizes the most critical software types and requirements.
- **M-22-01,** ***Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response,*** directs agencies to coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) to accelerate their adoption of robust EDR solutions, an essential component for ZTA that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.
- **M-22-09,** ***Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,*** **or the Federal Zero Trust Strategy,** sets forth a plan for migrating the Federal Government to a new cybersecurity paradigm that does not presume that any person or device inside an organization's perimeter is trusted, and focuses agencies on strengthening their capability to limit, and continuously verify, the access those people and devices have to government data.
- **M-22-18,** ***Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*** – which was published earlier this week on September 14, 2022 – initiates a Government-wide shift towards requiring agencies to use software developed in a secure manner. This will minimize the risks associated with running unvetted technologies on agency networks, increasing the resilience of Federal technology against cyber threats.
- Following the issuance of National Security Memorandum-10, *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*, my team is working with ONCD, in partnership with CISA, NIST, and the National Security Agency (NSA) to establish requirements for agencies to prioritize and identify where they are using cryptography within their most sensitive systems that is vulnerable to decryption by a future quantum computer.

OMB and ONCD are also partnering on the forthcoming National Cybersecurity Strategy to build a sustainable cybersecurity foundation to support our digital aspirations and the Administration's policy goals with respect to infrastructure, clean energy, equity, democracy, and economic opportunity. It will lay out the Administration's near-term investments in cybersecurity alongside the more deliberate and affirmative long-term construction of a secure digital future, of which my office will be responsible for executing the Federal component.

ESTABLISHING A COHESIVE APPROACH TO CYBERSECURITY INVESTMENTS

With differing levels of agency capability and diverse agency structures, cybersecurity outcomes across Federal agencies have varied widely. To assist agencies, OMB, in partnership with ONCD and other stakeholders, is working to assess where agencies are on their cybersecurity journey, identify and fill gaps, and ensure they are making the right investments at the right time to put their agency on a path to security – one that can successfully span across fiscal years and from administration to administration to meet real-time needs.

Building on the strategic direction set by EO 14028, *Improving the Nation's Cybersecurity*, OMB and ONCD issued M-22-16, *Administration Cybersecurity Priorities for the FY 2024 Budget*. This memorandum outlines the Administration's cross-agency cyber investment priorities for formulating fiscal year (FY) 2024 Budget submissions to OMB. By ensuring agencies have a strong cyber foundation, it will position them to retire legacy IT and launch technology that is secure by design, improve public facing digital services, enable the secure transit of data across agency silos to better serve customers across their Government journey, and set agencies on a path to achieving digital transformation.

Working as an Enterprise to Deliver on Our Mission

Securing and modernizing Federal IT takes a unified approach. As Federal CIO, I work daily with partners in OMB, ONCD, the United States Digital Service, and the General Services Administration (GSA) to drive impact by advancing four key priorities: Cybersecurity, IT Modernization, Digital-First Customer Experience, and using Data as a Strategic Asset. As highlighted through our June 2022 *Information Technology Operating Plan*, we are:

- **Championing consistency across the Federal IT and cyber enterprise**. This means working with partners across Government to align to the Administration's strategic IT priorities, achieving better outcomes by placing the customer at the center of everything we do, and leveraging shared tools and playbooks whenever possible.
- **Aligning resources to Administration priorities and delivering impact with the funds entrusted to us.** My team is partnering with OMB Resource Management Offices, ONCD, and others, to ensure agency budget requests are based on cybersecurity risk mitigation and strategic IT priorities with the goal of elevating data-driven insights to make the process more effective. Agencies will be expected to invest in and protect the systems, data, and services they manage on behalf of the American people and align future investments to an enterprise cybersecurity and IT modernization plan that spans multiple fiscal years, enabling the retirement of legacy systems and the launch of technology that is secure by design.
- **Driving innovation across the enterprise through innovative funding models such as the Technology Modernization Fund (TMF).** By building and launching modern tools, technology, and products that meet today's expectations, we show people what's possible, engage our Federal workforce, and inspire others to join us in serving our great country.

With Congress' support, we have already seen successes. Since the passage of the American Rescue Plan Act of 2021 (ARP), we have received more than 150 TMF proposals for projects totaling over $2.8 billion. The TMF Board has invested more than half of the TMF ARP funding, and – as the Board continues to invest the remaining ARP funds – our goal is to balance speed with ensuring we invest in high quality, impactful proposals that have a high likelihood of success. Looking ahead, we will focus on targeted investment areas, such as those in the Customer Experience (CX) Allocation announced in June 2022, as well as coordinate within OMB and with other key stakeholders to set goals for the next FY that better integrate agency budget requests and results.

OMB is also working across agencies to put the EO on *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* (EO 14058), into action. The Department of Agriculture's Farm Service Agency, which processes $7 billion a year in loans to family and farms, is in the process of building its online loan application, so that customers have the option to continue to submit a paper application or transition to a simplified online application. This is just one example of the progress being made across the Federal enterprise and the Administration is committed to building on successes such as this. this momentum. My office will continue to play our part, along with GSA, in developing Federal products and services that agencies can use to power a simple, seamless, and secure customer experience.

Driving and Sustaining Progress

Large-scale change as envisioned in the EO on *Improving the Nation's Cybersecurity* (EO 14028) and the EO on *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* (EO 14058) does not happen overnight; it requires continued investments, resources, collaboration, and cultural change derived from the visibility and support of leaders both within the Executive Branch and here in Congress. This work is based on technology best practices and will span multiple years across multiple administrations. As Federal CIO, I'm focused on ensuring we are putting the building blocks in place to enable future Federal CIOs and technology teams to achieve success.

One of the key ways we will impact change in the near-term is to ensure technologists are included upstream in the decision-making process. Since technology underpins an agency's ability to deliver on its mission, technologists have a unique understanding of the tools and technology in place – or perhaps needed – to deliver a product or service. Using human-centered design principles, technologists place customers at the center of the problem they're trying to solve – the Federal employee performing the work, as well as the end user they're trying to serve – and can vet the technical strategy to ensure it will be successful, driving down the failure rate of Federal IT investments. When technologists are missing from the process, it's a missed opportunity to deliver a product or service that will meet the needs of our customers. When technology investments fail, we lose trust with Congress, our partners in oversight, and the American people.

We have the ability to drive digital transformation across the Federal enterprise – and finally put an end to paper processes as the main way we conduct business in Government. Paper is slow, inaccessible in a digital world, a burden to the Federal workforce to process, and does not meet the bar for modern service delivery. We can do better, and we must.

With technologists being a key part of the process, we can deploy technology that is secure by design, maximize productivity, eliminate administrative burden, engage the workforce, and deliver Government services that meet modern expectations for the American people. With each new product and service we deliver, you will receive one less call, email, or letter from a constituent describing a fractured, frustrating experience with our Government.

We are demonstrating what's possible in digital service delivery by using technology and design to launch new products and services through the TMF. The TMF uses an iterative development model that enables us to improve outcomes and be more fiscally responsible. We partner with agencies to vet their technology strategy, ensure they have the team in place to execute the work, and provide executive support to work in new ways. Failure is a natural part of this process – but the key is to fail fast, course correct, and share lessons learned.

While outcomes from TMF investments do not happen overnight, outcomes from operating in a transparent manner – sharing data, case studies, playbooks, and reports – can and are happening now. Whether positive, negative, or indifferent, we're sharing what we're learning across the Federal enterprise so we can get smarter together. Transparency, information sharing, and collaboration are key to maximizing impact, and the TMF is leading by example.

OMB currently has an effort underway to publish information about agency cybersecurity risk and performance in order to provide Congress and the public with an accurate picture of how agencies are performing on key Federal cybersecurity indicators. I am also looking at ways we can measure agencies' digital efforts and look forward to releasing new website metrics with GSA in early 2023. A website is often how an individual first interacts with an agency, so it is important to track metrics across Federal public-facing websites to evaluate whether they meet the public's expectations for security, accessibility, design, and compatibility with mobile devices.

As worldwide technology capabilities rapidly evolve, so must Government technology, security, data collections, and IT policy. Our policies and practices must be as nimble and iterative as the emerging technology products and the evolving service expectations of our users. Getting this right by modernizing IT, maximizing taxpayer dollars, and eliminating administrative burden for both our customers and the Federal workforce will enable the Government to deliver the services that Americans rightly expect.

Thank you again for the opportunity to testify today, and I look forward to answering your questions.