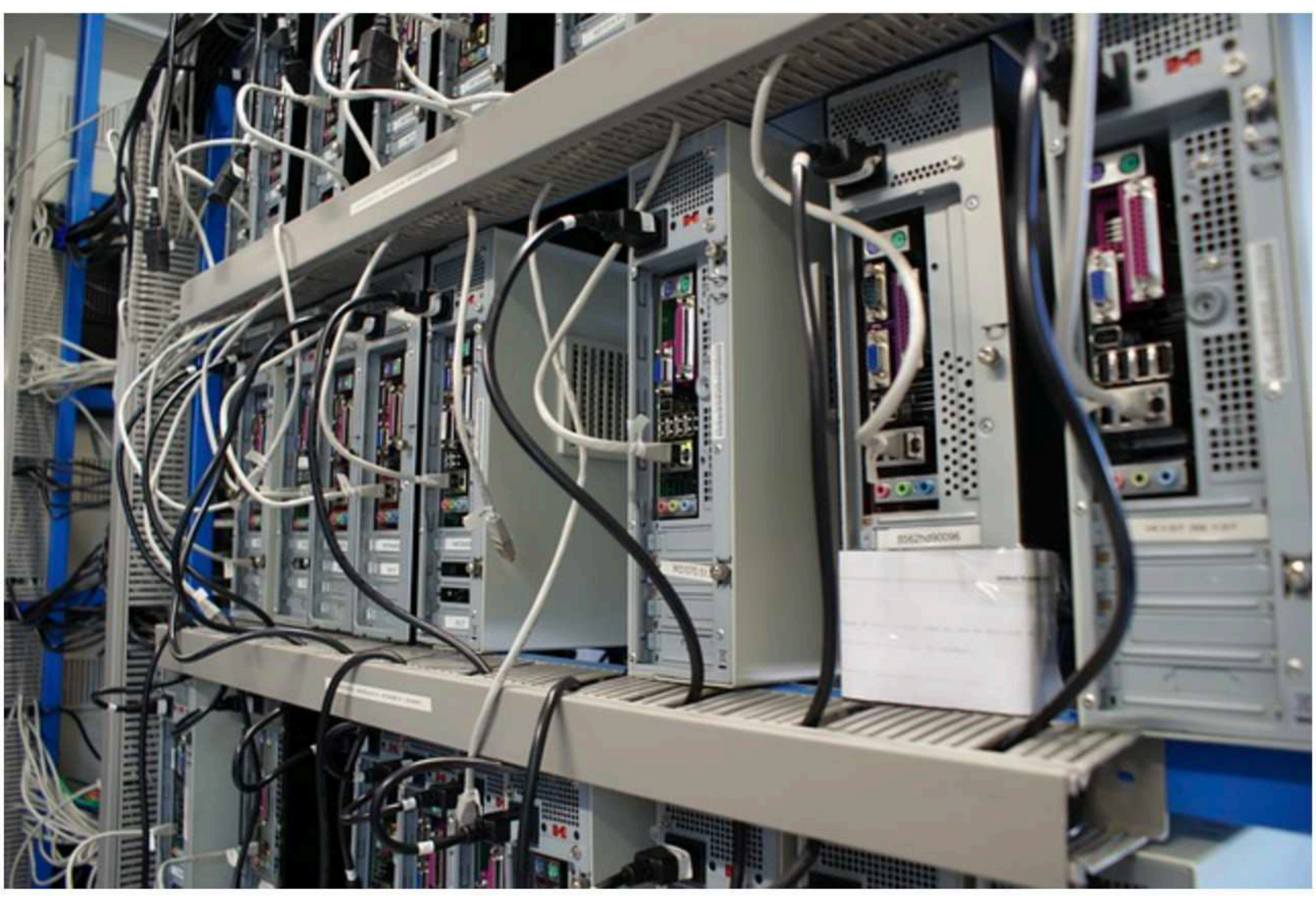
The DATACENTER Journal
Where IT, Facilities and Design Meet

Federal Agencies Should Focus On Mission, Not On Managing Data Centers



With a stroke of the pen, President Trump took one small step in dismantling the federal government's IT bureaucracy. And yet, if done right, his May 15 executive order (EO) could turn into the giant leap that finally brings a major part of our government's IT systems into the twenty-first century. As they say, the devil is in the details when executing any complex IT strategy, especially one that has enormous potential for today's cloud-service providers, data center operators and systems integrators. The ability to transform our government's aging IT infrastructure into one that befits the most powerful nation on Earth is long overdue.

The federal government has certainly been trying, though. In 2010, the Office of Management and Budget (OMB) launched the Federal Data Center Consolidation Initiative (FDCCI) to eliminate redundant federal data centers, improve the government's cybersecurity posture, reduce federal data center energy usage and save cost. The Federal Risk and Authorization Management Program (FedRAMP) launched in 2011 to accelerate cloud adoption across the federal government while appropriately handling cybersecurity risks and Federal Information Security Management Act (FISMA) rules. In 2014, the Federal Information Technology Acquisition Reform Act (FITARA) was enacted; among other things, it codified and built on the requirements of the FDCCI. In an August 2016 attempt to clarify the data center objectives of FITARA, the Data Center Optimization Initiative (DCOI) launched; one of its goals was to move from "core and non-core" data centers to industry-standard "tiered" data centers, adding new optimization metrics, and continuing efforts to close data centers and report cost savings.

Despite these multifaceted attempts over the years, CIO Dive reported that a November 2017 Congressional hearing found federal agencies performed at an overall C level according to a FITARA score that assessed their "digital hygiene." Unsurprisingly, a "majority of this hearing focused on data center optimization and transitioning to the cloud" and as to how disappointing various agency efforts had been up until then. In fact, an April 2018 Federal Times article offered this searing indictment of the Defense Department's data-consolidation efforts: "Dave Powner, director of IT management issues at GAO, said that the DoD has also failed to realize savings in IT modernization efforts. According to Powner, the department could have saved an estimated of $4.8 billion when data center consolidation efforts began, but has instead only saved a few hundred million dollars."

In addition, a 2017 State of Federal IT Report concluded that besides cost, several management issues relating to accountability, risk and policy hampered the modernization of the federal IT infrastructure at several agencies. From an accountability standpoint, inconsistent and constantly changing metrics yielded high compliance costs for agencies and made it difficult to measure and report the true cost of maintaining federal IT infrastructure. Also, many CIOs cited their agency's dated and obsolete IT infrastructure as an obstacle to meeting the rising expectations of citizens, employees and others. And, most importantly, IT policy and appropriations law didn't allow agencies to redirect operations and maintenance funding to update the IT systems that directly support their mission and goals.

Given these ongoing, complex issues, which are further compounded by a stifling federal bureaucracy, it's no surprise that the president's EO renews calls for an "agency-wide consolidation of the agency's IT infrastructure"—by eliminating unnecessary IT-management functions, merging or reorganizing agency IT functions, and increasing the use of industry best practices—across all government agencies. Most significantly, the EO requires that the CIO's role be dramatically enhanced so as to enable the implementation of appropriate risk-management measures and that each agency is empowered to prioritize "procurement of shared IT services, including modern email and other cloud-based services."

Such a massive consolidation of IT infrastructure typically requires moving costly, resource-hogging in-house data center operations to professional, efficient off-site data center. The best data center operators in the private sector offer a wide range of services from colocation to private-, public- and hybrid-cloud services as part of a comprehensive portfolio. I0n trying to overcome vulnerability to data breaches and persistent cybersecurity threats, however, many federal agencies have nevertheless made expensive and inefficient forays into data consolidation by running their own facilities in the naive belief that they'll be better protected if they control their own "sandbox."

And yet it's the control of the sandbox that's the elephant in many federal agencies' IT rooms. In a recent article responding to another presidential directive that makes it easier to fire federal employees for poor performance, Stewart Liff rightly points out that "the real problem is the culture of the federal government, which tends to encourage inaction over action." And that's the problem: the poorly managed efforts of federal agencies in their various snail-paced data consolidation and related cybersecurity-enhancement efforts, even as they try to gain control of their own sandbox by attempting to run their own data centers.

So it's high time the federal government got out of the data center business and looked to both commercial IT and public-private partnerships to get the job done in a more timely and cost-efficient manner, as the EO suggests. Implementing one of the EO's main demands—that is, to "enable agencies to reduce costs, mitigate cybersecurity risks, and deliver improved services"—requires adopting what we call a cloud-neutral approach to data consolidation in order to meet all of the EO's requirements.

At the heart of this approach is a state-of-the-art data center, designed with a deep knowledge of federal agencies' capital and operating expenditures. More importantly, a cloud-neutral data center offers the best of both the colocation and cloud worlds—it's the hybrid solution that makes perfect sense for the federal government. In addition to all of the physical data center requirements, including geographic location, diverse redundant communications infrastructure, scalability on demand and so on, a cloud-neutral solution necessarily hosts the on-premises cybersecurity services mandated by the federal government.

But even when the federal government begins outsourcing its data-consolidation efforts as this EO requires, it must simultaneously change how it pursues procurement of related IT services. The current model that first selects a prime contractor—typically a systems integrator (SI) and/or managed-services provider (MSP)—and then relies on that prime's to pick a technically relevant data center must be overturned. The cloud-neutral data center should be either the first choice or a mandate in the government's request for proposal (RFP) so the issuing agency isn't stuck with a prime that's unable to deliver the goods. Most prominent SI/MSP primes that offer data-consolidation services to the federal government don't own qualified data centers—they simply rent qualified rack space, even when data centers amount to more than half of the total data-consolidation solution.

A cloud-neutral approach necessarily entails having a data center with the flexibility to bring in any cloud provider that meets an agency's needs. The provider should offer convenient proximity to critical vendors and access to public-cloud providers plus dedicated infrastructure services that ensure scalable computing and storage with the physical space and capacity to accommodate such scaling. And, most importantly, it should be equipped with FedRAMP-enabled capabilities and meet DCOI objectives.

This EO provides both federal agencies and government contractors a golden opportunity to undertake their data-consolidation efforts in the right way. It means the federal government should be prohibited from building new data centers, which simply don't meet some of its own critical requirements relating to accountability, cost, risk management and cybersecurity. So the federal government must start moving and maintaining its data off site in highly secure, already available DCOI-compliant facilities designed to meet its unique, mission-critical requirements. In doing so, every federal agency can then rest assured that its data has finally moved to a state-of-the-art environment that will empower the agency to focus on its mission instead of squandering time and resources on managing a data center.

About the Author

Mark Gerard is President of DP Facilities, Inc., a data center colocation provider and services firm that has built and owned data centers for Fortune 500 companies in the U.S. and abroad.