Written Testimony of Max Everett
Former Chief Information Officer (2017–2020)
at the U.S. Department of Energy

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

April 27, 2021

Chairwoman Hassan, Ranking Member Paul, and Members of the Committee, thank you for the opportunity to speak on this important subject.

I have spent almost two decades in and around Federal IT, both as a Federal appointee and a contractor. I hope to candidly share what I have observed in that time.

The events of the last year have illuminated how truly critical dealing with legacy IT is for the effective operation of government. Dealing with the need to allow our Federal workforce to work remotely, providing efficient access to government services to all Americans impacted by COVID, and protecting our systems from recent serious cybersecurity attacks have all put this subject front and center.

I would begin by suggesting that we must be broad in our view of what constitutes legacy IT. It is not only those obvious systems that have passed their end of life – whether they are mainframes or unsupported software. It includes cobbled together systems like paper-based forms or outdated front-end websites that prevent customers – citizens – from finding what they need quickly and effectively.

One way to measure the value of our systems is data. We can look no further than the Federal government's efforts to combat COVID over the last year to understand the importance of data. Data helps us measure effectiveness and predict where resources should go to have the greatest impact. Yet some of the most valuable data the Federal government has continues to be locked up in our legacy systems, and often on paper.

During my tenure as Chief Information Officer (CIO) at the Department of Energy (DOE), we began focusing on the move to electronic document management to improve service delivery for citizens and liberate data from paper that was often merely filed away in a drawer or warehouse. I have been encouraged to see that effort continuing at across government under the path put forward by the 21st Century IDEA Act.

As we discuss the road from legacy systems to IT modernization, we must focus on sustainable and continuous innovation. One of the most straight forward ways we can talk about this challenge is in the two categories of people and process.

The people problem in Federal IT is significant. Our current human capital system is simply ill-prepared to meet the demands for recruiting, re-training, and retaining IT professionals of all kinds. The current channels for recruiting are not effective in reaching new and broader pools of candidates. Our job descriptions are often outdated and focused on irrelevant qualifications for the needs at hand.

As CIO at the Department of Energy, I often faced significant challenges exercising the expanded hiring authorities that I had on paper. The private sector offers more money and often more engaging workplaces. I believe we should continue to seek new paths for Departments and Agencies to be creative in bringing new technology talent into their ranks.

The good news here is that we have existing options. Progress has been made on greater hiring authorities for technology roles, but those need to be enforced and communicated across the Federal Human Capital community. The recent increase in funding for the US Digital Service will bring an influx of skilled technologists who can make an immediate impact.

Growing the number of digital focused internships and fellowships also provides an opportunity to let future leaders in the technology community see some of the unique challenges they can address in Federal government. Who else can offer an immediate opportunity to positively impact every American?

Contractors are also an incredibly important part of the staffing for IT across the Federal government. Technology contractors typically outnumber their Federal employee counterparts by three or four to one and sometimes even more. Contractors offer the ability to quickly onboard staff with new skills or access specific technical skills sets for short periods of time. I believe it is very important to keep our reliance on contractors in mind when discussing IT staffing solutions.

At DOE, we moved our primary IT services contract to a managed services model. This simply means we provide business requirements to our contractor and ask them to use their experience and capabilities to provide a result. This moves us out of the realm of micromanaging contractors that has failed time and again across government.

Process is a broader issue and one that I believe Congress can assist with by continuing to demand adherence to the laws already in place.

I am a biased observer, but I believe CIO authorities are critical to the success of modernization. I was fortunate to have the support of the Secretary and Deputy Secretary while I was at DOE. In fact, our Department moved into compliance with FITARA as soon as I joined when my reporting structure was moved to the Secretary and Deputy Secretary. Several agencies followed our lead afterwards.

That reporting structure and access allowed me to understand the priorities of the Department and engage other senior leaders as peers in conversations on budgeting and cybersecurity risk management.

Turning to other existing tools, the Modernizing Government Technology (MGT) Act can play a critical role in supporting accelerated modernization across Federal government.

The Department of Energy received one of the first Technology Modernization Fund (TMF) awards in 2018, something I take great pride in. I was incredibly encouraged that Congress provided $1 billion dollars to the TMF fund. That level of funding shows that Congress has prioritized modernization in a way that expects measurable results.

I would note that TMF is not simply about the money. TMF represents a methodology for managing IT and modernization. To receive a TMF award, the agency must demonstrate an understanding of their total cost of ownership for systems and show the numbers. That is a fundamental change in how technology is managed in the Federal government, in my experience.

One of the challenges we have seen in TMF projects is that the repayment requirement makes it very difficult to use for much needed projects that improve citizen and customer experience on websites and public-facing systems. It is notoriously hard to quantify cost savings for those type of systems.

With that in mind, I am supportive of suspending or waiving repayment of the TMF funds, but ONLY if the process is followed. The rigor in reporting and oversight that TMF brings Federal IT is, to me, just as critical as the dollars.

A second element that is less often discussed in the MGT Act is the IT working capital fund. Establishing these funds has been hamstrung at many Departments, but I believe they are invaluable to CIOs. Managing IT in the Federal government is already challenging, but most CIOs must spend an inordinate amount of time dealing with "color of money" issues. Single year money that must be spent by the end of a fiscal year is a recipe for incentivizing bad decisions.

Most major government systems are capital expenditures (CapEx). A large amount of money is spent over a set time to build the systems. The spending moves to operations and maintenance – O&M. An unfortunate process then begins in which we often run that system until it is already at the end of life before someone realizes it needs a radical update or replacement. Those costs necessary to modernize the systems accrue over time in what we call technical debt.

If the organization has single year funding, there are few options for saving over time to fund modernization of those larger systems. One is asking for a large appropriation for the new system, all too often without any analysis of how the previous system performed, or any type of cost benefit analysis. The second option is that a clever Federal manager might be able to put money aside in various ways if they have access to multi-year money or other funding mechanisms. The most common option is simply robbing Peter to pay Paul. Forced by necessity, other services or systems are cut to fund the updated system.

There are a few ways to improve this situation. The first is establishment and funding of Technology Working Capital Funds as envisioned in the MGT Act. This will allow Departments to fund larger modernization projects over time in a formal and visible way.

The second is moving to operational expenditure (OpEx) focused models – Software as a Service (SaaS) and cloud solutions. This is a less discussed value of using cloud solutions, but it allows for better management and projection of costs over time while building in the cost of upgrades and enhancements.

I will finally briefly mention cybersecurity, which is obviously top of mind for all of us in the IT community given the attacks on our systems over the last few months.

Modernizing our IT systems is a clear critical step in protecting the Federal enterprise. Cyber defenders already face significant challenges against dedicated nation state adversaries, but the odds against them become overwhelming when attempting to defend out of date and un-patched systems.

Our old models under FISMA, measuring cybersecurity over the course of months and years, is woefully inadequate. We have depended on compliance frameworks that are not focused on risk far too often. Most organizations simply do not have the time to keep up with all the cybersecurity checklists they are

asked to fill out, and so we have far too many people focused on that rather than the fundamental work of managing risk in real time. We must move to models for continuous monitoring of systems, which will require data and visibility at network speed.

Programs like FedRAMP need additional resources and must speed up so that we can bring innovative new solutions to the Federal market faster. Architectures like zero trust must be evolved and become the standards for additional defense in depth of our Federal networks.

My experience has been one of seeing slow and steady progress in these areas over the years, but our need for rapid progress has never been greater. As budgets increase for our technical needs, it becomes ever more important that we evolve and improve how we manage Federal technology.

I believe continuing the improvements embodied in legislation like FITARA and the MGT Act will make it easier to recruit some of the best and brightest innovators to become CIOs and digital leaders in Federal government. Many have given up substantial income in the private sector to join government out of a desire to serve, only to encounter bureaucratic processes that prevent them from making a real impact.

These changes will also have a direct impact on improving our Federal cybersecurity posture. Modernized systems will be more manageable and defendable for our cybersecurity teams across government.

Thank you again for inviting me here today. I look forward to answering your questions.