Testimony of Ann Dunkin

Chief Information Officer

U.S. Department of Energy

Before the

Subcommittee on Government Operations of the

House Committee on Oversight and Reform

January 20, 2022

Introduction

Chairman Connolly, Ranking Member Hice, and distinguished Members of the Committee, it is an honor to appear before you on behalf of the Department of Energy (DOE).

On behalf of Secretary Granholm and Deputy Secretary Turk, I thank you for providing me this opportunity to testify about DOE's implementation of the Federal Information Technology Acquisition Reform Act (FITARA). I would like to thank the Subcommittee for its leadership and bipartisan oversight of agency implementation of FITARA, which has enabled us to make real progress at DOE—progress that I'm excited to build on as the Department's CIO.

I want to start by sharing my own background in the public and private sectors so you can understand where I'm coming from. I am an engineer— not an information technology (IT) professional — by education. I spent the first part of my career working for Hewlett Packard (HP) in manufacturing engineering, operations, software quality, R&D, and, eventually, IT. After I left HP I moved to the public sector, joining the Palo Alto School District as its Chief Technology Officer. In 2014, I was nominated by President Obama to be the Assistant Administrator for Environmental Information for the Environmental Protection Agency (EPA) and I joined EPA later that year as Chief Information Officer (CIO). The EPA staff were some of the most capable and dedicated professionals I had ever worked with and taught me a great deal about how the federal government works.

After leaving EPA, I served as the CIO of Santa Clara County and spent a year at Dell. I'm thrilled to return to government as DOE's CIO — and work with another group of such highly capable and mission driven staff. I believe that the public and private sectors have much to teach each other, and that both sectors benefit when individuals move between the two. I bring my combination of public and private sector experience to bear as I guide the Department's digital transformation, IT modernization, and cybersecurity programs.

In alignment with the requirements of FITARA, I report directly to the Secretary and Deputy Secretary. I have their full support to drive change and make enterprise decisions that are necessary for the efficient delivery of secure, innovative, and value-added federal services. The implementation of FITARA at DOE is led by me, with active collaboration from the Department's Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO), and Senior Procurement Executive (SPE). FITARA and other associated laws, such as the Federal Information Security Modernization Act (FISMA) and the Modernizing Government Technology (MGT) Act, provide the Department with the authority necessary to accelerate our work to improve DOE's IT and cybersecurity programs.

I am pleased to testify today on the progress we are making in exercising our FITARA authority, which is reinforced by the support I receive as a direct report to the Secretary and the Deputy Secretary. I will share updates about how FITARA has shaped our technology, innovation, and cybersecurity efforts and informed our approach to working within DOE's unique operating environment. Although we have made significant progress, I want to acknowledge that DOE still faces challenges. I am committed to driving this important work ahead, and I look forward to working with you and keeping you informed on this effort.

Within the Department, our governance framework is our vehicle for fully implementing FITARA. This framework, under the direction of the Cyber Council, chaired by Deputy Secretary Turk, helps us effectuate change, enable collaboration, initiate new value conversations, and accelerate modernization efforts across DOE.

FITARA helps to ensure that DOE's IT and cybersecurity programs are strong enough to support and enable the vital work of the Department across the three main priorities set by Secretary Granholm: Combating the Climate Crisis, Creating Clean Energy Union Jobs, and Promoting Energy Justice.

Every year we become more dependent on technology in our work and personal lives. Since FITARA was enacted, our use of technology has increased dramatically and changed the way we live and work in fundamental ways. While this ever-expanding use of technology generates new opportunities, it also creates ever-expanding and evolving risks. We are in a challenging and dynamic environment where we must protect our valuable digital assets, assess threats and risks in an increasingly hostile cyber environment, and meet growing customer and regulatory expectations—all without degrading our ability to innovate and modernize. Today I would like to briefly address how we can bring this all together and make it work.

FITARA

Rapidly evolving technology can help us better serve the American people—and do so faster, driving change through continuous innovation while balancing risks. We need a bold vision, empowered workforce, mature IT management practices and processes, and strong governance combined with solid technology leadership. I believe that's exactly what FITARA helps us achieve. As the DOE FITARA program continues to mature — including at our national laboratories, Power Marketing Administrations (PMAs), plants, and sites—we will continue to focus on:

- enhancing our visibility into and understanding of IT-related resources and investments and their relationship to mission priorities;

- supporting CIO and IT management authorities at all levels of leadership and management throughout the Department;
- improving our cybersecurity posture;
- implementing new and updating existing policies and processes for managing IT resources from planning to execution; and
- strengthening governance and oversight processes.

I want to share a few highlights from our FITARA implementation, as well as our implementation of MGT and FISMA, and the areas where we have been able to influence and change behavior.

IT Budget Planning: The DOE Office of the Chief Information Officer (OCIO) manages the Department's IT portfolio, consisting of investments from all departmental elements, including the management and operating (M&O) contracted national labs and environmental clean-up sites, as well as the Power Marketing Administrations (PMAs). OCIO also leads the Department's Technology Business Management (TBM) implementation, enhancing my ability to be an active partner in IT budget decision making through increased visibility into IT spending. OCIO provides IT-related budgeting guidance to the Department to assist with annual budget formulation. I receive annual cybersecurity budget briefings from several larger departmental elements to ensure I am aware of major funding needs and gaps. In addition, as part of the annual budget planning process, departmental elements are asked to provide a consolidated list of planned IT acquisitions for OCIO review.

These processes enhance visibility into IT investments and strengthen alignment with mission priorities through:

- increasing collaboration and providing opportunities for improved transparency and resource alignment;
- identifying potential uses of Enterprise Wide Agreements (EWAs);
- affirming security controls such as FedRAMP, Supply Chain Risk Management (SCRM), and security authorizations; and
- streamlining the planning, budgeting, and acquisition phases of IT investments.

IT Acquisition: In addition to defining processes for ensuring all IT related contract actions have been reviewed and approved by the CIO, we also built an EWA program that identifies, acquires, and oversees contract vehicles for widely-used, commercially-available products and services across the entire Department. This program enables DOE to reduce duplicative work within the enterprise, take advantage of economies of scale and be good stewards of taxpayer dollars. DOE integrated the SCRM process into all IT acquisition processes and we are establishing SCRM timeframes and assessment capabilities to reduce supply chain risks. This will further enhance our cybersecurity posture through use of trusted vendors. Overall, the EWA program achieved savings of $217 million and is a significant contributor to DOE's total portfolio savings of $542 million for the period FY12 to FY22. One example of the results of the EWA program is we recently established enterprise agreements with three major cloud service providers.

Data Center Consolidation: The Department closed 146 data centers since the inception of the Data Center Optimization Initiative (DCOI). We expect to close another seven data centers by 2025. DOE continues to build supercomputers at a rate of one per year to meet our national security goals. We will continue to support and optimize data centers that house these important assets while we continue to strategically close commodity data centers.

Sustainability is an important value to me and to DOE. We are committed to sustainability, including through increasing the energy efficiency of our data centers. To assist with optimization of energy use at data centers, DOE utilizes a collection of innovative tools which includes products developed by one of our national laboratories to improve the efficiency of our data centers. The tool identifies areas where we can improve energy efficiency, including by monitoring how much energy our infrastructure uses, measuring the power and utilization levels for servers, and providing key predictive analytics to increase efficiency. Among other important capabilities, it can be used to determine the best time to run large simulation models, helping us save on energy costs by scheduling jobs during off-peak hours.

Transition from Networx: DOE is transitioning from the old Networx telecommunications systems to GSA's Enterprise Infrastructure Solutions (EIS) for enterprise telecommunications and networking solutions. DOE has awarded contracts for both data and voice. While our contract awards were made later than we would have preferred, DOE is confident we can meet the GSA disconnect target of September 2022. We will be leveraging GSA's expertise, as well as that of our transition management vendor, to implement risk mitigation strategies and to accelerate our transition.

Innovation

I would now like to provide an update on some of our initiatives to enhance innovation at the Department, especially by leveraging the MGT Act (Pub. L. No. 115-91). The MGT Act supports our wide-ranging and ambitious modernization efforts, including upgrading our IT systems, moving systems and data to the cloud, and implementing new infrastructure. Continuing this progress will be crucial for the success of the innovation efforts that I'm leading at DOE and—in my capacity as chair of the CIO Council's Innovation Committee—across the federal government.

Working Capital Fund: DOE utilizes the Department's Working Capital Fund (WCF) for some IT services. We are also exploring the option of creating a new WCF for IT modernization and evaluating options to add more services to DOE's existing WCF. This evaluation is a joint effort of the CIO and CFO.

Technology Modernization Fund: DOE was an early advocate and adopter of the MGT Act's Technology Modernization Fund (TMF) and was initially awarded $15 million dollars in 2018 as part of the first cohort of TMF projects. This award funded migration of email from legacy, on-premises servers to cloud services. We were happy to see that the American Rescue Plan (P.L. No. 117-2) provided additional TMF funds to address urgent IT modernization challenges, bolster cybersecurity defenses following the SolarWinds incident, and improve the delivery of COVID-19 relief. The TMF has the potential to be a transformative funding vehicle for DOE, enabling us to modernize and secure our environment. Since the release of the TMF ARP guidance, DOE submitted three TMF proposals totaling approximately $55 million. These requests, if approved, will give the Department the opportunity to make significant investments in secure cloud architecture, business system secure client service architecture, and reduce technical debt across the Office of Science. That said, given the large number of requests received for this round of the TMF, the current $1B allocation is far less than the demand for TMF funding.

Cybersecurity

Next, I would like to address the vital work we are performing to secure the DOE enterprise.

DOE continues to make progress toward improving our cybersecurity posture. Our efforts are focused on:

- strengthening enterprise visibility and situational awareness;
- combating advanced persistent threats;
- forging interagency and sector partnerships to protect critical infrastructure;
- promoting information sharing;
- enhancing policy and guidance; and
- advancing technologies for cyber defense.

DOE is responsible for a diverse mission spanning nuclear security, classified and open science, energy generation, and environmental management. The varying security needs within DOE's mission space present unique cybersecurity challenges, requiring our risk management program to be flexible to allow leaders to make risk-based decisions that enable the mission. Under the existing DOE Cybersecurity Order 205.1C, heads of department elements are given significant autonomy to manage their cybersecurity programs. The approach requires significant coordination and collaboration to assure and report compliance and cyber performance at the enterprise level.

We are encouraged by the new FY22 FISMA Guidance and Metrics and the shift from pure compliance to a more risk-based approach to cybersecurity, which will allow DOE to focus on our highest priority mission areas and risks. We continue to work closely with the Office of Management and Budget and CISA on efforts to continuously improve FISMA and ensure that the metrics that are tracked are timely and relevant.

The Department is also leveraging the Department of Homeland Security's (DHS) Continuous Diagnostic Mitigation (CDM) program to obtain additional security tools, including, most recently, hardware and software asset management. While these tools were delayed due to pandemic-related funding shortfalls, we are looking forward to significant increases in enterprise visibility as we roll them out in the coming months.

DOE has also made investments targeting vulnerability management, big data analytics, crowdsourced penetration testing, enhanced training initiatives and workforce engagement. These are all designed to improve enterprise-level visibility and foster the level of collaboration necessary to accomplish our mission.

IT and Cyber Workforce Development

As we face an ever-growing shortage of cybersecurity and IT talent, I am focused on strengthening DOE's IT and cybersecurity federal workforce by bringing new talent on board with a focus on hiring women and underrepresented minorities. According to CyberSeek, a Department of Commerce funded project to understand the cybersecurity job market, nearly 600,000 cybersecurity jobs are vacant across the public and private sectors nationwide. At DOE, we are implementing a multi-pronged approach to compete for talent. We regularly leverage our direct hire authority, which enables us to fill certain IT, cyber and information management positions more rapidly and DOE is engaging across the federal enterprise to discuss and implement increased incentives for cybersecurity professionals.

DOE's OCIO, along with the Office of Economic Impact and Diversity's Office of Minority Programs, the Office of Science, and the National Nuclear Security Agency, recently launched the Omni Internship Alliance. This paid internship program is designed to employ students from overburdened and underserved communities and provide these students the opportunity to intern at DOE. The program seeks to build new career pathways for students from underserved communities while simultaneously building the cyber/IT talent pipeline needed to support the energy sector in the years ahead. Interns will hold appointments at DOE national laboratories, PMAs, plants, headquarters, and other approved sites, where they will receive hands-on job experience in an immersive environment that provides them with an understanding of the mission, operations, and culture of DOE.

I would now like to share some thoughts about the future of IT at DOE and across the federal government.

Lessons Learned on Accelerating Innovation

Almost a decade ago, we recognized the way the government had been buying and building technology took too long, cost too much, and failed too often. This resulted in a concerted effort to make government better and deliver services that we can all be proud of. That includes the launch of a variety of digital services, teams, approaches, and playbooks across the government. We have learned how to use agile development and implement Development, Security, and Operations (DevSecOps) pipelines. We learned that our challenges are not technology related, but rather that they are caused by people, processes, procurement, policy, and politics. Congress passed laws like FITARA and the MGT Act to enable these changes. While many of us now understand that to change the services we deliver, we need to change our culture, our progress—while real—has been inconsistent and slow.

The government's response to the COVID-19 pandemic provided a window into what government services can look like when we move fast. DOE and every other department and agency pivoted to nearly one hundred percent telework and did it seamlessly. Agencies stood up new portals and processes and disbursed trillions of dollars through new and existing mechanisms. We moved at the speed of need because lives depended upon it. In the process, we proved that government can move fast and deliver exactly what is needed when we remove many of the cultural, process, and political constraints that make us move slowly.

To innovate at scale, we need to utilize shared services, increase reuse through microservices, and scale the tools and practices that enable transformation across agencies and the government. Low-code software development platforms, DevSecOps pipelines, and rapid Authorization to Operate or “ATO” processes are all critical building blocks for driving innovation.

While we cannot and do not want to operate in a pandemic-induced crisis all the time, our response to the pandemic inspired DOE to double down on our efforts to make DOE better, remove barriers to innovation, and lead change across the federal government. To address this, I am leading the development of an innovation playbook to capture critical strategies for scaling IT innovation. This playbook will gather the input of thought leaders across government and the private sector and will become a resource not only for DOE but also, in collaboration with the CIO Council, for departments and agencies across the federal enterprise.

At DOE we are committed to modeling the plays in the playbook we are developing. My office has set up low-code application development platforms in a shared services model to streamline access to enterprise-class solutions. These platforms will serve as a launchpad for modernizing aging systems and provide DOE more opportunities to shorten the timeline between concept and deployment.

Conclusion

When I was CIO of EPA, you may have heard me say that FITARA is a great law that helps CIOs make the government better. I also appreciate FITARA and leadership from Congress and the White House at a deeper level because of my experience in other roles where I could have used a little extra authority behind my calls for increased agility, costs savings, and security. So, it’s not surprising I still believe FITARA laid the groundwork for CIOs to lead significant cultural change and create organizational habits and behaviors enabling greater collaboration and agility. I am committed to driving these improvements and outcomes forward, keeping the legislative intent front and center as we optimize our operations.

To sum up, there is a lot more to accomplish—as there always will be, because technology evolves far faster than we can move—even at our very best. But I’m confident that with my team’s commitment, dedication, and passion, and with the leadership of Secretary Granholm and Deputy Secretary Turk, we will achieve significant results. The pandemic elevated the visibility and raised the stakes of our work, but it also showed we have the vision and the momentum necessary to enact real transformational change. It is my pledge to you today that we will be relentless in our work to strengthen the Department of Energy by effectively implementing FITARA, and I look forward to working with each of you as we proceed.