VERTIV WHITE PAPER

Federal Data Center Modernization

The Truth About Federal Data Center Modernization

The Obama administration launched the Federal Data Center Consolidation Initiative (FDCCI) in 2010 as part of an ambitious effort to push the federal government to modernize its aging data centers, IT systems and cyber practices. In 2016, the introduction of the Data Center Optimization Initiative (DCOI) superseded FDCCI and further prioritized the modernization of aging government data centers. Uncle Sam has notoriously lagged behind the private sector in terms of adoption of IT innovations, a problem that compounds with every new generation of data centers and IT systems.

The FDCCI and DCOI were intended to address those issues and, if not put the government on equal footing with the rest of us, at least force it to close the gap. It was an important step in the right direction, and some agencies have reduced costs and streamlined operations by implementing cloud-based and hybrid environments. The Trump administration maintained the focus on improving federal computing facilities with the introduction of the Technology Modernization Fund (TMF), a 2018 budget initiative designed to accelerate modernization efforts across the government.

These are good, well-intentioned efforts that have improved the state of federal IT systems, but any objective analysis will show progress remains slow and legacy systems largely entrenched. In fact, the Office of Management and Budget (OMB), in the budget request[1] for the TMF, reported that from fiscal year 2015 to fiscal year 2018, legacy spending across the government as a percentage of total IT spending actually rose from 68 percent to 70.3 percent.

In April 2019, the U.S. Government Accountability Office (GAO) issued a report on government efforts toward data center modernization that indicated progress was, at best, mixed. The full 98-page report[2] looks at achievements across 24 federal agencies in a variety of areas. From the report:

The 24 agencies participating in the Office of Management and Budget's (OMB) Data Center Optimization Initiative (DCOI) reported mixed progress toward achieving OMB's goals for closing data centers and realizing the associated savings by September 2018. As of August 2018, 13 agencies reported that they had met, or had plans to meet, all of their OMB-assigned closure goals by the deadline. However, 11 agencies reported that they did not have plans to meet their goals. Further, 16 agencies reported that, as of August 2018, they had met, or planned to meet, their cost savings targets, for a total of $2.36 billion in cost savings for fiscal years 2016 through 2018. This is about $0.38 billion less than OMB's DCOI savings goal of $2.7 billion. This shortfall is the result of 5 agencies reporting less in planned cost savings and avoidances in their DCOI strategic plans, as compared to their savings targets established for them by OMB. Three agencies did not have a cost savings target and did not report any achieved savings.

In addition, the 24 agencies reported limited progress against OMB's five data center optimization targets for server utilization and automated monitoring, energy metering, power usage effectiveness (PUE), facility utilization, and virtualization. As of August 2018, the agencies reported that 3 had met three targets, 9 had met one target, and 10 met none of the targets. Two agencies did not have a basis to report on progress as they do not own any data centers. Further, as of August 2018, 20 agencies did not plan to meet all of OMB's fiscal year 2018 optimization goals. Specifically, only 2 agencies reported plans to meet all applicable targets; 6 reported that they did not plan to meet any of the targets.

[1] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/ap_16_it.pdf

[2] https://www.gao.gov/assets/700/698448.pdf

That OMB budget request summarizes the dangers of inaction nicely:

> *Aging legacy systems may pose efficiency and mission risk issues, such as ever-rising costs to maintain and an inability to meet current or expected mission requirements. Legacy systems may also operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address and thus may hinder agencies' ability to comply with critical statutory and policy cybersecurity requirements.*

The risks are clear and well known. Two administrations, with Democratic and Republican presidents, have prioritized modernizing federal data centers, and yet – by the government's own admission – progress is limited and spending on legacy equipment is actually increasing. That begs an obvious question: Why?

Understanding and Overcoming Obstacles to Modernization

There is no one reason why modernization efforts have stalled or failed to start altogether. To be fair, these are complex environments supporting complex agencies trying to solve complex problems while facing the prospect of adjusting to new leadership every four years. But there are real, tangible reasons for inaction. Through our work with federal government data center professionals, we have identified four perceived reasons why so many modernization projects can't seem to gain traction. Use of the word "perceived" here is intentional and important to note. In reality, these perceptions are largely inaccurate.

1. Modernization is difficult

Before we discuss why this doesn't have to be true, let's acknowledge some realities about the federal data center system and the men and women who manage those facilities. Facebook, perhaps the most famous and among the largest data center operators in the world, had a revenue of $62.6 billion in fiscal year 2018. That's a lot of cat videos and status updates. And yet, Facebook's annual revenue is less than 1.5 percent of the $4.407 trillion federal budget for 2019. The federal data center system is supporting the world's largest government, which supports the world's largest economy, in the interests of the world's third largest population. This is worth remembering because there is at least a perception that a data center modernization project can be disruptive, and disruption at that scale is unacceptable.

There also are political realities worth considering. Administrations have different priorities. The Trump administration, for example, rolled back more than 80 Obama-era rules or regulations[3] related to the environment alone. Working in the political arena sometimes puts federal employees in the unusual position of undoing efforts they spent four or eight years pursuing. Some sluggishness in taking on big changes is only natural.

Of course, the political calendar isn't the only calculus data center managers must consider. According to Vertiv's Data Center 2025[4] survey, 33 percent of U.S. data center professionals expect to retire by 2025. Assuming those numbers are consistent across the government space, that will represent a massive exodus of experienced, senior data center personnel. Again, it's only human nature to feel some ambivalence toward a large, potentially disruptive modernization project that will mostly benefit your successor – or even some reluctance to implement significant changes the next person may or may not support.

But all of this assumes modernization is a big, difficult process, when the reality is it doesn't have to be. Today's data center infrastructure systems are built for incremental, modular growth. In the past – as recently as 10 years ago – a modernization project might well have been a massive undertaking requiring significant scheduled downtime as systems were transitioned. That is no longer the case. Today, modernization can be managed smoothly, phasing out legacy systems over time to meet the changing needs of the data center. Today's UPS and thermal management systems are designed to be scalable, with the ability to add or subtract capacity as needed without disruption.

Taking that a step further, integrated infrastructure systems are designed and built to tightly integrate power, cooling and IT in modules that are virtually plug-and-play. These can be built in rack, row or aisle configurations and often leverage prefabricated design and construction to ensure quality, rapid deployment and ease of installation and service.

[3] https://www.nytimes.com/interactive/2019/climate/trump-environment-rollbacks.html

[4] https://www.vertiv.com/en-us/about/news-and-insights/articles/pr-campaigns-reports/data-center-2025-closer-to-the-edge/

Simply put, modernization isn't the intimidating, paralyzing prospect it might have been a decade ago. The alternative – inefficiency, rising costs, increased risk of downtime and security vulnerabilities, more frequent service calls, and inability to keep pace with more modern systems – presents far more headaches than a proactive approach to modernizing older data centers.

2. Modernization is expensive

This is a more complicated consideration for federal agencies delaying modernization projects. They live in a world where Congress must approve the federal budget, and members of congress facing electoral scrutiny from their constituents can be understandably wary of sizable capital investments even if those investments promise outstanding total cost of ownership (TCO).

But make no mistake, the price tag for inaction is even larger. According to IDC Government[5], the cost of technology per federal employee is, on average, about $39,000. That's almost $30,000 more than the average industry spends per employee. There are a variety of reasons for that shocking disparity, but propping up inefficient legacy equipment and systems with expensive service and maintenance is on that list.

Make no mistake, there are up-front costs required for a real data center modernization effort. Those costs include everything from new equipment and software to training for staff. As discussed previously, today's scalable solutions make it possible to add only the capacity needed. That makes those up-front costs more manageable than they have been in the past, which is part of a compelling TCO calculation. Consider:

a. Increased efficiency. The industry's understanding of data center energy efficiency is far superior to where it was 10 years ago, and the equipment itself is much more efficient. Today's thermal management systems can leverage outside air to reduce cooling costs and direct cooling to the right areas of the data center more efficiently than ever before. And UPS systems today routinely operate at up to 98 percent efficiency in eco-mode, well ahead of legacy systems that typically operated at 92-94 percent efficiency. While increasing efficiency is a priority in the federal space, the government is smartly moving away from PUE as a metric. Per a June 2019 update to the DCOI[6], data center managers are prioritizing actions and metrics to ensure efficiency, including virtualization, advanced energy metering, server utilization and availability.

b. Reduced footprint. Today's infrastructure systems offer a variety of space-saving benefits. Modular solutions add capacity as needed rather than overprovisioning by adding equipment and infrastructure beyond what is needed to support the load. Integration and creative design have shrunk the amount of floor space required for many devices. Lithium-ion batteries are smaller, lighter, and longer lasting than traditional valve-regulated lead-acid (VRLA) batteries, often reducing the amount of space required for battery storage. That extra space can be used in other ways, potentially reducing facility costs.

c. Simplified operation. Modern IT and infrastructure systems are designed for easy installation and service, machine-to-machine communication, and remote monitoring and management. The equipment is smarter than ever, taking much of the management responsibilities out of the hands of the data center manager.

d. Reduced service. Modern infrastructure equipment is more reliable than even the new versions of corresponding systems installed five or 10 years ago, and exponentially more reliable than outdated legacy versions of the same equipment. Years of use and patchwork fixes only lead to more patchwork fixes. Those service calls can be costly, both financially and in terms of network disruption.

e. Unplanned downtime. The average cost of an unplanned data center outage in 2016 was almost $9,000 per minute[7], up from $7,900 per minute[8] three years earlier. Those costs are only going to go up. Service and maintenance can only do so much. Eventually, older systems fail. The risk is simply too great to bet on squeezing more out of aging legacy systems.

3. Legacy systems work

This is the "if it ain't broke, don't fix it" argument, and it's specious on a number of levels. Not only is simply "working" too low a bar (being functional is far from being an asset), it's also a relative term. Sure, legacy systems may handle the most basic responsibilities of the network, but infrastructure equipment dating back 5-10 years is significantly less efficient, less reliable, and less secure than today's newer, smarter technologies. Older equipment may be "working" in the strictest sense of the word, but it probably isn't working for you.

The federal government has its own ways of doing things and rhythms that often are out of step with the private sector. It isn't immune to outside influence, however. The reality is the

[5]https://federalnewsnetwork.com/reporters-notebook-jason-miller/2016/09/39000-shows-modernization-effort-matters-much/

[6]https://datacenters.cio.gov/policy/#fnref:19

private sector sees the data center as a critical business asset capable of creating a competitive advantage and invests in that asset accordingly. The aging data centers of the federal government aren't keeping pace. In fact, they increasingly are falling behind not just the private sector, but other developed countries as well. Patches to software and firmware work for a while, but eventually secure communication with more advanced outside systems becomes an issue.

Riding outdated data center infrastructure also ignores the reality that data centers around the world are evolving to support a more distributed model. Consumers expect fast, responsive services and applications in all walks of life, and that is driving the push to the edge of the network. The federal government isn't immune to this trend. Modernization isn't just about replacing old equipment with new; it's about fundamental changes to the data ecosystem.

Finally, aging data centers inevitably require more and more service calls. Those calls add up, increasing costs and disruptions in kind. If your approach to your data center is, "if it ain't broke, don't fix it," be prepared for this reality: If it ain't broke, it will be.

4. No market motivation

This gets tossed around quite a bit when discussing differences between government and private sector data centers (among other things), but it simply isn't true. Businesses are beholden to shareholders, who are responsible for driving revenue. Some point to this as the fundamental difference between public and private data centers and the primary reason for lack of enthusiasm for modernization on the government side. In reality, the federal data center managers we speak to feel tremendous pressure to be responsible stewards for their stakeholders – U.S. taxpayers.

Whether it's the Federal Reserve, the Pentagon and U.S. armed forces, or the VA hospital system, federal activities are influenced by outside forces all the time. The federal government doesn't function like a Fortune 500 company, but it isn't immune to external stimuli. That may not be the market in the traditional sense of the word, but it's every bit as competitive and critical to the welfare of countless Americans.

Making the Case for and Moving to Modernization

The government continues to prioritize data center modernization, but progress remains slow and pocketed. The case for modernization can be summarized in three key points.

1. Total cost of ownership

Any concerns about initial capital expenses related to modernization should be alleviated with consideration of the project's TCO. Today's equipment and architectures are more efficient, which reduces energy costs. They are more reliable and more secure, which increases availability and reduces or eliminates costs related to both planned and unplanned downtime. They require less service and maintenance, reducing those costs as well as costs related to disruption caused by service visits. They often are smaller and require less floorspace, opening up that space for other uses. They also have remote monitoring and management capabilities, which certainly reduce worry and likely reduce overtime among data center managers and staff.

2. Benefits of modularity

In the past, data center commissioning has been an exercise in predictive analytics that too often results in bloated, overprovisioned, inefficient facilities. Today's technologies are designed with modularity and scalability in mind, allowing organizations to add capacity only when and where they need it. That eliminates the guesswork and makes for a more streamlined, optimized data center.

3. Keeping pace with the rest of the world

Many federal agencies may be uncomfortable with rapid changes in their data centers and IT systems, but the private sector and many international friends and foes are not. Those who fail to keep pace are left behind, and in the data center that means you run the risk of slow or failed communication with more modern systems. As we've learned in recent years, a new Cold War is being waged online, and enemies of the U.S. are continuously searching for vulnerabilities in government networks they can exploit for their own benefit. Closer to home,

[7] https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf

[8] https://www.ponemon.org/local/upload/file/2013%20Cost%20of%20Data%20Center%20Outages%20FINAL%2012.pdf

many federal data centers have thus far ignored the industry-wide migration to the cloud and the edge of the network, even as demand for those solutions increases across the government. Whether it's the pending $10 billion Project JEDI[9], which could shift massive amounts of Department of Defense activity to the cloud, or the ongoing efforts of the VA system[10] to enhance management of electronic medical records and improve the patient experience, the government IT model is changing. The question every federal Chief Information Officer (CIO) and data center manager must answer is: Will you be prepared to support it?

Modernization Is Possible

Despite the slow and often uneven progress toward modernization, realizing the performance, security and savings goals that have been set in the government IT space is possible. You can be an advocate for change within your organization, busting the myths that have left us with outdated and underperforming legacy systems. These changes will require updated infrastructure, a partner with expertise, and, equally importantly, a willingness to roll up your sleeves and do the important work of bringing government IT fully into the 21st century.

DCOI Strategic Plan Requirement[11]

In accordance with the Federal IT Acquisition Reform Act (FITARA), every federal agency must annually publish a strategic plan to describe the agency's consolidation and optimization strategy. Agencies' DCOI strategic plans must include, at a minimum, the following:

1. Planned and achieved performance levels for each optimization metric by year
2. Planned and achieved closures by year
3. An explanation for any optimization metrics and closures for which the agency did not meet the planned level in a previous strategic plan
4. Year-by-year calculations of target and actual agency-wide spending and cost savings on data centers through the sunset of this policy, including:
    - **a.** A description of any initial costs for data center consolidation and optimization
    - **b.** Lifecycle cost savings and other improvements (including those beyond the sunset of this policy, if applicable)
5. Historical costs, cost savings, and cost avoidances due to data center consolidation and optimization
6. A statement from the agency CIO stating whether the agency has complied with all reporting requirements in this memorandum and the data center requirements of FITARA. If the agency has not complied with all reporting requirements, the agency must provide a statement describing the reasons for not complying.

[9] https://finance.yahoo.com/news/project-jedi-amazon-microsoft-pentagon-175143574.html

[10] https://www.va.gov/opa/pressrel/pressrelease.cfm?id=5084

[11] https://datacenters.cio.gov/policy/#fnref:19

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

VR-11553 (R09/19)