

Opening Statement
Hearing on “Using Cutting-Edge Technologies to Keep America Safe”
Subcommittee on Cybersecurity, Information Technology, and Government
Innovation

1:00 PM, Thursday, June 22, 2023

Rep. Gerald E. Connolly (D-VA)

Today, the Subcommittee has invited three cutting-edge technology companies and their products into the hearing room to help us envision the kinds of gadgets the federal government could use to enhance our nation’s security. But before we get ahead of ourselves, it is important to remember our Subcommittee’s mission. At the beginning of this Congress, all the Members sitting on this dais were vested with the responsibility to conduct dutiful oversight over “information security, including cybersecurity and privacy; government-wide federal information technology management and innovation; and procurement.” I hope those oversight imperatives are not lost among the excitement over robot dogs and unmanned aircraft systems.

I am grateful to our minority witness, Dr. Benjamin Boudreaux a former diplomat at the State Department and privacy expert, for coming today to share his expertise on an issue explicitly within our jurisdiction. I am, however, deeply disappointed that the majority planned a hearing to discuss “the adoption and sustainment of these innovations by federal agencies, including those related to the federal procurement process,” and yet we have no federal agency witnesses nor procurement policy experts here to share their perspective.

Federal IT modernization efforts, procurement policies and federal contracting issues rarely make the front-page news, but the consequences of these programs are significant. We need to get them right. The Government Accountability Office (GAO) estimates that the federal government’s fiscal year 2023 IT investment budget will be \$122 billion. These kinds of budgets deserve and require our attention and focus.

As many of you know, I have held 16 FITARA Scorecard hearings, and the reason we continue to do so is because of the results. Since 2015, our oversight efforts closed 4,000 unnecessary data centers—saving taxpayers \$4.7 billion. We have also saved taxpayers approximately \$25.2 billion through the PortfolioStat initiative and increased the number of functioning working capital funds at federal agencies from zero to five — providing federal agencies with opportunities to fund much-needed technology upgrades outside of the unpredictable annual budget

process. Nine additional agencies plan to establish working capital fund. These savings are huge, and the effects of these modernization efforts are revolutionary. It is often rare that bills save money, no less billions of dollars. These examples poignantly display how vital it is that we stay committed to oversight efforts and get our IT fundamentals right. New toys and innovations are fun and can help agencies meet their missions. But getting fundamentals right is what ensures government delivers for our constituents. One way we can ensure effective and efficient delivery through fundamental practices is through upholding procurement standards.

It is no secret that I spent the last five years of my career in Congress dedicated to codifying the federal government-wide compliance program, the Federal Risk and Authorization Management Program also known as FedRAMP. After leading the effort to pass this bill six times in the House, it was finally signed into law just last year. What made this effort to ensure a standardized approach to cyber security assessment, authorization, and continuous monitoring for federal cloud products and services a success was a dedicated concerted effort backed by invested stakeholders. It wasn't flashy new tools in search of need, it was a deliberative, bipartisan collaboration with those who understood the value of procurement policy and prioritized and standardized cybersecurity services.

Today, we continue to improve the cloud authorization process with stakeholders representing federal agencies, small businesses, and private industry so that we instill appropriate guardrails to ensure the United States is acquiring technology effectively, efficiency, and responsibly. The business of government requires careful and deliberate use of taxpayer dollars — and is not the same as Silicon Valley's mantra move fast and break everything. Our mission requires that each action is a deliberate choice that serves the public and protects our democratic values —including privacy.

While technological advancements come with many benefits, we must learn to balance the added convenience and capabilities with the ongoing risks against our civil rights and civil liberties. Foreign governments like China have taken emerging technologies like facial recognition to an extreme, using it to expand domestic surveillance, detect ethnicities, label individuals, track their movements, and take oppressive actions against certain ethnic groups. While the U.S. government is far from using technologies for these kinds of egregious surveillance tactics, we cannot continue to stand idly by as other countries dictate the technological and moral standards. America should be out in front with its own standards and condemn the use of technologies to violate civil and human rights.

As someone who comes from industry, I understand how public-private partnerships can deliver public services. But these partnerships must provide for good stewardship of taxpayer dollars as well as help government serve and protect constituents. I look forward to learning more of how Congress can foster adequate safeguards for deploying new and emerging technologies in the federal government that protect privacy and civil liberties – and ensure equity and fairness in federal contracting.